Chapter

How Is the Internet of Things Industry Responding to the Cybersecurity Challenges of the Smart Home?

Sara Cannizzaro and Rob Procter

Abstract

In this article, we investigate the privacy and security challenges of the smart home as perceived by the industry, with findings relating to cybersecurity awareness, transparency on legal data use, malicious data use, regulation issues, liability, and market incentives for cybersecurity; we also reveal how the industry has been responding to these challenges. Based on survey findings, we outlined a series of socio-technical challenges to smart home adoption. To understand these findings in more depth, we investigated qualitatively how these challenges were perceived and responded to by organizations in the Internet of Things (IoT) sector. We interviewed seven experts from six organizations involved in the design, development, or review of consumer IoT devices and services including both businesses and NGOs. Thematic analysis focused on two main themes, that is, responses to privacy and responses to security challenges of smart home adoption. Our study revealed that industry stakeholders are looking to address these adoption challenges by providing new technical solutions to mitigate the privacy and security risk of the smart home, producing new standards and influencing regulation, as well as building up communities of learning surrounding common issues. With this knowledge, industry stakeholders can take steps toward increasing smart home acceptability for consumers.

Keywords: IoT, smart home, industry stakeholder, acceptability, adoption, thematic analysis, privacy, security

1. Introduction

Smart home technologies are marketed to enhance consumers' home life. The "smart home" can be defined as the integration of the Internet of Things (IoT, i.e., Internet-enabled, digital devices with sensors) and machine learning in domestic environments. The aim of smart home technologies is to provide enhanced entertainment services, easier management of the home, domestic chores, and protection from domestic risks. They can be found in devices such as smart speakers and hubs, lighting, sensors, door locks and cameras, central heating thermostats, and domestic appliances. The European market for smart home devices is expected to boom in the next 5 years [1], but amid such positive expectations, there looms the productivity paradox identified by scholars of social informatics—that technology alone, even good technology, is not sufficient to create social or economic value and strategies of computerization do not readily produce expected economic and social benefits in a vast number of cases [2].

Currently, businesses are actively promoting positive visions of what the smart home means for consumers (e.g., convenience, economy, and home security). However, at the same time, consumers are actively comparing their smart home experiences against these visions and some are coming up with different interpretations and meanings from those that business is promoting [3, 4]. Hence, if the expected growth of the smart home market is to be realized, it is important for smart home device manufacturers and service providers to understand consumer reactions and thereby reduce the chance that the technology may not be valuable or meaningful to consumers.

Previous studies have found that UK consumers are not convinced that they can trust the privacy and security of smart home technologies [3, 5]. Cannizzaro et al. [3] predicted that the potential for security incidents happening through smart home devices would be a significant obstacle to smart home adoption. They also showed that consumers are unconvinced that their privacy will not be at risk. Consumers' perceived risk of using the Eco-friendly smart home (ESHM) reduces their intention to adopt IT [6]. This means that there are issues with the acceptability of smart home technologies; hence, it is highly likely that privacy and security concerns will impact negatively on their future adoption [7]. Proof of robust cybersecurity and low risk of privacy breaches will be key in smart home technology companies persuading consumers to invest in their products. Businesses and policymakers need to work together in order to increase consumers' trust [3] and ensure consumers' safety and well-being while using these devices. However, the smart home business community is not likely to act speedily to address consumers' concerns without a strong regulatory incentive. However, other incentives for businesses, other than regulation, would clearly include the reputation of having products that do not violate users' privacy. At the same time, some argue that the rapid pace of IoT development militates against effective policy interventions [8]. The UK government has produced the Code of Practice for Consumer Internet of Things Security [9] with 13 voluntary recommendations, but debate is currently open as to whether to enforce some of these on the UK market [10].

When it comes to understanding the implications of issues, such as the privacy and security risks of smart home devices, it is important to consider the views of a full range of stakeholders [11]. In this article, we report the findings of our IoT industry stakeholder study, which was conducted as part of the Petras research programme, the UK's Research Hub for IoT[1]. In addition to representing the voices of consumers, we sought to discover the opinions of industry stakeholders (such as small and large businesses), as well as NGOs (including community and IoT interest groups), to understand how these stakeholders influence the smart home development in the UK and respond to the challenges that have been reported. Our aim is to enrich our understanding of the socio-technical context in which the technology is being promoted. We argue that this can help businesses to harness the economic opportunities of the smart home, while increasing the technology's acceptability for consumers.

[1] https://petras-iot.org/.

2. Literature review

2.1 Technology adoption and acceptability

Social informatics studies the relationships between people, digital technologies, and their contexts of use [12]. In this approach, the focus is on the relationship between technology and society from a perspective that does not privilege either [2] but examines, as they put it, the hyphen in the "socio-technical" expression. Adoption studies can be a practical application of social informatics approaches because, to be able to study and promote adoption, an understanding of the possibilities harnessed by the materiality of the technology—as well as the value that the technology brings into people's lives—is necessary. It is an approach that contrasts with an *a priori* promotion of technologies that occasionally work well for people, occasionally are valuable, are sometimes abandoned, are sometimes unusable, and thus incur predictable waste and inspire misplaced hopes [13].

