Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras

George Chalhoub and Ivan Flechais, *University of Oxford;* Norbert Nthala, *Michigan State University;* Ruba Abu-Salma, *University College London* (*UCL*) *& Inria*

https://www.usenix.org/conference/soups2020/presentation/chalhoub

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

Open access to the Proceedings of the Sixteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras

George Chalhoub[1], Ivan Flechais[1], Norbert Nthala[2], Ruba Abu-Salma[3]
[1]*University of Oxford*
[2]*Michigan State University (MSU)*
[3]*University College London (UCL) & Inria*
[1]*{george.chalhoub, ivan.flechais}@cs.ox.ac.uk,* [2]*nthalano@msu.edu,* [3]*r.abu-salma@cs.ucl.ac.uk*

Abstract

Smart homes are under attack. Threats can harm both the security of these homes and the privacy of their inhabitants. As a result, in addition to delivering pleasing and aesthetic devices, smart home product designers need to factor security and privacy into the design of their devices. Further, the need for user-centered security and privacy design is particularly important for such an environment, given that inhabitants are demographically-diverse (e.g., age, gender, educational level) and have different skills and (dis)abilities.

Prior work has explored different usable security and privacy solutions for smart homes; however, the applicability of *user experience (UX)* principles to security and privacy design is under-explored. In this paper, we present a qualitative study to explore the development of smart home cameras manufactured by three companies. We conduct semi-structured interviews with 20 designers and their collaborators, and analyze these interviews using Grounded Theory. We find that UX was seen as helpful by our participants in fostering innovation in the design of privacy solutions. However, UX was not used or considered in the design of security solutions due to an explicit need for established, tried-and-tested solutions (i.e., previous traditional security solutions that were seen as effective and reliable to fix certain design problems). Drawing from the findings of our study, we propose a model of UX factors influencing security and privacy design of smart home cameras. We also extract a set of recommendations to improve the security and privacy design of smart cameras. We finally outline several areas for future investigation.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

1 Introduction

Homes are increasingly becoming instrumented, connected, and smart. Devices (including light bulbs, doorbells, door locks, thermostats, and coffee makers) are designed to be Internet-connected and offer greater convenience, functionality, and energy efficiency. However, the rise in the adoption and use of smart home devices is accompanied by new security and privacy threats [1]. Most smart home devices have always-on sensors that collect different types of data and then transmit the data over the Internet to various destinations [2, 3]. The data can be used to spy on or create fine-grained inferences of device users and other home inhabitants. Smart devices also increase the technical complexity of the security infrastructure in smart homes; non-expert home users are expected to protect themselves and their families from various attacks. Increasing numbers of attacks, which have seen attackers taking control of smart homes (e.g., [4,5]), emphasize the need for protecting smart homes. When such attacks happen, smart home device manufacturers often blame users for behaving insecurely (e.g., choosing weak passwords to secure smart home mobile applications [5]), while users ascribe the shortfalls to manufacturers.

Smart home devices do not only affect the privacy and lifestyle of users of these devices, but also those of every inhabitant of the home. In one example, a husband decided to unplug a smart home camera that his wife placed in their house (to check in on her family while she was away) because he felt that the camera was staring at him while he was making coffee [6]. This example illustrates, as Hassenzahl and Tractinsky [7] state, that product attributes must be linked to the needs and values of users (and bystanders in this instance). This entails considering the affective consequences of technology on people, as well as the situatedness and temporality of the product (e.g., the actual or anticipated experience of a user—and a bystander—with the product). Hassenzahl and Tractinsky argue that experience is a combination of elements including the product and internal states of the user (e.g.,

mood, expectations, active goals), which extends over time. The elements interact and modify one another and, hence, understanding the *user experience (UX)* of security and privacy design is important for the successful adoption and use of smart home devices. The importance of UX in the design of smart home devices has long been recognized and advocated for [8–10]. UX encompasses more than usability: it covers emotions, psychological responses, beliefs, perceptions, behaviors, and accomplishments [11].

Prior work has investigated how to achieve security and privacy in smart homes, focusing mainly on technical aspects (e.g., [12, 13]). Other work has also explored the security and privacy of smart homes in a user-centered way, specifically investigating users' knowledge of threats, attitudes, and expectations (e.g., [14]). While studies suggest that factoring UX into security and privacy design can be challenging [15, 16], research is needed to explore the practices of designers (or manufacturers) of smart home devices.

To make a step in this direction, we conducted qualitative user studies with three companies that developed smart home security cameras. We interviewed 20 participants from these companies (n=6, n=8, n=6) who were involved in the design process of smart cameras. Our aim was twofold: (1) to understand how companies factored UX into the design of security and privacy solutions and (2) to investigate how UX influenced the design of security and privacy solutions. We summarize our key findings and contributions below:

1. Product design teams used UX as a means of designing innovative privacy solutions.
2. UX was not used to design innovative security solutions due to an explicit need for established security solutions.
3. Data protection regulations triggered security and privacy considerations, but some regulations were regarded as impractical from a UX perspective.
4. Conflicting interests among departments represented in the design team impeded the UX design of security and privacy solutions.

The rest of the paper is structured as follows: we give an overview of relevant literature in Section 2. We describe our methods in Section 3. We present and discuss our results in Section 4 and Section 5, respectively. Finally, we present our design recommendations in Section 6.

2 Related Work

2.1 Security and Privacy in Smart Homes

Several studies have explored users' experiences, values, needs, and concerns in relation to smart home surveillance (e.g., data collection, use, and sharing) [17–20]. Zeng et al. [14] interviewed 15 smart home users and found that their understanding of threats depended on the sophistication of their mental models. Malkin et al. [21] surveyed 116 users of smart speakers and found that they were protective of the audio command history of children and guests, and that they strongly opposed third-party data tracking. Malkin et al. [22] also surveyed 591 smart TV users and found that they disagreed with their data being shared with other parties despite a lack of understanding of regulations that protected their rights. Geeng and Roesner [23] interviewed 18 smart home users to investigate multi-user interactions and found tensions during installation, normal use, and long-term use. Abdi et al. [24] conducted interviews with 17 smart assistant users and found that they had limited understanding of data storage and sharing. Naeini et al. [25] conducted a vignette study with 1,007 users to investigate privacy preferences, and found that users were more comfortable with data collected publicly, and that they would more likely consent to providing data if it were perceived as beneficial. Apthorpe et al. [26] surveyed 1,731 smart home users to measure the acceptability of third-party data sharing. They provided insights into existing privacy norms and extracted best design practices.

Other studies have investigated the concerns and perceptions of bystanders—such as visitors or co-habitants—who do not make the choice to install smart home devices. Yao et al. [27] ran focus groups and design activities with 18 participants and found three factors impacting the privacy perceptions of bystanders. Bernd et al. [28] proposed to use the framework of Contextual Integrity to research the privacy of domestic workers that are affected by smart home devices, and the design process of product teams who build such devices.

2.2 UX of Security and Privacy

As technology use evolves and becomes embedded in everyday life, the focus on usability (i.e., how easy, efficient, and effective technology is to use) becomes necessary, but insufficient. Broader issues need to be considered, such as social communication, contextual trust, and even aesthetic aspects of security and privacy design.

Dunphy et al. argue that it is crucial to understand how UX is factored into the security and privacy design of technologies [29]. However, there are several gaps in this space: Shava and Van Greunen [30] state there is a "missing link" between UX and usable security and privacy. Other researchers have also reported on the lack of scientific research into UX and usable security and privacy [31, 32].

2.3 UX in Smart Home Security and Privacy

There has been an increased focus on designing user-centered smart home devices [14, 23, 24, 33–36]. However, there has been little research into the role of UX in the security and privacy design of smart home devices [37]. Further, there has been little work exploring how designers and their collabora-

tors think about the UX of these devices [38,39]. In particular, there is a research gap in how designers consider UX during the security and privacy design of smart home devices [40,41]. Bergman and Johansson [42] conducted a structured literature review of 150 smart home research papers and found that there was no research into how product teams factored UX into the security and privacy design of smart homes. Without an in-depth understanding of designers' processes, challenges, and responsibilities, we argue that existing security and privacy issues in smart homes will persist.

Existing research has focused mostly on the practices of developers. Assal and Chiasson [43] interviewed 20 developers to explore real-life software security practices during the development lifecycle and found that security was not considered in the design stage. Similarly, Waldman [44] interviewed 36 product developers and found that product teams did not consider privacy in their decision-making. Further, previous research has found that many gaps existed among product teams on the one hand and security teams on the other hand, which included miscommunication and lack of security knowledge [45,46]. As a result, they found that some companies contracted developers who were security experts to act as an intermediary between product and security teams [47].

The literature suggests that security and privacy may pose UX challenges for smart home developers. Oh and Lee [16] analyzed reviews of quantified self applications and found that privacy was a key problem affecting UX, security, and privacy design processes. This was later confirmed by Bergman et al. [15], 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. [48] found that smart home designers often faced tensions between UX and security in smart homes (e.g., trade-offs between strong authentication and users' ease of interaction with smart devices). Unlike desktop computing, smart home applications span inter-connected physical and digital devices [49], increasing the complexity of factoring UX into the design of smart devices [50]. While UX and usability guidelines are established for desktop systems and web applications, guidelines that specifically target smart home devices are under-researched [49,51]. Moreover, smart home devices lack standardization and quality dimensions [52]. Some general UX rules are recommended for the design and implementation of smart home devices [53], but their effectiveness and suitability have not been explored in detail [54].