Adoption is a process "starting with the user becoming aware of the technology, and ending with the user embracing the technology and making full use of it" [14]. Awareness has been seen as the key to developing new ICT infrastructures [15] and as a key determinant of consumers' adoption behavior [16]. Lack of awareness was identified as an obstacle to mobile phone adoption [17] and in the IoT landscape, our survey showed that the less aware people are of the expression "Internet of Things," the higher the odds (1.3 times) that they will not want to use the technology in the future [3]. Furthermore, security and privacy can influence the adoption of smart home technologies. For example, in their investigation of trust in the cybersecurity-preserving capabilities of smart home devices, Cannizzaro et al. [3] revealed how anxiety about the likelihood of a security incident in IoT for the home, emerged as a statistically significant factor influencing the adoption of smart home technology. Lipford et al. [18] outlined how IoT technologies introduce challenging privacy issues that may frustrate their widespread adoption, whereas Guhr et al. [19] emphasize how privacy concerns directly and indirectly influence the intended smart home usage.

Adoption studies are typically carried out by what Rogers [20] calls "change agencies," whose short-term goal is to facilitate the adoption of innovations and who often follow a segmentation strategy of least resistance to innovations. This logic of pursuing economic gain and sidelining wider societal interests also appears in recent key IoT adoption studies (e.g., [21–24]), which justify adoption purely through economic arguments and do not mention the societal risks that the technology may raise. The underlying economic model of the new wave of digital innovations has been dubbed "surveillance capitalism" [24], defined by the harvesting of data and its analysis for the commodification of human activity. In response, Helbing [25] states that we must ensure the ethical use of new digital technologies. Hence, acceptability is a way to mitigate this one-sided approach to adoption and can help to understand the impact of unintended consequences, for example, the erosion trust in technology, privacy [12], or the rate of acceptance of the smart home in older adults [6, 26] Technology acceptability is "the degree of primary users' predisposition to carry out daily activities using the intended device" [27]. Philosophically, technology acceptability is a judgment that prescribes the way in which the technology examined ought to be desirable [28]. Acceptability is a popular perspective in health and assistive technology-related IoT services and products, where, for example, Shahrestani [29] defines acceptability as "guidelines to evaluate how a particular approach or technology is working for the elderly or people with disability," thus relating acceptability to the general process of *evaluation*. In regard to the IoT, Taylor et al. [30] define acceptability in conjunction with "attitudes," for example, "Policymakers need to investigate the *attitudes* of the public if *acceptability* of IoT is to be understood" ([30], emphasis added). Hence, "acceptability" feeds on evaluations, predispositions, and attitudes toward a given technology, foregrounding the user in the user-technology relation. As such, acceptability has the potential to give consumers a voice and thus rebalance the business-consumer relationship. The socio-technical approach intrinsic in acceptability can encourage a discovery process that helps designers effectively understand the relevant life worlds and work worlds of the people who will use their systems [2].

Outside of academia, acceptability-related studies are rather popular and are often carried out by interest groups [31, 32] or organizations defending consumers' rights (e.g., [5]). Trust is fundamental to consumer technology where the transmission of personal and sensitive information is involved.

De Poel and Verbeek note how science and technology scholars have shied away from explicit normative or ethical discussions [33], but with the advent of the IoT, and the smart home being marketed to the wider population, ignoring technology ethical-acceptability concerns and disregarding consumer trust is no longer possible.

Trust in privacy and security are key factors affecting the acceptability of the smart home [3, 34]. To date, there have been few nontechnical studies of security and privacy concerns of smart home device users [35].

3. Methodology

3.1 Interviews as survey follow-up

In previous work [3], we confirmed one of the social informatics' key lessons, that is, the effects of technology are always unequal, in other words, "that some social groups will benefit more than others from the uses of digital technologies" [12]. We also found that the privacy and security-preserving capability of devices are the most significant challenges to smart home adoption. Hence, we further investigated how organizations in the sector perceive and respond to these challenges. This study involving Human Subject Research received full approval by the University of Warwick ethics committee on May 29, 2019 (ref. no BSREC 51/18-19). The methodology consisted of a series of semi-structured interviews: seven experts from six organizations involved in the design, development, or review of smart home devices and services (**Table 1**)[2]. We adopted a semi-structured interview format as this is more likely to ensure that valid and reliable data can be obtained from interviewees [36]. Also, semi-structured interviews provide respondents with enough flexibility to build and expand on the initial guiding topic, which, in turn, allows the researcher to analyze the dataset with different degrees of depth.

In order to achieve a balance of views, a broadly equal proportion of business and nonbusiness organizations were included in the sample with four experts from NGOs and three experts from businesses. Respondents from interviews [2, 3, 7] are business respondents, whereas those from interviews [4, 5, 8] are NGO respondents. Interview [5] includes two NGO experts from the same organization (see **Table 1**).