In summary, prior research has uncovered a variety of design-related security and privacy issues from the user perspective for which UX is critical (e.g., the need to consider aesthetic aspects of security and privacy). Researchers have argued for understanding and designing the UX of security and privacy [29]. However, the literature reveals that there has been limited work on frameworks, models, and scientific research bridging UX, security, and privacy. Our work takes a step to solve this problem by investigating the role of UX in the security and privacy design of smart home cameras.

3 Methods

We designed and conducted a qualitative user study of designers of smart home cameras based on approaches described in [55–57]. We interviewed 20 participants in the United Kingdom, focusing on understanding the design processes and practices of smart home cameras manufactured by three different companies A (n=6), B (n=8), and C (n=6). We aimed to investigate the design, development, and implementation of three security camera products that had been in production for years. We concentrated on the design of these products because smart home security cameras (i) have a growing adoption rate [58], (ii) are subject to increased security attacks [59], and (iii) are seen as particularly invasive by end-users [60,61]. Our institution's ethics committee approved this study.

3.1 Research Questions

Our work aims to address the following research question:

RQ. How do product design teams factor UX into the security and privacy design of smart home cameras?

To address our main research question, we explore the following sub-questions:

1. How do designers and their collaborators make decisions during the security and privacy design process of smart home cameras?
2. What are the different aspects of the design process of smart home cameras that explicitly deal with UX factors?
3. What are the challenges that different stakeholders face when factoring UX into the security and privacy design of smart home cameras?

3.2 Recruitment

To recruit our participants, we posted flyers and distributed leaflets in the United Kingdom, and advertised the study on online platforms (e.g., LinkedIn). We also recruited participants through snowball sampling, which allowed us to reach employees that were not easily accessible through other strategies. At the time of recruitment, interested participants were employees who were active at their company and responsible for the design, development, or maintenance of a smart home camera product. The participants we recruited from each company were all on the same development team and worked on the same product.

We asked interested participants to complete an online screening questionnaire (see Appendix A). We received 31 complete responses. In addition to asking demographic ques-

tions, we provided participants with a list of job titles and then asked them to choose the title that best described their position at the company (e.g., UX Designer, Security Engineer, Product Manager). We describe the demographics of our participants in Table 1 in Section 4.

Additionally, we asked participants to provide information about their company. We also asked them to specify the type of products that their company manufactured (e.g., security, lighting, or phone systems), as well as the specific products their company manufactured (e.g., cameras, hubs, voice assistants, lights). Finally, we asked participants to estimate the number of employees who worked at their company. The number allowed us to establish the company size (e.g., startup, mid-size, enterprise) since we were interested in targeting large-scale product development companies that were more likely to put effort into improving the UX of products [62].

3.3 Interview Procedure

We conducted semi-structured interviews with 20 employees working at companies that manufactured smart home devices: Company A (n=6), Company B (n=8), and Company C (n=6). We used the funnel technique [63] to structure our initial interview questionnaire (study script), starting with general questions and then drilling down to specific ones.

The interview started with general questions characterizing participants' role at the company (e.g., responsibilities, duration of employment), the type of products they designed or developed, and their perspectives on UX, security, and privacy. Members of design teams referred to different groups of people (e.g., device purchaser, device administrator, and device user in the house) as 'users' without distinction. 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., UX in the security and privacy design process, UX design methods, techniques, and artifacts).

Finally, we asked specific questions related to the profession of participants: regulatory stakeholders were asked about data protection regulations, product liabilities, and regulatory affairs; management stakeholders were asked about roles and responsibilities related to security and privacy; security stakeholders were asked about security requirements, the design of security, security maintenance, and security breaches.

We conducted our interviews remotely using Skype and Zoom. We also audio-recorded and transcribed all interviews. Interviews lasted for an average of 52 minutes. Our interview questions can be found in Appendix C.

3.4 Pilot Study

After creating our initial interview questions (see Appendix B), we conducted a pilot study with four smart home product designers at a local conference. Two researchers recorded and analyzed the pilot interviews. We used the findings to identify potential problems (e.g., adverse events, time, cost) in advance prior to conducting the full-scale study. Drawing from our findings, we made the following changes:

- We refined our interview questions to reduce bias and improve their quality.
- We changed our data analysis method from Thematic Analysis to Grounded Theory because we aimed to (i) develop a substantive theory, (ii) deeply explore design processes, and (iii) derive grounded recommendations.
- We were better informed of the average duration of our interviews, which turned out to be around 50 minutes.

3.5 Data Analysis

We transcribed and analyzed all 20 semi-structured interviews using Grounded Theory, following Strauss and Corbin's procedure [64]. 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 [65].

Four researchers in total analyzed the transcripts. The primary researcher (who conducted the interviews) and a second researcher independently completed the initial coding of all interview transcripts. To verify the credibility of the initial codes, a third researcher cross-checked the codes against the interview transcripts. At the same time, the fourth researcher reviewed the initial codes and supporting quotes. The four researchers discussed any differences and generated a codebook of 155 codes. The researchers then grouped the codes into themes (axial coding) and categories (selective coding).

We observed data saturation [66–68] between the 18^{th} and the 20^{th} interview; i.e., no new codes emerged in interviews 18–20, and, hence, we stopped interviewing. After creating the final codebook (see Table 4 in Appendix D), we tested for inter-rater reliability. The average Cohen's kappa coefficient (κ) for all codes in our data was 0.81. Cohen's kappa values over 0.80 indicate almost perfect agreement [69].

3.6 Research Ethics

The University of Oxford Central University Research Ethics Committee reviewed and approved the study (CUREC/CS_C1A_19_049). Before each interview, we asked participants to read an information sheet and sign a consent form that presented all the information required. Participants had the option to withdraw at any point during the study.

3.7 Limitations

Security, privacy, and regulatory matters are sensitive issues in big organizations like the ones we interviewed (see Table 2). Our participants' corporate responsibilities as well as their company's reputation might have biased their responses. To mitigate this, we explained to our participants that data would be collected and processed in accordance with the General Data Protection Regulation (GDPR).

Further, self-reporting bias is common in user studies [70]. Some participants might not have responded accurately to our questions because they did not remember specific details or wanted to be viewed as socially acceptable. 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.

Finally, 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 [71], we interviewed 20 participants until new codes stopped emerging.

4 Results

In this section, we detail the findings of our study. We present our participant demographics (Section 4.1), and then discuss our key findings organized according to the main themes of our analysis, as illustrated in Figure 1. The main themes are:

- Development Process (Section 4.2);
- UX in Security Design (Section 4.3);
- UX in Privacy Design (Section 4.4);
- Innovation in Security and Privacy Design (Section 4.5);
- Trust (Section 4.6).

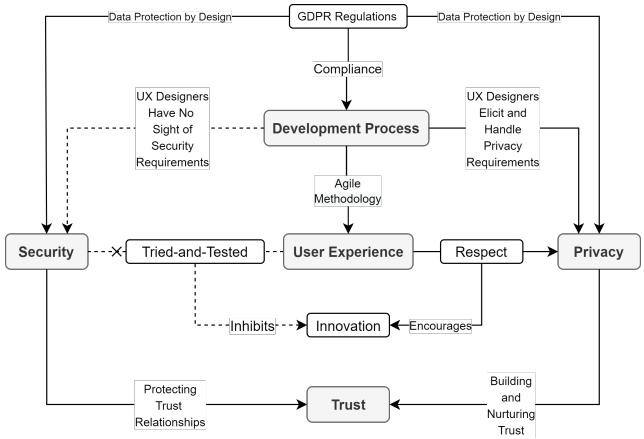

Figure 1: Drawing from the findings of our study, the figure describes a model showing how UX was factored into the security and privacy design of smart home cameras.

4.1 Participant Demographics

Table 1 summarizes the demographics of our sample (n=20). We interviewed 12 male and eight female participants. Ages ranged from 25 to 52. Ten participants had a college (or an undergraduate) degree, and ten had a graduate (or postgraduate) degree. We divided our participants (n=20) into six groups of stakeholders based on employment: security stakeholders (n=4), regulatory stakeholders (n=3), UX stakeholders (n=5), management stakeholders (n=4), software stakeholders (n=2), and hardware stakeholders (n=2).

	Gender	Age	Degree	Experience	Employment
A01	Female	46	M.A.	4 years	Product Manager
A02	Male	28	B.A.	2 years	UX Designer
A03	Female	42	M.Sc.	5 years	Security Manager
A04	Male	30	M.Eng.	2 years	Security Engineer
A05	Male	32	M.Sc.	2 years	Hardware Designer
A06	Male	44	M.A.	6 years	UX Director
B07	Female	52	J.D.	7 years	Legal Counsel
B08	Female	31	J.D.	2 years	Compliance Counsel
B09	Female	38	B.A.	4 years	Experience Designer
B10	Male	43	B.A.	7 years	Product Designer
B11	Male	27	B.A.	2 years	UX Designer
B12	Male	35	M.Sc.	4 years	Security Architect
B13	Male	28	M.Sc.	3 years	Mobile Developer
B14	Female	31	B.Sc.	4 years	Software Engineer
C15	Female	46	J.D.	6 years	Product Counsel
C16	Male	36	B.A.	6 years	Senior UX Designer
C17	Male	29	B.Eng.	2 years	Hardware Engineer
C18	Male	50	B.Bus.	8 years	Product Manager
C19	Female	34	B.Sc.	4 years	Security Engineer
C20	Male	25	B.Sc.	1 year	Software Developer

Table 1: Semi-structured interview participant demographics.

4.2 Development Process

All participants (designers and their collaborators) followed an agile product development process, which included requirements analysis, design, development, testing, and maintenance [72]. In this section, we report on the requirements analysis, design, and development stages that companies A, B, and C (see Table 2) followed to develop products PA, PB, and PC (see Table 3). We describe how GDPR influenced the development process of smart home cameras. We also describe the challenges that UX design activities and smart homes introduced to our participants.

Company	HQ	Employees	Product	Designed in
A	UK	500+	PA	UK
B	USA	1000+	PB	UK
C	USA	1000+	PC	UK

Table 2: Summary of companies.

Product	Type	Major Functionality
PA	Camera	Motion and sound detection with alerts.
PB	Doorbell	Real-time monitoring/audio features.
PC	Camera	Face recognition/detection of intruders.

Table 3: Summary of products.

4.2.1 Processes and Approaches

We briefly describe the processes and approaches of the design teams working at companies A, B, and C. All teams combined hardware and software development in agile and iterative design processes.

Company A. A cross-functional team that involved various stakeholders (e.g., senior UX/UI designers, software and mobile application developers, industrial designers, product managers) was in charge of questioning, exploring, defining, and making decisions related to the design of product PA (a camera). The team ran multiple workshops with designers and developers to explore various ideas and techniques, become familiar with common design patterns, and understand the product's business strategy. They followed a collaborative UX design process (multi-staged UX [73]).

Company B. A self-managing agile team was in charge of the design and development of product PB (a doorbell). The team was composed of different experts (e.g., designers, developers, engineers) who met on a regular basis to share data, communicate, collaborate, and discuss their progress. No managers were controlling or directing the team because team members decided how to prioritize their work, manage their team, and achieve the goals of the project. UX designers were in charge of eliciting functional and quality requirements by applying different UX activities related to the use cases of the product. The requirements were extracted from user needs identified by UX research (e.g., personas, prototypes, interviews).

Company C. A functional team—operating in a traditional organizational structure—adopted agile mindsets, principles, and practices and was in charge of the development lifecycle of product PC (a camera). The team consisted of senior UX designers, product managers, and software developers. The team leader reshuffled team members regularly depending on the project's needs and requirements. Team members met regularly and were familiar with each other's work processes. UX designers, developers, and content designers conducted user research and made explicit UX decisions during the early stages of their projects. The team elicited requirements during the design, development, and implementation phases.

4.2.2 GDPR and Compliance

All three companies were required to comply with GDPR [74], which mandated *Data Protection by Design* (DPbD) [75] practices (as reported by A3, B7, and C15). In practice, a DPbD approach requires companies to *"consider privacy and data protection issues at the design phase of any system, service, or product."* [76]

Delayed effect. GDPR came into force on May 25th, 2018, after the smart cameras of companies A, B, and C had been developed and released. Product Counsel C15 said that the devices produced before the enforcement date were non-compliant with GDPR. Similarly, Legal Counsel B7 said that the company's infrastructure that stored user data was not equipped to deal with GDPR requests. Security Architect B12 stated that making changes in the existing product architecture required an increased demand for labor, money, and effort.

Obtaining consent. GDPR requires smart home companies to obtain clear and valid consent from users to the use of their data. Due to the large amount of data exchanged in the ecosystem of company C's products, consenting to *all* uses of data was described as technically challenging by Product Manager C18. UX Designer A2, who was familiar with GDPR, stated that asking users to consent to all uses of data in their ecosystem would be detrimental to UX. A2 said: "*I think it would be too overwhelming for users to see every single piece of data that we collect.*"

Right to withdraw consent. Under GDPR rules, smart home users have the right to withdraw their consent at any time, which requires companies to delete user data. However, in the case of company C, Security Engineer C19 reported that their smart camera was often used with other company products as well as by third-party products (e.g., Amazon Alexa). C19 explained that the increased number of devices that shared customer data made complying with this regulation demanding. C19 described that their infrastructure "*is not designed to destroy the data just like this, with one click.*" C19 also mentioned that lack of control of data collected by third-party devices made complying with this regulation "*very challenging*." In particular, C19 stated that it was difficult to determine whether third-party devices; e.g., Amazon Echo, were GDPR-compliant due to the lack of clear guidelines showing how third-parties collected and processed user data.

Conflict between business and regulation. Different and conflicting design goals could arise during the design phase. Security Manager A3 reported dealing with a tension between commercial and regulatory stakeholders. The *Legal Department* wanted some of the data collected from users to remain stored on users' cameras (i.e., offline); however, the *Commercial Department* requested all data collected to be stored on the company's cloud servers. A3 explained: "*The legal team asked to keep the data local only, but at the same time the commercial team wanted us to collect it. I guess they wanted to monetize it.*" This reported conflict highlights the important role of regulation in smart homes.

4.2.3 UX Design Activities

Participants reported different challenges during different activities of the UX design process.

Identifying pain points. UX designers (n=2) investigated data monitoring and collection in smart home cameras (through conducting research) to appropriately *"identify the main sort of frustrations and pain points"* (A2). A2 interviewed smart camera users to research *"acceptable areas of monitoring"*; however, they could not identify the pain points resulting from monitoring. To address this problem, A2 interviewed psychologists and visited existing customers in their house. A2 was able to identify six major pain points related to video monitoring. For example, A2 found that customers were concerned about cameras spying on them—by passively collecting data without their knowledge.

Making UX design decisions. UX designers made recommendations, but did not always make design decisions. UX Designer B11 reported that despite conducting user research and suggesting UX-aware changes, they did not make any final decisions; they were instead made by the project manager. B11 said: "*Ultimately, it's always their decision at the end of the day, but it has always been difficult for my job to ensure that I'm providing the best experience possible.*"

Fully understanding user behavior. UX designers (n=3) mentioned that one persistent UX challenge they faced was to fully understand the security behavior of users. A6 commented: "*The reality is we won't know the exact behavior until the product is out.*" The difficulty of understanding real user behavior is a challenge that is well-known to the usable security and privacy community [77].

Making hardware design changes. Hardware stakeholders (n=2) faced issues when applying UX-related changes to existing products. In company A, industrial designers faced difficulties when implementing a privacy feature which would visualize the on/off state of smart cameras. Hardware Designer A5 explained that software developers were more flexible: *"while mobile developers are flexible, we have to make early decisions that are not easy to change."* Similarly, Hardware Engineer C17 said there was not enough time to build hardware sprints. The lack of flexibility (e.g., time, effort) made it difficult to apply UX changes to existing products.

4.2.4 Interoperability of Smart Home Devices

Participants reported two smart home interoperability challenges that occurred during design and development.

Heterogeneous devices. Participants (n=2) stated that the integration between heterogeneous devices and company products was important to companies. For example, most products in company A supported heterogeneous devices and services, such as Amazon Alexa, If This Then That (IFTTT) applications, and Apple's Siri (A1). Third-party services (e.g., Amazon Alexa) "*improve[d] [user] experience*" (A2); however, they created difficulties for security stakeholders. Security Engineer A4—who worked on encrypting the data exchanged between the company's ecosystem of products and Amazon Alexa—described the process as *"complex"* and *"time-consuming."* A4 specifically reported dealing with a legacy platform unable to send and receive encrypted messages with the API of Alexa Voice Service [78].

Securing connections between devices. Security Engineer C19 stressed that their company's smart home devices had *"solid security."* The challenge, however, was encrypting data exchanged among the increased number of devices in the company's ecosystem. C19 explained: *"Smart home devices are generally secure... The problem is the number of connections between all of those devices, they all have to be protected."* In addition, Product Designer B10 explained that the increased connections between devices, touch points, and objects would add to the complexity of this challenge. Complexity in smart homes was previously reported in the literature [79].

4.3 UX in Security Design

In this section, we present how design teams applied UX principles and practices to the design of security features that end-users interacted with. We found that UX was not factored into the design of security solutions due to lack of expertise and the misperception of security being a low-priority technical-only problem. In addition, we found that GDPR and security audits motivated UX considerations.

4.3.1 Alignments between UX and Security Design

Regulations and legal liabilities. We found that regulation triggered security design considerations. Although security was not explicitly factored into company B's design phase, regulations and legal liabilities required designers to consider some security requirements. UX designers in company B attempted to consider regulatory requirements in the design phase although they faced several obstacles (i.e., high-level guidelines). Legal Counsel B7 mentioned that the introduction of GDPR's *"Data Protection by Design"* requirements prompted doorbell design teams to implement new security features (i.e., stronger encryption during authentication).

Security audits looking into user behavior. All three companies conducted security audits to establish how well their information system conformed to security standards and frameworks. We found that security audits in companies B and C prompted security design considerations. During a security audit led by Security Architect B12, a security review was conducted to investigate the password strength of the accounts of PB's users. B12 found several instances of poor password

behavior, which prompted an evaluation of password strength as well as the creation of UX-aware password requirements (e.g., the addition of password strength meters).