[2] Ethical approval for the study was secured from the Biomedical and Scientific Research Ethics Committee (BSREC) at the University of Warwick on 29 May 2019.

	Organization type	**Location**	**Type of IoT product/ approach developed**	**Target represented**	**Respondent role within the organization**
Interview (ref. 1)	Business	UK	Telecommunication products		Innovation consultant
Interview (ref. 2)	Business	UK	Developing innovative solutions, advisory, and management activities		CEO
Interview (ref. 3)	NGO	UK	Social purpose corporation	Consumers	Advisor
Interview (ref. 4)	NGO	Worldwide	Online community	Smart home industry business leaders	Co-founder
Interview (ref. 4)	NGO	Worldwide	Online community	Smart home industry business leaders	Chief operations officer
Interview (ref. 5)	Business	Germany (UK office)	Auditing, testing services, and product certification		Business development manager
Interview (ref. 6)	NGO	Worldwide (UK office)	Consumer group	Consumers	Digital advocacy manager

Table 1.
Details of sample composition consisting of business (product provided and respondent role) and NGO (target represented and respondent role) organizations.

We sought to include policy-side views on the security threats in smart home adoption. The majority of our respondents were from large organizations but we sought to include at least one small business among them.

The sample of interviewees arrived through suggestions made by Petras project colleagues. Interviews were conducted face-to-face and by video conference call and lasted between 30 min and 1 h.

To ensure rigorous data collection, we followed the guidelines set by Braun and Clarke [37] concerning planning thematic analysis. Hence, in devising the interview questions, we first clarified the scientific method upon which the analysis would rest and opted for a broadly deductive approach, constrained by the survey findings and adoption challenges of the smart home identified in Cannizzaro et al. [3] and listed below:

i. Overall, fairly low levels of trust.

ii. Overall, levels of satisfaction are still uncertain despite the prolonged presence of IoT in society.

iii. Younger respondents' low-risk awareness.

iv. Older respondents' resistance to IoT.

v. Less-educated respondents' resistance to IoT.

Our questionnaire was developed based on these challenges that allowed us to formulate a question guide. Each question topic was formed of guiding questions as well as some follow-up questions [38] (see Appendix A). The interviews were transcribed and a thematic analysis via coding was conducted on the transcripts. The thematic analysis was based on Braun and Clarke's [37] principle of *realism*. These questions were rotated according to the background of the respondents, particularly whether they were businesses or NGO organizations. Topics forming the questions guide included general background questions to allow participants to respond to questions about their roles within the organization and break the ice; followed by the topics pertaining to the most significant factors affecting IoT adoption, as previously explored quantitatively in [3, 39], such as IoT and smart home *awareness*, *risks and benefits* of IoT for both organizations and consumers, *trust, digital* divide in IoT adoption, *future and change* in the sector, including *responses to IoT challenges* (see Appendix A). The interviews were transcribed and a thematic analysis via coding (based on the topics above) was conducted on the transcripts. In order to reach the saturation point, we then examined the transcripts further using Social Construction of Technology (SCOT), a mid-ground theoretical framework, which is outlined below.

3.2 Theoretical framework: SCOT's interpretive flexibility

Within innovation studies, approaches to understanding meanings range from technological determinist (e.g., [40]) to social constructivist (e.g., [41]). Occupying a conceptual middle ground is the SCOT framework [42]. In SCOT, a key concept is "interpretive flexibility" [43], which recognizes that the "meaning" of an innovation may be initially contested by different stakeholders or social groups before "closure"—and hence its use-value—is reached [44]. According to Orlikowski [43], interpretive flexibility is an attribute of the relationship between people and technology, a function of the material artifact, the characteristics of the human agents, and the institutional context in which technology is being introduced [45]. The social groups involved in interpreting the meanings of the technology include producers, engineers, designers, marketers, and investors; those who have a direct relationship with technology and develop an artifact—advocates—policymakers, lobbyists, and academics; those who are indirectly related with technology and work on policymaking, lobbying, and research; and also, users and bystanders [46]. Elle et al. [47] contend that, in most cases, interpretive flexibility diminishes when the social groups reach an agreement on an interpretation.

Initially, SCOT perspectives originated in studies of organizational innovation processes. Unsurprisingly, Rowland [48] argues that SCOT emphasizes the role of large business corporations, whereas Burns et al. [49] see innovation within a context of receptivity and institutionalization. However, some argue that in the current context where digital innovation is a largely available consumer commodity, SCOT needs to be translated to the consumer digital technology marketplace, and hence it requires a new framework variant, Social Construction of Digital Technologies (SCODT). The SCODT framework posits that dimensions of innovation ought to be considered in light of digital advances [50, 51]. This implies that the social groups involved interact in different ways from those involved with technological innovation—traditional employees-employers' hierarchies typical of the workplace are replaced by consumer-seller relationships, where power relationships occur in an always connected, and competitive, digital context. Wellman et al. [52] argue that digital technology users are connected in a specific way, that is, by means of networked individualism: fragmented, opportunistic, fast connecting individuals, and organizations forming temporary relevant social groups. Furthermore, SCODT posits that interaction switches from interpersonal to interpersonal, person-technology, technology-technology, and technology-physical environment interactions [50], where it is also artificial agents (*sensu* [53]) in addition to human agents that take decisions within such relationships.

4. Findings

Through thematic analysis, we identified three key themes in the dataset: (1) IoT awareness, including both industry and perceived public awareness; (2) trust in privacy and trust in security as industry challenges; (3) responses to privacy and security challenges of the IoT. **Table 2** shows how the challenges and the responses map.

	Challenges	Industry responses to the challenges
Privacy	Data collection is always on • uncertainty and insecurity surrounding data use • transparency of the smart device in regard with how it collects data and uses Illegal, malicious data use • impact of a privacy breach	Trials to find new ways to protect people's privacy • working on a safety program involving the practice of obscuring personal data Public campaigns • "Trust by Design for IoT products" • designing a new standard for "Privacy by Design" in smart home devices and services as part of the ISO PC 317 standard
Security	Lack of security awareness in the public • average person does not understand the security risks associated with IoT devices • difficulty in gauging which device has more security at the point of making a purchase • lack of education on how to make security judgments • Not understanding the impact of security breaches on smart home devices Regulation issues • Lack of regulation • lack of focus and fragmentation of government's efforts and responsibility • regulatory efforts not being sufficient since they rely on voluntary compliance Liability for the consumer Problem at the market level • security not being a priority because it lacks a sufficient market incentive	Security as a default setting Companies to develop standards and guidelines with the support of consumer organizations Security labeling to help consumers make informed choices Regulation enforcement to be made clear for consumers Developing specific technical security solutions External review and independent testing of devices Governments to take responsibility for the security of smart home devices Responsibility for the security of smart home devices should be transnational

Table 2.
Summary of the cybersecurity challenges of the smart home as perceived by the IoT industry, and of the industry's responses to these challenges.

4.1 Awareness

4.1.1 IoT awareness: connectedness and the problems IoT can solve

Businesses tended to provide general definitions of IoT—one in terms of the shape of communication it entails, its abstract structure, that is, IoT stands for "connected to everything everywhere" [3], and another in terms of its material structure, or "bare bones" [7], that is, "a piece of electronic equipment with a radio in it, in a box" [7]. NGO organizations, instead, defined the IoT less in terms of its shape and structure but more in terms of its function:

> *For most people it is the smart speaker, it's the home hub, it's the thing that does lots of tasks, which don't really add much – remove much friction from your daily life but they're nice to have. I don't really think they think about the more advanced areas that do actually remove friction. [4]*

In this case, the function of IoT, "not removing much friction" points at consumers' IoT identity coinciding with something superfluous—perhaps a luxury product of a consumeristic society.

The case of IoT being purely functional was made even stronger by this NGO respondent, who explained that a "true" IoT is "the problem that that device or that product is trying to solve" [5]. Also, the respondent elaborated on the idea of IoT as benign primarily represented by its function:

> *We're purists as an organisation, we want to see IoT for the real purpose of IoT rather than it being IoT washed if you like, where everyone is just putting a sensor on something or connecting something to call it IoT. I think that's the false IoT. [5]*

In this view, definitions of IoT simply based on structure, shape, network, and connections, do not fully represent the "real" IoT. Furthermore, both business organizations and NGOs point to privacy and security being issues that are intrinsic to IoT's identity.

4.1.2 Perceived public awareness

Business respondents were in agreement that public awareness of IoT was low: "I'd imagine there's still some people who won't know what IoT stands for" [3]. Also, they thought that while the public may be familiar with services such as Alexa (introduced in 2016 in the UK) they did not connect them with IoT, for example, "lots of people have got Alexa, lots of people have got Google Home, but they don't know that that's actually part of the IoT" [7]. Furthermore, the lack of awareness is also related to the need to have specific knowledge and skillset to be able to grasp IoT identity*:* "I don't think anybody I know that is not an engineer works for this industry understands what the IoT is or have heard of it" [7].

Regarding awareness of privacy and security issues, a business respondent stated that "I don't think people understand exactly what privacy is and what it means as a consumer." This view was echoed by an NGO respondent:

> *You see the stories of murder cases that use a small bit of audio from an Amazon Echo recording or how someone has been able to play a song in someone else's room when*

> *they shouldn't have. And they're funny, they're intriguing, they're engaging, but as I mentioned earlier, it's not tangible until it happens to you. [4]*

The "Stories" mentioned by the respondent point to the role of media reports of security incidents potentially shaping risk perception. However, these may be insufficient for the public to understand the risks more fully. The respondent explained that direct experience of working with IoT gives a more realistic idea of the extent to which security is an intrinsic aspect of IoT's identity:

> *there are much more concerning areas to it that I in my job are fully aware of and I would never have a smart home hub in my house, ever, and I wouldn't let my house mate bring his into my house because I just didn't like the idea of that thing being on. [4]*

4.2 Privacy

A prominent challenge pertaining to the smart home industry was privacy. Industry respondents pinpointed some examples of privacy issues pertaining to the smart home and also provided responses to these challenges.