4.3.2 Incompatibilities between UX & Security Design

Design of security features was not explicitly anyone's responsibility. Among our participants (n=20), no one took responsibility for the design of security features. Participants (n=5) who handled security design tasks said they were not accountable for security design issues. Those participants did not have UX design expertise. For instance, Product Manager A1, who made security design decisions based on their understanding of common security practices, said that the *Information Security Team* was responsible for all matters related to security, including security design. However, Security Engineer A4 from the *Information Security Team* dismissed any responsibilities related to the design of security features.

Security design was a low-priority concern. For some stakeholders (n=2), security design was acknowledged but perceived as low-priority. As a result, minimal efforts were made to introduce security stakeholders in design teams that handled UX design. Security Manager A3 explained that the budget of the *Information Security Team* was limited, and that adding security experts to the design team was a *"luxury"* they could not afford. Moreover, Product Designer B10 expressed similar thoughts when discussing the addition of a '*usable security expert*' to the design team.

Security was seen only as a technical problem. Many participants (n=15) described security as being only a technical problem that should be addressed from a technical perspective. As a result, participants expected that security to be exclusively handled by developers and security experts. This perception gave little to no consideration to social aspects of security. For instance, when we asked UX Designer B11 why security was not part of the design process, B11 stated that this was *"a development question."* Security Engineer A4 had a similar response: *"Designers do not have any security expertise and it doesn't make sense to expect them to handle security problems."* This finding is not novel, but confirms the existence of a long-term challenge in HCI where security is treated as a technical problem [80], regardless of ongoing efforts to bridge the gap between social and technical aspects of security design [77].

Security features were not designed by usable security or UX experts. In company C, sensitive features related to the connectivity of security cameras, firmware upgrades, and registration were designed by Software Developer C20. Similarly, Product Manager A1 – in company A – did not "*see the value*" of including security experts in the design team, and chose security features – such as authentication – based on their understanding of common security practices.

UX designers had no sight of security requirements. Security requirements were not always present in the UX design phase. Experience Designer B9, who played a core part in the design of the doorbell (PB), said that the requirements he was provided with did not include data protection or security requirements. Similarly, UX Designer A2 explained that the security of registering and processing data was discussed during the design phase. However, there were no requirements related to security design: "*There wasn't specific kind of UX work around data protection or user protection or something like that.*"

Security design considerations were ad hoc. For some participants (n=5), features handling sensitive information (e.g., authentication, software patches, access to video footage) created security design considerations on an ad hoc basis. For example, Mobile Developer B13 designed the software update development process for the doorbell mobile application. B13 strongly valued the design of update features because they realized that these features could be used to deliver security updates. In all five cases, ad hoc design security considerations were triggered by non-experts of security design: management stakeholders (n=3) and development stakeholders (n=2). This finding confirms Assal and Chiasson's study results [43], which suggested that ad hoc security considerations are fragile because non-experts of security design (e.g., developers) could fail to identify security-sensitive features.

Lack of security experts in design teams. The product design teams of companies A, B, and C did not include security experts. In company A, the *Information Security Team* was not involved in the design phase of their smart camera. Justifying the decision, Security Manager A3 stated that all company employees underwent annual training and followed the company's *"information security management framework."*

Security was only considered at the implementation stage. For some security stakeholders, security design was acknowledged but was not seen as a priority. The *Security Team* in company B prioritized working with the *Development Team* over the *Design Team*. Security Architect B12 who worked with the doorbell *Development Team* said: "*I know that we can get involved with designers, but well, it's more efficient to work with the development team.*"

Security was reactive and not proactive. Security stakeholders (n=2) reported that security design was treated as reactive, rather than proactive, in companies A and B. Companies preferred a reactive approach, in which they made security design considerations or changes based on security incidents reported by customers. For example, Security Architect B12 reported that their security teams had implemented multi-factor authentication as an option to secure user accounts after successful account hijacking attacks were reported.

4.4 UX in Privacy Design

In this section, we present how design teams applied UX principles and practices to the design of privacy features that end-users interacted with. We found that UX was factored into the design of privacy solutions in companies A and B through considerations of consent, transparency, and user control. However, in company C, UX was not considered in the design of privacy features due to lack of expertise and relying on a general understanding of privacy issues and product use.

4.4.1 Alignments between UX and Privacy Design

Giving users control. Companies A and B gave customers more control of their privacy settings, which UX designers reported to increase trust. For example, both companies implemented a privacy mode in their mobile application in order to allow users to stop camera monitoring. In company A, designers also aimed to make users "*feel in control*" by adding (1) a visible on/off feature that showed the current state of cameras and (2) a privacy mode to give users "*peace of mind*" (A2)—allowing users to automatically or manually disable cameras when using their mobile application. In company B, UX Designer B11 explained that they added a private mode because their customers shared their cameras with family members: "*We do have a privacy feature in our product which allows you to switch the [...] whenever users want to have privacy. [...] When we interviewed users, we realized that a lot of them share their camera with others, mostly family members.*"

Being transparent with users. Participants (n=7) reported that their company made numerous efforts to be transparent with users. Legal Counsel B7 described that the *Legal Department* at company B worked with UX designers to create user-friendly FAQ pages that explained how their company collected and processed user data, as well as the measures they took to protect data. Further, B7 mentioned that the company constantly reminded users of their right to get their data deleted (by sending regular reminder emails). On the other hand, company A, which had to deal with multiple security vulnerabilities in the past, had recently updated its data breach incident response plan to inform customers of data breaches (A3). UX Director A6 helped the company use best practices to ensure that affected users had the best experience possible.

Obtaining explicit consent from users. UX designers (n=2) described different projects that looked into obtaining explicit consent from users in relation to data collection and sharing. UX Director A6 described an on-going project looking into obtaining consent through visual indicators instead of text-heavy documentation that would be difficult for users to read. UX Designer B11 worked on developing user-friendly consent notifications for the camera's mobile application. In addition, developments were made to allow customers to change their own privacy settings based on their needs.

Ensuring smart home cameras were not 'creepy' or intrusive. UX designers (n=3) conducted user research with the aim to design smart home products that were not 'creepy' or 'intrusive'. In company A, the goal of UX designers was to ensure users felt comfortable with their camera (PA), and that it did not make users feel that it was a "*tool of surveillance*" (A6). To achieve their goal, UX Designer A2 interviewed psychologists and visited existing customers in their house to identify acceptable and non-intrusive "*areas of monitoring.*" In company B, Experience Designer B9 assisted in the design of a feature which allowed cameras to "*detect human activity based on geographic location*." B9 explained that the feature allowed users to automatically disable their smart home camera when they were at home and, hence, the device did not feel "*creepy*."

4.4.2 Incompatibilities between UX and Privacy Design

Designers of privacy features lacked expertise. In company C, privacy features were designed by stakeholders (n=2) who did not possess design or privacy expertise (e.g., developers, product managers). Software Developer C20 designed the privacy mode settings of the camera's mobile application during the development process. C20 made privacy design decisions based on their own understanding of sensitive data. Similarly, Product Manager C18 made privacy decisions related to a feature that allowed family members to disable video monitoring and notifications. Both stakeholders did not refer to any design or data protection guidelines. C18 said: "*We didn't follow any requirements, no. [...] I don't know why, I wasn't aware of any requirements.*"

Some privacy solutions were designed based on a general understanding of product use. Company C's *Product Design Team* appeared to deal with privacy design based on a general understanding of product use, rather than a thorough investigation of the specific context of use. For instance, Product Manager C18 believed that privacy concerns of users would better be dealt with by understanding users in a broad and wider context of user-centered design.

Privacy was not explicitly discussed during user research. The *Product Design Team* of company C did not explicitly discuss privacy during the design phase. Senior UX Designer C16 – who worked with product designers, engineers, and managers – said that privacy was not discussed during the user research phase when user interviews were conducted.

4.5 Innovation in Security and Privacy Design

We found that innovation cross-cut UX with security and privacy. In this section, we describe how innovation seemed to enhance the design of privacy solutions, but also to impede the design of security solutions.

4.5.1 Enablers of Innovation in Privacy Design

New privacy features were supported by qualitative and quantitative UX research. UX stakeholders (n=4) working at companies A and B adopted a mixed qualitative-quantitative approach to build new features that addressed user privacy (e.g., concerns, pain points, expectations) during the design phase. To design features related to camera monitoring, UX Designer A2 conducted qualitative interviews with users as well as observed users in their homes to address any privacy concerns. UX Director A6 conducted quantitative research by collecting and analyzing survey data to design a visible indicator that showed whether a camera was turned on or off. A6 also used existing quantitative data from Google Analytics to prioritize which privacy features to implement. Experience Designer B9 created detailed storyboards and personas to visualize how their doorbell would be used in users' homes and whether it would be intrusive.

New privacy features were evaluated through usability testing. UX stakeholders (n=2) conducted usability testing of new privacy features introduced by company B. This was used to ensure that new privacy features did not negatively affect customer experience. UX Designer B11 delivered usability testing results to the *Product Design Team* based on the analysis of mobile application prototypes. B11 mentioned that among these prototypes, some requirements were related to privacy features. B11 explained that users were observed interacting with and changing privacy settings. Similarly, Experience Designer B9 conducted usability testing of the doorbell privacy features and was able to identify issues that prompted design considerations.

4.5.2 Barriers to Innovation in Security Design

Security solutions were tried-and-tested. Security experts (n=3) mentioned that their companies' *Information Security Team* did not design their own security solutions. Instead, they used existing security solutions in their company's security protection paradigms, a practice known as *tried-and-tested* security. Additionally, non-experts also made security design choices supported by their own understanding of common security solutions. Product Manager A1, who worked with the *Design Team* that did not include security experts, chose the *"username and password"* authentication mechanism since it was familiar, widely-used, and accepted in industry.

New security solutions increased uncertainty. Participants (n=2) explained that incorporating tried-and-tested security solutions avoided uncertainties that arose out of the introduction of new security features. Product Manager C18 mentioned that new security solutions were likely to create usability concerns due to lacking information on how users would interact with such features. Similarly, Security Engineer C19 mentioned that attempts to introduce new security features were discouraged in the *Security Team*. C19 explained that introducing new security features would increase security risks due to lacking the knowledge required to design these features.

4.6 Trust

We found that trust heavily influenced UX design choices: product teams aimed to build customer trust through better privacy experiences, and also aimed to protect trust relationships with their customers through data protection policies.

Building and nurturing trust through privacy experiences. We found concerted efforts in the companies that aimed to build a culture of fostering trust. In company C, Product Counsel C15 explained that employees were encouraged to take an interest in and care about protecting user privacy. Similarly, in company B, Legal Counsel B7 described efforts put into creating a customer-first culture, where user privacy was not only seen in development processes but also discussed and encouraged culturally among product teams.

Protecting trust relationships through data protection policies. Product teams (n=5) used data protection policies to protect their company's reputation and build user trust. Many companies had established policies to deal with security vulnerabilities and attacks. For example, Security Manager A3 reported that his company adopted an incident response plan in case of a breach, in order to maintain its reputation, which we identified as a powerful motivator for companies to take security measures. Similarly, Security Architect B12 reported that their *Security Team* had invested in "*developing well-founded requirements*" for responding to security incidents, even when incidents resulted from users' incompetence (e.g., falling for a phishing attack, a compromised home router). Security Engineer C19 said their company drafted a "*responsible disclosure policy*" which dealt with managing security vulnerabilities reported by users.

Overall, our interview participants identified that customer trust was strongly linked to data protection: security was needed to mitigate loss of trust arising from exploiting security vulnerabilities. Further, user privacy was used by product teams to build and nurture trust relationships.

4.7 Summary

All product teams used an agile methodology to drive the development of their smart home products. We found that the practice of using tried-and-tested security solutions inhibited innovation in security design. In addition, the perception of security being only a technical problem, for which there were 'best-practice' technical solutions, limited the consideration of social and interactive aspects of security. In particular, it created a gap between UX considerations and security design (e.g., UX designers had no sight of security requirements).

Despite the gaps that we found in security design, our results show companies innovated in the privacy design space (e.g., company B created a novel geographic-based privacy feature). Our data shows that UX stakeholders in design teams elicited and handled privacy requirements. The practice of using UX design principles to respect user privacy (e.g., giving users control, avoiding creepiness and intrusiveness) seemed to encourage innovation in the privacy space. Moreover, we found that companies were motivated to preserve a trust relationship and build trust with their customers, as privacy or security failures (e.g., intrusive or vulnerable products) would undermine that relationship. Finally, regulations (e.g., GDPR) legally required design teams to consider data protection by design in their requirements.

5 Discussion

Our results uncover complex challenges and limitations that product designers faced: challenges arising from complying with GDPR; the importance and role of building trust; barriers to factoring UX into security design solutions. In this section, we use our findings to discuss the wider role of innovation in designing security and privacy solutions, as well as the implications of adopting a user-centered agile approach to data protection. We also highlight areas for future work.

5.1 The Role of Innovation in Security and Privacy Design

All novel issues related to smart home security and privacy point to significant challenges where innovative solutions are necessary. Despite recognizing the importance of security in the design process, our results show design and security teams are less innovative due to existing practices and perceptions. These practices include favoring tried-and-tested security solutions or procuring security solutions from reputable vendors. This finding highlights a desire to avoid novelty and a preference to 'follow the crowd' in the design of security.

Further, the perception of security as only a technical problem, for which there are "best-practice" technical solutions, limits design considerations for security solutions (e.g., authentication consisting of only username and password combinations). Many smart home devices are designed for operating in privacy-sensitive environments (e.g., personal spaces). Given the relative immaturity of the smart home device space, tried-and-tested solutions are not particularly suitable, and innovative solutions are required. For example, current designs do not accommodate the diversity of social aspects of smart home security and privacy (e.g., the nuance between a device being in a shared space in a flat-share vs. being in a shared space in a single-family household).

While we found no evidence of innovation in security design, our results show that efforts have been made to innovate in the privacy space. For instance, company B created a geographic location privacy feature which could detect human activity and make their doorbell less intrusive. One reason for this was that companies wanted to preserve their trust relationship with their customers, and privacy failures were seen as potentially "creepy" and "intrusive," which would undermine this relationship.

The current efforts of innovation in privacy design are a good first step, but more is needed. For example, the challenge of communicating and obtaining user consent in smart homes needs to be systematic (e.g., within the same device ecosystem) and coordinated (e.g., among device ecosystems). However, this is currently not the case and highlights the need for better communication and coordination between stakeholders and product teams.

While data protection regulations (e.g., GDPR) appear to be consistent with better UX design for privacy in smart homes, these regulations remain unclear as to whether the same could be true with regards to UX for security design. Security and privacy qualities of smart homes are not the same; however, both are qualities of data protection. It is not clear how much responsibility users should have to ensure the secure operation of their devices. However, some manufacturers blame breaches on users who do not adopt secure practices (e.g., failing to change default passwords). Regardless of where responsibility lies, manufacturers could put effort into improving security experience, making it easier for users to achieve their desired security outcomes. One option would be for data protection legislation to explicitly cover security experiences, as currently there are very few incentives for manufacturers to put additional effort into enhancing the UX of security.

Regardless of whether regulations should encompass UX aspects of both security and privacy, design standards, guidelines, frameworks, and APIs are other options which have not been explored from an innovation perspective. The tensions that exist between regulators and UX designers over communicating the use of data (e.g., despite being required by GDPR, UX designers do not typically ask users to consent to all uses of their data because—otherwise—it would be detrimental to UX) should invite us to find innovative solutions that satisfy both parties: regulators and users.

5.2 Security Design in Agile Development

Agile teams have historically treated security as a technical problem, ignoring its social and interaction aspects [81]. With that in mind, we argue that in an agile setting, security would still not be considered during the design stage and would, hence, remain an implementation problem. In company A, Security Manager A3 described their *Information Security Team* as "*the department of 'no' when it comes to enforcing security.*" This problem has been common in the past where

security teams blocked progress in agile environments with the attitude of "security says no" [82].

Moreover, agile development does not have built-in steps for explicitly dealing with security issues because it was not designed with security in mind [83]. This might explain our results which show that product design teams who used an agile development process did not explicitly consider security issues during the design phase. However, our results show that GDPR required design teams to follow DPbD requirements, in order to build legally-compliant products. We argue that this is a promising step toward better considerations of security design in agile teams, but this is accompanied with noteworthy challenges and barriers, especially in the context of smart home ecosystems.

5.3 Directions for Future Work

In this section, we outline areas for future investigation.

Innovation without hindering security. Our results show that tried-and-tested solutions were highly demanded in companies A, B, and C which preferred reliability and assurance (e.g., reusing best-security practices). Those practices were shown to hinder innovation; however, we believe more research is needed to explore the relationship between UX, innovation, and security. A key issue to uncover is what aspects of security design can be safely innovated, and how UX can be used to design more effective security experiences.

UX-aware data protection guidelines. Our findings show that data protection regulations (e.g., GDPR) influenced the design phase. Our participants reported that GDPR touched on facets of product design but often failed to translate into specific requirements, which caused disparities in the design process. While GDPR requires practitioners to factor security and privacy into the design process, it can bring more confusion to the design table: regulatory requirements have been reported to be high-level and impractical [84]. New techniques and tools are needed to address how data protection regulations and practices can factor the application of UX design principles.

Improving communication among different stakeholders. Our results show poor communication among multi-stakeholder teams where security design happens. In the absence of regular communication among stakeholders, the number of implicit assumptions made increases (e.g., in our study, Product Manager A1 selecting security features based on their own knowledge of common practices) [85]. Similarly, tensions among stakeholders also increase. For example, in Company B, UX Designer B11 was frustrated that they could not make UX-aware decisions. Expecting largely autonomous groups of stakeholders (e.g., security, legal, design, UX) with different goals, motivations, and constraints to speak the same language is unrealistic. Therefore, more research into this area should explore how to make different teams communicate effectively about factoring UX into the security and privacy design of smart home products.

6 Conclusion

Studies and recent events show that security and privacy of smart home products can have detrimental and life-threatening effects on people (e.g., compromised products have allowed attackers to spy on residents and control home networks). Design must consider users' motivations, perceptions, and expectations to enable users to effectively protect themselves when using these products.