4.2.1 Privacy challenges perceived by the IoT industry

In general, the context surrounding privacy issues was defined as a tradeoff between privacy versus productivity and a response concluded that "We're in a bit of a catch 22 scenario." Zubiaga et al. [4] explained the NGO respondent representing consumers. Smart home privacy issues were raised in unison across the industry spectrum since there was not a marked distinction between business organizations and NGOs in the kind of privacy issues being recollected.

Both NGO and business respondents referred to a privacy-problematic aspect of smart home devices, that is, data collection being always on: "Alexa, for example, has had a bad rep to the fact she's always listening" [3] and "every single word, every single tone, every single character is being referenced and archived for the evolution of AI for Alexa" [5]. This creates uncertainty and insecurity surrounding data use. The business respondent providing consultancy and design solutions, highlighted the central role of trust in the transparency of the smart device in regard to how it collects data and uses it, in other words, its integrity: "Not only the collection of data, what are you going to do with that data? Are you going to do what you're saying? And even if you do what you're saying, what does that mean for me?" [2]. This industry view displays awareness of how key a concern trust is in systems' integrity for successful smart home adoption.

Illegal, malicious data use is also a concern according to a respondent who reported the example of remote control wireless plugs used to control an appliance that was then discovered to be sending data to a server in China. A business respondent outlined the general lack of awareness in regard to the meaning and consequences of privacy breach: "People are not bothered if somebody can see their light going off" [7]. However, the respondent suggested that public attitudes can change when they become aware of the potential impact of a privacy breach:

> *It's when people understand what that privacy data that's getting out there means in a different context, and it starts to worry them. […] what happens if somebody breaks into your system and there's a guy there with the crowbar that knows that when the light's turned off you've gone to bed, and then he comes and breaks your back door? [7]*

4.2.2 Responses to privacy challenges

In order to respond to the privacy challenges of the smart home, business respondents reported experimenting with trials to find out the extent to which data can be collected and used. A business organization respondent providing services and products explained how they were having to be cautious of problems that are raised with the smart home in terms of what data can be shared and that they are experimenting with "workaround" trials to find new ways to protect people's privacy [3]. Specifically, they were working on a safety program involving the practice of obscuring personal data, thereby relying on partial data use: "what we've done is for that particular trial, we would hide parts of their journey so they can't actually be identified" [3].

An NGO respondent representing smart home consumers described two initiatives aimed at protecting privacy: the campaign "Trust by Design for IoT products" to make consumers aware of security risks in products such as IoT baby monitors, and principles and recommendations to make consumer rights, privacy, safety, and security key features of smart home devices; and designing a new standard for "Privacy by Design" in smart home devices and services as part of the ISO PC 317 standard [8], "Consumer protection: privacy by design for consumer goods and services" [54].

A service and product provider business respondent outlined that there are others in the sector, like service providers, who bear responsibility for protecting privacy: "providers, like the voice assistants like Google and Amazon, I think people are quite wary of. [...] So, I think they have a certain level of responsibility to reassure people and let people know where that data is going" [3]. The importance of integrity for increasing consumer trust is underlined by the business respondent who argued that it is service providers that have the greatest responsibility toward data integrity:

> *They need to do more and at least be open and honest what that data is being used for, because obviously the cases where you see an advert has been personalised for them from what it's heard in the home, then the data is being used for other purposes than what it stated. So, it does need to be more honest. [3]*

NGOs take responsibility for improving industry practices in regard to protecting privacy, while also calling for collaboration with external, noncommercial, and nongovernmental players as academic institutions and researchers:

> *there is certainly better than evil being done with AI. It is up to folks like us as a community, you all with your research, to participate in trying to help create this balance or expose the risk but expose the value of the technology. So that we don't have binary decisions. We want to make adjustments to ensure privacy that don't hinder the ongoing development and capability of things like AI. [5]*

In other words, the NGO respondent clearly declared their own responsibility but also the need to work alongside other players "as a community" to improve industry practices, persuade businesses to be more transparent about data use, and increase consumers' trust.