While research suggests that factoring UX into security and privacy design is important, the practices of product designers in this space have not been empirically explored. To bridge this gap, we conducted three user studies involving 20 interviews with security camera designers. We analyzed the data using Grounded Theory and found that design teams used UX as a means of innovating in privacy design to address social aspects of privacy, in particular to avoid intrusiveness. However, UX was seen as undesirable for innovating in security design due to the belief that security was only a technical problem where tried-and-tested solutions were the only option. Based on our findings, we conclude with recommendations to improve design practices in smart homes:

Explicitly aim to innovate through UX of security. Tried-and-tested security solutions are preferred by design teams as they provide a measure of assurance that they are effective and reduce vulnerabilities. The challenges introduced by smart homes (e.g., diverse social contexts, varying levels of skill and ability, subtle tensions among stakeholders) are not addressed by current tried-and-tested security solutions. By exploring security through the lens of UX, new ways of simplifying and streamlining interactions can be uncovered. While these innovations may also lead to new security challenges, it is necessary to innovate in order to design better solutions that will eventually become tried-and-tested for smart homes.

Align security and privacy in UX. Our results show that UX of security design is not distinct in practice from UX of privacy design. Many technical aspects of security and privacy design have common principles and, thus, could be considered as part of a single UX domain—instead of being broken down into separate components, such that one is in scope and one is not.

Factor UX into the practice of data protection compliance. The compliance aspect of data protection regulations strongly motivates security and privacy considerations (e.g., DPbD). Our results show that UX can help identify issues with compliance, and suggest more workable alternatives.

Acknowledgments

This research was supported by the 2018-2019 Information Commissioner's Office's (ICO) Grants Programme. The authors would like to thank Elie Tom, Martin J. Kraemer, and the anonymous SOUPS reviewers for their valuable input. George Chalhoub is funded by Fondation Sesam. 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] Junia Valente, Matthew A. Wyn, and Alvaro A. Cardenas. Stealing, Spying, and Abusing: Consequences of Attacks on Internet of Things Devices. *IEEE Security & Privacy*, 17(5):10–21, 2019.

[2] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. *ArXiv*, 2017.

[3] Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach. In *Proceedings of the Internet Measurement Conference*, pages 267–279, New York, New York, United States, 2019.

[4] Tribune Media Wire. Couple 'Felt So Violated' After Hacker Took Over Smart Home Devices, Began Talking to Them. `https://wtkr.com/2019/09/23/felt-so-violated-couple-scared-after-hacker-targets-homes-smart-devices/`, September 2019.

[5] Joseph Cox and Samantha Cole. How Hackers Are Breaking Into Ring Cameras. `https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras`, December 2019.

[6] Kashmir Hill and Surya Mattu. The House That Spied on Me. `https://gizmodo.com/the-house-that-spied-on-me-1822429852`, 2018.

[7] Marc Hassenzahl and Noam Tractinsky. User experience — a research agenda. *Behaviour & Information Technology*, 25(2):91–97, 2006.

[8] Claire Rowland, Elizabeth Goodman, Martin Charlier, Ann Light, and Alfred Lui. *Designing Connected Products : UX for the Consumer Internet of Things*. O'Reilly Media, Inc., Sebastopol, California, 2015.

[9] Jong-bum Woo and Youn-kyung Lim. User Experience in Do-It-Yourself-Style Smart Homes. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing(UbiComp 2015)*, pages 779–790, New York, NY, United States, 2015.

[10] Gregory D. Abowd and Elizabeth D. Mynatt. *Designing for the Human Experience in Smart Environments*, chapter 7, pages 151–174. 2005.

[11] John McCarthy and Peter Wright. *Technology as Experience*. MIT Press, Cambridge, Mass, 2007.

[12] Andreas Jacobsson and Paul Davidsson. Towards a Model of Privacy and Security for Smart Homes. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT 2015)*, pages 727–732, 2015.

[13] Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops 2017)*, pages 618–623, United States, 2017.

[14] Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security & Privacy Concerns with Smart Homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, 2017.

[15] Johanna Bergman, Thomas Olsson, Isabelle Johansson, and Kirsten Rassmus-Gröhn. An Exploratory Study on How Internet of Things Developing Companies Handle User Experience Requirements. In *Requirements Engineering: Foundation for Software Quality*, volume 10753 LNCS, pages 20–36, Germany, 2018.

[16] Jeungmin Oh and Uichin Lee. Exploring UX Issues in Quantified Self Technologies. In *2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking (ICMU 2015)*, pages 53–59, 2015.

[17] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating Receptiveness to Sensing and Inference in the Home Using Sensor Proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp 2012)*, pages 61–70, New York, NY, USA, 2012.

[18] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. Benefits and Risks of Smart Home Technologies. *Energy Policy*, 103:72–83, 2017.

[19] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. Smart Homes and Their Users: A Systematic Analysis and Key Challenges. *Personal and Ubiquitous Computing*, 19(2):463–476, 2014.

[20] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, pages 181–18109. IEEE, 2017.

[21] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies*, 2019(4):250–271, 2019.

[22] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "What Can't Data Be Used For?": Privacy Expectations about Smart TVs in the U.S. In *European Workshop on Usable Security (EuroUSEC 2018)*, 2018.

[23] Christine Geeng and Franziska Roesner. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI 2019)*, pages 1–13, 2019.

[24] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants . In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 451–466, USA, 2019.

[25] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy Expectations and Preferences in an IoT World. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, Santa Clara, CA, 2017.

[26] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2), 2018.

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

[28] Julia Bernd, Alisa Frik, Maritza L. Johnson, and Nathan Malkin. Smart Home Bystanders: Further Complexifying a Complex Context. In *Proceedings of the 2nd Symposium on Applications of Contextual Integrity*, 2019.

[29] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. Understanding the Experience-Centeredness of Privacy and Security Technologies. In *Proceedings of the 2014 workshop on New Security Paradigms Workshop (NSPW 2014)*, pages 83–94, 2014.

[30] Fungai Bhunu Shava and Darelle Van Greunen. Factors Affecting User Experience with Security Features: A Case Study of an Academic Institution in Namibia. In *2013 Information Security for South Africa*, pages 1–8. IEEE, 2013.

[31] Niels Raabjerg Mathiasen and Susanne Bødker. Threats or Threads - From Usable Security to Secure Experience? In *Proceedings of the 5th Nordic cConference on Human-Computer Interaction: Building Bridges*, volume 358, pages 283–289. ACM International Conference Proceeding Series, 2008.

[32] Panagiotis Zagouras, Christos Kalloniatis, and Stefanos Gritzalis. Managing User Experience: Usability and Security in a New Era of Software Supremacy. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 174–188, 2017.

[33] Norbert Nthala and Ivan Flechais. Informal Support Networks: An Investigation Into Home Data Security Practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 63–82, Baltimore, MD, 2018.

[34] Eric Zeng and Franziska Roesner. 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)*, pages 159–176, Santa Clara, CA, 2019.

[35] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User Perceptions of Smart Home IoT Privacy. In *Proceedings of the ACM on Human-Computer Interaction*, number 2 in CSCW, 2018.

[36] Noah Apthorpe, Dillon Reisman, and Nick Feamster. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. *ArXiv*, 2017.

[37] George Chalhoub. The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA 2020)*, page 1–6, New York, New York, United States, 2020.

[38] Noura Aleisa and Karen Renaud. Privacy of the Internet of Things: A Systematic Literature Review. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, pages 5947–5956, 2017.

[39] Kai Zhao and Lina Ge. A Survey on the Internet of Things Security. In *2013 Ninth International Conference on Computational Intelligence and Security*, pages 663–667, 2013.

[40] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA 2020)*, page 1–9, 2020.

[41] George Chalhoub and Ivan Flechais. "Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users. In *Human Aspects of Information Security, Privacy and Trust*, Cham, 2020.

[42] Johanna Bergman and Isabelle Johansson. The User Experience Perspective of Internet of Things Development. Master's thesis, Certec, Department of Design Sciences, LUND University, Lund, Sweden, 2017.

[43] Hala Assal and Sonia Chiasson. Security in the Software Development Lifecycle. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* , pages 281–296, 2018.

[44] Ari Ezra Waldman. Designing Without Privacy. *Houston Law Review*, 55(659):659, 2017. Available at SSRN: `https://ssrn.com/abstract=2944185`.

[45] Tayyaba Nafees, Natalie Coull, Robert Ian Ferguson, and Adam Sampson. Idea-caution Before Exploitation: The Use of Cybersecurity Domain Knowledge to Educate Software Engineers Against Software Vulnerabilities. In *Engineering Secure Software and Systems*, pages 133–142, 2017.

[46] Tayyaba Nafees, Natalie Coull, Ian Ferguson, and Adam Sampson. Vulnerability Anti-patterns: A Timeless Way to Capture Poor Software Practices (Vulnerabilities). In *Proceedings of the 24th Conference on Pattern Languages of Programs (PLoP2017)*, United States, 2018.

[47] Tyler W. Thomas, Madiha Tabassum, Bill Chu, and Heather Lipford. Security During Application Development: An Application Security Expert Perspective. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI 2018)*, pages 1–12.