4.3 Security

4.3.1 Security challenges perceived by the IoT industry

Both NGO and business respondents believe there is a general lack of public awareness of smart home security issues. An NGO respondent representing the business community reported not feeling confident that the average person understands the risks associated with the security of IoT devices [5][3]. A business respondent providing testing and certification also agreed that the public lacks security awareness and that "the consumer doesn't really understand [...] how important it is to have a secure device..." [7]. The NGO respondent recollected a famous case of a hack of a smart home device in a Las Vegas casino, one of the most commercially secure areas as there can be, which allowed hackers to gain entry into their entire network and download its "high roller" database [5]. The underlying problem here is that the consumer finds themselves in a difficult position when having to gauge which device has more security at the point of making a purchase: "the end user ends up trying to make a decision, 'do I want to buy this for twenty dollars a person or do I want to buy this for fifty dollars a person?'" [5]. A business respondent pointed to a lack of a communication strategy to help the consumer make their choices in regard to the security of devices: "The way of explaining to them [the consumers] how secure a device is, is secure or isn't, there's no real way of demonstrating that by say a cybersecurity mark" [7]. An NGO respondent outlined how this lack of awareness of security issues of smart home devices coupled with a lack of education on how to make security judgments, creates a "ticking timebomb" situation: "[if] we put a whole bunch of IoT devices out there that are not secure, we're just creating a botnet army for the cyber guys" [5].

Furthermore, as with privacy, there may be a gap in regard to understanding the impact of security breaches of smart home devices. As a business respondent put it: "some people just don't even care. I know a number of people that have these cameras at home and they say they don't care... But I would hazard a guess that they would care if they were to find that their camera was livestreaming on the internet and they could see it themselves" [7].

Another key problem for both NGO and business respondents is the lack of regulation. For one NGO respondent, security standards are difficult to implement because of a lack of focus and fragmentation of the government's efforts and responsibility, for example, "security, for example, it's fragmented across government [...] it's with the National Security Secretariat, it's with DCMS, it's with Cabinet Office" [4]. For a business respondent, there was a sense that existing regulatory efforts are not sufficient, since they rely on voluntary compliance. This business respondent stated that businesses are slow to take action: "But the biggest problem I've noticed when I speak to customers is that cyber security is not yet mandated in products and because of that, people will not pay for that work to be done" [7].

An NGO-specific security concern is a liability for the consumer, for example, "I don't know about the UK but in the United States... If the hack goes through your network, known or unknown to you, you have a level of legal liability" [5].

[3] This reference number refers to the interview reference code used to preserve the businesses' anonymity in **Table** 1.

From a business perspective, however, security may not be a priority, as this business respondent stated: “When I speak to customers [product makers] their idea of security is, well, it’s something we want and something we’re thinking about, but it’s not a priority” [7]. Furthermore, there is a sense in the industry that security is not a priority because it lacks a sufficient market incentive: “Whether [cybersecurity] it’s a marketing point I’m not really sure. And I would even be not as sure to go towards a no.”

4.3.2 Responses to security challenges

Responses to security challenges differ between NGO and business respondents. An NGO respondent representing the business community stressed the importance of security being a default setting of devices that prevents security issues rather than reacts to them: “we want to see secure by design IoT devices out there rather than people thinking about security as an afterthought when it comes to just getting the product to market” [5]. Another NGO respondent representing consumers stated that standards and guidelines developed by companies with the support of consumer organizations can provide transparency of how IoT products should be developed [8]. As for a consumer-centered approach, a respondent stressed the need for security labeling that could help consumers to understand what kind of levels of privacy, security, and trust they could have in that product [5] and help them to make more informed choices. Also, in response to the challenge of fragmented regulation and lack of regulation enforcement, an NGO respondent stated that clarity about enforcement needs to be made clear for consumers: “regulation should be designed with consumers at the heart… [and] clear guidance needs to be set out on how policy and regulation will be enforced, and the measures need to be clear” [8].

Business respondents, on the other hand, reported working on specific technical security solutions such as blockchains in security and quantum key distribution and were “confident that the smart home will be protected through the use of these security technologies” [3]. Another business respondent providing consultancy and design solutions also stressed the need for external review and independent testing of devices to ensure security:

> *we would provide information about how secure we believe their product is, and then they would take that information and through some kind of dialogue work out some kind of solution on what they want to do to make the actual product more secure. [2]*

NGO respondents representing consumers stressed that, ultimately, the responsibility for ensuring the security of smart home devices lay with the government:

> *I think it’s really up to the government to think more broadly about how you change the discourse around security, about preparing for things that go wrong, rather than just reacting to them. [4]*

That smart home security is seen as the government’s responsibility is significant because it is unlike privacy, where responsibility seems to be down to the user to consent to data collection and use: “it really shouldn’t necessarily be solely down to the consumer to become security-savvy, to have to be the one that protects their device. The device should have some adequate level of protection to the consumer from the get-go” [5] stated the respondent representing the business community.

Another NGO respondent representing consumers stressed that such responsibility toward ensuring the security of smart home devices is transnational:

> *The responsibility for ensuring that consumers' rights are protected online, and autonomy and personal freedom are upheld, cannot be managed by one country alone. It requires international collaboration across governments, international organisations and businesses. [8]*

For this respondent, given the cross-border nature of data flows and the size of technology companies that are major market leaders in the development of smart home devices, national efforts should link to international approaches.

5. Discussion

The discussion of results centers on revealing the interpretive flexibility and closure of meaning that characterizes smart home devices. When technology is interpretively flexible, it means that the "interaction of technology and organizations is a function of the different actors and socio-historical contexts implicated in its development and use" [43].

In terms of awareness, business respondents tended to provide definitions of IoT in terms of its structural properties, that is, connectedness. NGO respondents, instead, defined the IoT more in terms of its function and the problems the IoT can solve. In this view, the IoT's identity is intrinsically connected to its pragmatic aspect, that is, its role in a context or "situatedness." This might explain why the wider UK population awareness is greater for the expression "smart home" (90% of people are aware of "smart home") than for the expression IoT (47% of people are aware of "IoT") [3], since "smart home" indicates a recognizable context for use of these devices.

Business respondents are uncertain about the public awareness of IoT. This finding was also reflected in [3]. A deeper awareness of IoT examples and functions may be crucial. Zeng and Roesner [55] point out in fact some of the limitations of current smart home devices design, for example, in regard with the management of multiple users and sometimes lacking basic access control. Hence, promoting awareness of functionalities of this kind may also stimulate adoption in the home, and different players in the industry may need to act in concert to stimulate this functional awareness.

The lack of awareness is also related to the need to have specific technical knowledge and skillsets to be able to grasp both the connectedness and functionality of IoT. This requirement for a technical mindset and expertise could place adopting the IoT beyond the reach of the layperson, particularly those who are less well-educated since usually, it is the "more highly educated individuals who tend to adopt innovations sooner" [56]. Also, [3] survey showed how those with high and medium levels of education were early adopters of smart home devices, though those with less education were catching up.

Business and NGO respondents feel privacy and security issues are not sufficiently part of IoT awareness for the wider public, which is consistent with the finding that 59% of the wider population are not aware of media reports of security incidents involving smart home devices [57].

Previous research [58] showed that the smart home industry is insufficiently emphasizing measures to build consumer confidence in data security and privacy. The industry respondents we recruited, felt they possessed the skillset to judge the security-preserving capacity of smart home devices, but were unsure about the public possessing adequate skillsets. This suggests there is a perceived need to educate the population in regard to security issues pertaining to IoT. This is consistent with the survey finding that consumers' security concerns are likely to impact negatively on IoT adoption. In regard to privacy, both business and NGO respondents raised privacy issues as an industry-wide IoT concern. Hence, privacy as an obstacle to the adoption of the smart home emerges as a stable and established meaning of the smart home. The specific issues respondents raised concern data collection being always on, the uncertainty of data use, illegal malicious data use, and legal but harmful data use. Particular emphasis was placed on the importance of trusting smart home systems' integrity—the belief that the entity is honest and will fulfill its promise to the client [59]—for successful smart home adoption; this view reflects the finding that public trust in companies *not* using data produced by smart home devices without consumers' explicit consent, was fairly low [3]. Significantly, the issue of the influence of friends and experts may have on Privacy Decision Making (e.g., allowing or denying data collection) was not mentioned by any of the participants but this was shown to be an important factor for IoT adoption [60].

One respondent outlined what was perceived to be the neutral position of the public in regard to the likelihood of privacy breach, which was also reflected in our survey [3]. However, in our survey, the public's neutrality changed when the emphasis was placed on understanding the impact or consequences of a privacy breach. Again, this emerging feeling was consistent with our survey finding that the UK public tends to agree that the impact of privacy-related incidents is high [3].

Actions in the form of responses to privacy challenges revolved mainly around taking responsibility for mitigating privacy-related risks. This is key because it has been shown that even when users do indeed trust device manufacturers to protect their privacy, they do not verify that these protections are in place [61]. For business respondents taking responsibility to address privacy-related risks involved taking direct action and experimenting with the technology in order to find new ways to protect privacy. Business respondents felt that a big part of the responsibility toward guaranteeing data integrity was with big service providers. On the other hand, NGO respondents responded to privacy challenges by emphasizing standards, applying pressure to improve industry practices toward data use, and persuading consumers that their data is properly curated and looked after. They also called for collaboration with external, noncommercial, and nongovernmental players, such as academic institutions and researchers. Synergy among industry or industry-relevant stakeholders emerges in this view as the key mechanism toward responding to the privacy challenges of the smart home. When it came to security, both NGO and business respondents associated security issues with the public's lack of awareness of security and uncertainty over making security judgments about a device, which is consistent with the survey finding that people seem to be more concerned about the likelihood of a security incident rather than its impact [3] (unlike for privacy, where it is the other way round), suggesting that there is an education gap in regard to the practical consequences of security breaches.

NGO and business respondents alike thought that security risks were exacerbated by problems at the level of regulation. Specifically, NGO respondents felt that the issue is with a fragmented security-regulation effort, with security being too thinly spread as an issue across government, which is therefore unable to provide a solid answer to this challenge. Steps have been made toward providing a unified approach, with the UK government producing the Code of Practice for Consumer Internet of Things Security [9]. However, this effort may not be sufficient to unify security improvement practice in the sector. Brass et al. [62] point to the proliferation of non-governmental *de facto* standards for smart home cybersecurity produced by businesses, trade associations, and interest groups, as well as NGOs themselves. For businesses, the issue with regulation is felt through a lack of enforcement.