[48] Claire Rowland. UX and Service Design for Connected Products. `https://iotuk.org.uk/wp-content/uploads/2018/06/UX-and-Service-Design-IoTUK.pdf`, June 2018.

[49] Michael Onuoha Thomas, Beverly Amunga Onyimbo, and Rajasvaran Logeswaran. Usability Evaluation Criteria for Internet of Things. *International Journal of Information Technology and Computer Science*, 8(12):10–18, 2016.

[50] Jonathan Follett. *Designing for Emerging Technologies : UX for Genomics, Robotics, and the Internet of Things*. O'Reilly Media, Inc., Sebastopol, CA, 2014.

[51] Ali Asghar Nazari Shirehjini and Azin Semsar. Human Interaction with IoT-Based Smart Environments. *Multimedia Tools and Applications*, 76(11):13343–13365, 2017.

[52] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: A Survey. *Computer Networks*, 54(15):2787–2805, 2010.

[53] Timo Jokela. Assessments of Usability Engineering Processes: Experiences from Experiments. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS '03) - Track 9 - Volume 9*, HICSS '03, page 328, USA, 2003.

[54] Rosa Yáñez Gómez, Daniel Cascado Caballero, and José-Luis Sevillano. Heuristic Evaluation on Mobile Interfaces: A New Checklist. *The Scientific World Journal*, 2014:1–19, 2014.

[55] Sharan B. Merriam. *Case Study Research in Education: A Qualitative Approach*. San Francisco, 1988.

[56] Sharan B. Merriam. *Qualitative Research and Case Study Applications in Education*. Jossey-Bass Publishers, San Francisco, 1998.

[57] Dennis Basil Bromley and Dennis Basil Bromley. *The Case-study Method in Psychology and Related Disciplines*. Wiley Chichester, 1986.

[58] Jack Narcotta and William Ablondi. Smart Home Surveillance Camera Market Analysis and Forecast. *Strategy Analytics*, 2018.

[59] Matt Burgess. The IoT's Security Nightmare Will Never End. You Can Now Search Insecure Cameras by Address. `https://www.wired.co.uk/article/internet-of-things-security-camera-search-location`, November 2018.

[60] Kambiz Ghazinour and Emil Shirima. Privacy for Security Monitoring Systems. *USENIX Symposium on Usable Privacy and Security (SOUPS 2018)*, 2018.

[61] Anuroop Gaddam, Subhas Chandra Mukhopadhyay, and Gourab Sen Gupta. Trial & Experimentation of a Smart Home Monitoring System for Elderly. In *2011 IEEE International Instrumentation and Measurement Technology Conference*, pages 1–6. IEEE, 2011.

[62] Jasper van Kuijk, Heimrich Kanis, Henri Christiaans, and Daan van Eijk. Barriers to and Enablers of Usability in Electronic Consumer Product Development: A

Multiple Case Study. *Human-Computer Interaction*, 32(1):1–71, 2017.

[63] Charles F. Cannell, Peter V. Miller, and Lois Oksenberg. Research on Interviewing Techniques. *Sociological Methodology*, 12:389–437, 1981.

[64] Anselm Strauss and Juliet M. Corbin. *Grounded Theory in Practice*. SAGE Publications, Thousand Oaks, California, 1997.

[65] Anselm Strauss. *Basics of qualitative research : techniques and procedures for developing grounded theory*. SAGE Publications, Thousand Oaks, California, 1998.

[66] Clive Seale. Quality in Qualitative Research. *Qualitative Inquiry*, 5(4):465–478, 1999.

[67] Juliet Corbin and Anselm Strauss. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, Inc., 2014.

[68] Greg Guest, Arwen Bunce, and Laura Johnson. How Many Interviews are Enough? An experiment with data saturation and variability. *Field Methods*, 18(1):59–82, 2006.

[69] Marry L. McHugh. Interrater Reliability: the Kappa Statistic. *Biochemia Medica*, pages 276–282, 2012.

[70] Victor Jupp, editor. *The SAGE Dictionary of Social Research Methods*. SAGE Publications, London Thousand Oaks, Calif, 2006.

[71] Kathy Charmaz. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. Constructing grounded theory. SAGE Publications, 2006.

[72] Nayan B. Ruparelia. Software Development Lifecycle Models. *ACM SIGSOFT Software Engineering Notes*, 35(3):8–13, 2010.

[73] Lassi A. Liikkanen, Harri Kilpiö, Lauri Svan, and Miko Hiltunen. Lean UX: The Next Generation of User-Centered Agile Development? In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational (NordiCHI 2014)*, pages 1095–1100, 2014.

[74] Paul Voigt and Axel Von dem Bussche. *The EU General Data Protection Regulation (GDPR) : A Practical Guide*. Cham, Switzerland, 1 edition, 2017.

[75] Lee A. Bygrave. Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements. *Oslo Law Review*, 1(02):105–120, 2017.

[76] Information Commissioner Office. Data Protection by Design and Default. `https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/`, August 2019.

[77] Mary Ellen Zurko. User-Centered Security: Stepping Up to the Grand Challenge. In *Proceedings of the 21st Annual Computer Security Applications Conference*, ACSAC '05, pages 187–202, USA, 2005.

[78] Marcia Ford and William Palmer. Alexa, are you listening to me? An analysis of Alexa voice service network traffic. *Personal and Ubiquitous Computing*, 23(1):67–79, 2019.

[79] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. IoT Security: Ongoing Challenges and Research Opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pages 230–234. IEEE, 2014.

[80] Teng Xu, James B. Wendt, and Miodrag Potkonjak. Security of IoT Systems: Design Challenges and Opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2014)*, pages 417–423. IEEE Press, 2014.

[81] Xiaocheng Ge, Richard F. Paige, Fiona Polack, and Phil Brooke. Extreme Programming Security Practices. In *Agile Processes in Software Engineering and Extreme Programming*, pages 226–230, Berlin, Heidelberg, 2007.

[82] James Stewart. Why 'Security Says No' Won't Cut it Anymore - Technology in Government. `https://technology.blog.gov.uk/2016/07/13/why-security-says-no-wont-cut-it-anymore/`, July 2016.

[83] Steffen Bartsch. Practitioners' Perspectives on Security in Agile Development. In *Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security (ARES 2011)*, pages 479–484, United States, 2011.

[84] Seda Gürses, Carmela Troncoso, and Claudia Diaz. Engineering Privacy by Design Reloaded. In *Amsterdam Privacy Conference*, pages 1–21, 2015.

[85] Ivan Flechais, M. Angela Sasse, and Stephen M. V. Hailes. Bringing Security Home: A Process for Developing Secure and Usable Systems. In *Proceedings of the 2003 Workshop on New Security Paradigms (NSPW 2003)*, pages 49–57, New York, United States, 2003.

A Screening Questionnaire

1. Select your gender:
   - ◯ Male
   - ◯ Female
   - ◯ Other
   - ◯ Prefer not to answer
2. Select your age group:
   - ◯ 18-24
   - ◯ 25-34
   - ◯ 35-44
   - ◯ 45-54
   - ◯ 55-64
   - ◯ 65-74
   - ◯ 75 or older
   - ◯ Prefer not to answer
3. What best describes your job at the company?
   - ◯ UI Designer
   - ◯ UX Designer
   - ◯ UX Director
   - ◯ Interaction Designer
   - ◯ Sales Manager
   - ◯ Software Developer
   - ◯ Security Officer
   - ◯ Legal Officer
   - ◯ Hardware Designer
   - ◯ Hardware Engineer
   - ◯ Product Manager
   - ◯ Other:
4. How long have you been working at your company?
   - ◯ No Experience
   - ◯ Less than 1 year
   - ◯ More than 1 year and less than 3 years
   - ◯ More than 3 years and less than 5 years
   - ◯ More than 5 years and less than 7 years
   - ◯ More than 7 years
5. What best describes your company?
   - ◯ Consultant Company
   - ◯ Product Company
   - ◯ Service Company
   - ◯ Platform Company
   - ◯ Other:
6. Select the smart-home product category (or categories) that your company deals with:
   - ☐ Phone Systems
   - ☐ Smart Lights and Dimmers
   - ☐ Temperature and Climate Control Systems
   - ☐ Security Access Control Systems
   - ☐ Other:
7. Select the type of device(s) that your company deals with:
   - ☐ Cameras
   - ☐ Door Locks
   - ☐ Home Theaters
   - ☐ Hubs
   - ☐ Voice Assistants
   - ☐ Leak Detectors
   - ☐ Lights
   - ☐ Motion Sensors
   - ☐ Power Outlets and Switches
   - ☐ Smoke Detectors
   - ☐ Thermostats
   - ☐ Other:
8. How many employees does your company have?
   - ◯ less than 25
   - ◯ 26-50
   - ◯ 51-100
   - ◯ 101-250
   - ◯ 251-500
   - ◯ 501-1000
   - ◯ More than 1000

B Pilot Interview Questions

1. What company do you work for? What does the company do? What is your role in the company?
2. Can you describe your product design process?
3. Do you consider UX when designing security and privacy solutions for your smart home products? If so, how?
4. What are the typical challenges that you face when designing smart home products? Are there any challenges specific to factoring UX into security and privacy design?
5. Is there anything in the design process that could help address user-centered security and privacy challenges in smart homes? If so, please elaborate.

C Main Interview Questions

Our interviews were semi-structured. We below describe our study script (divided into several sections). The last four sections describe specific questions that we asked to employees who had different responsibilities.

C.1 Characterizations

1. Would you tell us about your role in the company that you work at?
   (a) When did you join the company?
   (b) What are your responsibilities?
   (c) What is your specific role in the development or design process of smart home devices?
2. Would you tell us about the products that you develop?
   (a) Is there a specific product that you focus on developing?
3. Would you tell us about your users (or customers)?
   (a) How would you describe the typical customers that use your products?

C.2 Introductory Questions

1. How would you describe User Experience (UX)?
   (a) What UX characteristics do you regard as important?
   (b) What do you think the role of security/privacy in UX is?
2. Do you think there is a relation between UX and security/privacy?
   (a) (if yes) Could you describe this relation?
   (b) (if no) Could you explain why not?

C.3 Requirements Gathering and Specification

1. How do you identify or specify the requirements of a smart home camera before you design it?
   (a) What kind of requirements do you consider?
   (b) How do you prioritize requirements?
2. Do you handle any security/privacy requirements during the requirements gathering or specification process?
   (a) (if yes) How do you handle these requirements?
   (b) (if yes) Do you consider UX when addressing security or privacy requirements in the design process?
   (c) (if no) What do you think of designers who do so?

C.4 UX Design Process

1. Do you consider UX to be an important factor in the design process of smart home devices?
   (a) Where in the design process do you apply UX techniques?
   (b) Is there a specific UX team or role in a specific department?
   (c) How are decisions made when it comes to UX?
   (d) Do you factor UX into the security and privacy design of smart home cameras? If so, could you give us more details?
2. Does security or privacy play a role in the UX development process that you take part of?
   (a) (if yes) Could you explain the role?
   (b) (if no) What type of effect would it have if it did?
3. Do you collect user data for UX development?
   (a) (if yes) What type of user data do you collect? How do you collect it?
   (b) (if yes) What sort of data-driven methods do you use?
   (c) (if yes) Have you ever handled UX requirements within the context of security and privacy? Can you give us more details?
4. Do you have a UX requirements gathering process?
   (a) (if yes) Could you give us more details?
5. What design processes—including methods, techniques (e.g., storyboards), and artifacts (e.g., personas)—do you use in the context of data protection?
6. Regardless of whether you have a UX requirements gathering process, what do you think the best design practices are (e.g., programming patterns, artifacts)?

C.5 End-user Involvement

1. Do you engage end-users in the development of smart camera products or features?
2. (if yes) How do you involve end-users in the design phase?
   (a) To which extent do you involve end-users?
   (b) Do you consider data security or user privacy during the process? Why/Why not?
   (c) Does the type of product influence whether end-users can be involved? What about security or privacy risks?
3. (if no) What are your thoughts on involving end-users in the design of smart home cameras?

C.6 Ecosystem Considerations

1. Is your product part of an ecosystem of products used in smart home environments?
2. (if yes) Have you faced any obstacles when considering the ecosystem?
    (a) (if yes) What were they? Could you describe the main obstacles? How did you deal with them?
3. (if security/privacy was mentioned) Can you describe how do you deal with security and privacy?
4. (if security/privacy was not mentioned) What do you think of the role of security and privacy in a smart home ecosystem?

C.7 UX Challenges

1. What were the UX challenges that you faced during the design of smart cameras?
    (a) How did you overcome those challenges?
    (b) Were there any challenges without any solutions in sight?
2. (if security/privacy was mentioned) Could you give us more details of the security or privacy challenges?
    (a) How did you address those challenges?
3. (if security/privacy was not mentioned) Smart homes are associated with security/privacy threats. Have you ever experienced challenges specific to UX during the security/privacy design process of smart cameras?
    (a) (if yes) Could you describe the challenges you faced, and how did you address them?
    (b) (if no) What do you think of the role(s) of security/privacy and UX in smart home environments?

C.8 Security Stakeholder Questions

1. Can you tell us how security is taken into consideration at your company?
2. How do you ensure that your product is secure? Is there a process? How does it look like?
3. How do you identify security requirements?
4. Do you work/communicate with the design team? Do you get involved in the security and privacy design of smart cameras?
5. In general, who is responsible for designing the security/privacy features of smart cameras?
6. How do you update the firmware of smart cameras that you sell? Who is responsible for this task?
7. How often does security need to be maintained?
8. If a security breach happens in the physical products sold to clients, who will take responsibility?
9. If your company suffers from a data breach, how will you address this? Do you notify users?
10. How do you make sure that users who use your products are protected when it comes to breaches?

C.9 Regulatory Stakeholder Questions

1. Who deals with GDPR and Product Liability?
2. Do you deal with legislation?
3. How is data protection represented in your organization?
4. Do you interact with any regulatory bodies (e.g., ICO) when it comes to matters of data protection?
    (a) (if yes) What are these matters?
    (b) (if no) Do you think it would be useful to do so?

C.10 Management Stakeholder Questions

1. Are there any restrictions (e.g., legal, security, privacy) that make it harder for you to use customer data for product design or making decisions?
2. What data protection roles/responsibilities are there for:
    (a) Product management (and data management)?
    (b) Product design and development?
    (c) UX, usability, and experience-centered jobs?
    (d) Marketing and sales?
3. What does privacy mean in terms of your products?
4. How do you design for data protection when devices are shared among multiple users?

C.11 Concluding Remarks

1. Do you think there is anything in the design/development process that makes it easier to address user-centered security and privacy challenges in cameras?
2. We have reached the end of the interview. Thank you for talking to us!
    (a) Do you have any questions?
    (b) Do you have any comments you want to add?

D Codebook

Development	Stakeholder Limitations	Internal Security Audits	Obtaining Consent
AB Testing	Stakeholder Responsibilities	Low-Priority Security	Opt-Out Services
Acceptability	Storyboarding	No One's Responsibility	Privacy by Design
Agile Development	Surveys	No Sight of Security Requirements	Privacy Mode
Agile Sprint Reviews	Technical Requirements	Reactive Security	Privacy Requirements
Agile User Stories	Tensions Between Stakeholders	Security by Design	Privacy Settings
Analyzing Requirements	The Complexity of Smart Home Devices	Security Maintenance	Privacy Threats
Company Policies	Time Constraints	Security Mode	Privacy Vulnerabilities
Conceptual Sketches	Usability Testing	Security not Factored into Design	Putting Users in Control
Conflicts Between Stakeholders	Usefulness	Security Practices	Security Management Frameworks
Convenience Aspects	User Cases	Security Requirements	Subjective Awareness of Privacy
Cost Constraints	User Frustration	Security Settings	Transparency
Design Process	User Integrity	Security Threats	UX in Privacy Requirements
Development Process	User Interviews	Security Vulnerabilities	UX of Consent
Development Teams	User Involvement in Design	Subjective Awareness of Security	UX of Privacy
Diffusion of Responsibilities	User Observation	Subjective Security Decisions	Withdrawing Consent
End-User Incompetence	User Personas	Technical-Only Security	**Innovation**
End-User Tests	User Research	Understanding User Behavior	Best Practices
Focus Group Interviews	User Respect	Usable Security	Common Practices
Functional Requirements	Utility	Usable Security Experts	Designing New Devices
GDPR Vagueness	UX Best Practices	UX in Security Requirements	Designing New Features
Hardware Design	UX Challenges	Vulnerability Reporting Programs	Designing New Solutions
Heterogeneous Devices	UX Departments	**Privacy**	Lack of Innovation
Indirect User Feedback	UX Design Process	Collecting/Processing Data (GDPR)	Novel Security Uncertainty
Industrial Design	UX Guidelines	Creepiness	Privacy Innovation
Interoperability	UX Pain Points	Creepiness-Convenience Trade-off	Security Innovation
Legal Compliance	UX Policies	Data Protection by Design	Security Uncertainty
Less Time for Hardware Design	UX Requirements Gathering	Data Protection Practices	Tried-And-Tested Security
No Flexibility to Upgrade Hardware	UX Research	Data Protection Requirements	**Trust**
Non-Functional Requirements	UX Roles	Data Protection Responsibilities	Culture of Trust
Not Enough Hardware Sprints	**Security**	Data Protection Roles	Data Breach Response Plan
Product Liabilities	Ad-hoc Security	End-User Compliance	Experience of Harm
Project Constraints	Afterthought Security	Explicit Consent	Incident Response Plan
Requirements Gathering	Awareness Based on Outside Sources	GDPR Consent	Increasing Trust
Requirements Specification	Awareness Based on Social Influences	GDPR Impracticality	Informing Users of Their Rights
Scope Constraints	Encryption Between Devices	GDPR Delayed Effect	Motivation for Privacy
Stakeholder Authority	Evidence-Based Security Decisions	Handling Sensitive Data	Motivation for Security
Stakeholder Characteristics	External Security Audits	Help Pages and FAQs	Motivation for Trust
Stakeholder Communication	Fit-and-Forget Security	Making Devices not Creepy	Preserving Trust
Stakeholder Knowledge	Incidents	No Sight of Privacy Requirements	Trust Relationship

Table 4: Codebook (Grounded Theory).