Addressing a specific security concern, one NGO respondent felt that liability may be exacerbated through the public-wide lack of awareness of security issues of smart home devices. Businesses felt that a key security issue is the lack of a marketing incentive for smart home cybersecurity, a feeling that reflects a wider trend with cybersecurity in the private sector in general. Gordon et al. [63] underline how, in general, firms invest in cybersecurity activities at a level below what would be optimal. The issue is particularly significant in regard to small to medium enterprises (SMEs), which are deemed to be potentially the ones most at risk [64], as they often neglect cybercrime prevention [65] and do not possess adequate knowledge in cyber security [66].

In terms of actions, we found NGOs to be leading with the range of responses to the security challenges posed by smart home devices, as they primarily aim to make security a default positioning of devices. They stressed the key role of government in changing the *discourse* around smart home security. The choice of the socio-philosophical term “discourse” refers to the fact that it is both ideas and actions [67] around security that should be promoted and performed, a task for which the government is held to be both capable and responsible for. This perception underlines how it is important that the consumer does not feel he or she is solely responsible for smart home security. However, this feeling contrasts with the attitudes of the public, who ranked the service provider (e.g., Google, Amazon, and Apple) as the main actor responsible for the security of smart home devices, followed by the consumer and the manufacturer, with the government ranking fifth only [57]. This misalignment of perception across NGO experts and consumers may represent an opportunity for intervention for a number of players in the smart home ecosystem. Finally, the global marketplace for smart home devices reminds us that responsibility toward ensuring the security of smart home devices requires an international effort.

6. Conclusions for adoption and acceptability of the smart home

The aims of this project were to investigate smart home adoption from a socio-technical perspective that holds that people and the technologies they use are “co-constitutive” [12]. To this end, we qualitatively interrogated the survey findings pertaining to the most significant factors affecting smart home adoption, as previously flagged up quantitatively in [3]. Our objective was to understand how industry stakeholders interpret and influence smart home’s development in the UK and respond to the socio-technical challenges that smart home adoption flags up. The following findings reflect the different levels of interpretive flexibility regarding the challenges of smart home adoption

- Businesses are uncertain about the level of public awareness of IoT, particularly about privacy and security issues.

- Industry-wide concerns surrounding the privacy issues of smart home, concern data collection being always on, the uncertainty of data use, illegal malicious data use, and legal—yet harmful—data use.

- To respond to smart home privacy challenges, businesses are providing new technical solutions, whereas NGOs are producing standards and encouraging synergy amongst industry stakeholders at various levels and academia.

- Industry-wide concerns surrounding key security issues of a smart home are public uncertainty over how to make security judgments when purchasing a device, fragmented regulation for NGOs, and lack of regulation enforcement for businesses; an NGO-specific security concern is a liability; a business-specific concern is the lack of marketing incentive for security.

- In terms of actions, NGOs were found to be leading businesses in regard to the variety of responses to smart home security challenges as they aim to make security a default positioning of devices by underlining the need to change the discourse around security, to make the effort transnational, and to not make the consumer feel solely responsible for the security of smart home devices.

Overall, the smart home industry is responding to the smart home adoption challenges by providing new technical solutions to mitigate the privacy and security risk of smart homes, producing new standards and influencing regulation and building up communities of learning. These findings reveal that there is awareness in the industry of the need to improve sector practices by mitigating privacy and security risks of smart homes in order to increase consumers' trust and promote sector growth.

In terms of implications for the management of smart home adoption, this stakeholders' picture of smart home adoption in the UK and worldwide may help influence future business models and regulatory frameworks. Our study contributes to building awareness of obstacles to adoption and of ethics of data so that new, adaptable, and ethical business models can be proposed; policymaking by providing evidence of stakeholders' opinions toward regulation for common security or data interchange standards. With this knowledge, an open challenge for the smart home is the ethical concerns it may raise, in regard, among other things, cybersecurity. Hence future directions for this work may include the identification and specification of ethical principles relevant to assessing the ethical impact of the smart home and steps that can be taken toward increasing smart home acceptability—that is, the ethical and instrumental desirability for consumers of adopting new technologies.

The study has some limitations that can provide avenues for further research. We strived to achieve a balance of businesses and NGOs in our sample, and included one SME among the business respondents quota. Despite efforts taken to ensure a balanced sample, the small number of interview participants may still introduce bias in the results. Hence, to improve the approach taken in this work, the sample size could be increased in order to include: (1) a higher number of SMEs as these provide new ideas for products and services which can disrupt the sector's business models yet can also exacerbate security and privacy risks; also, this work does not address the voice of non-Western organizations involved in the development and management of the smart home. Hence future work could include the voice of more non-Western organizations to balance and achieve a more culturally diverse sample on the cybersecurity of the smart home. Of particular importance would be to also include representatives from developing countries, for whom the cybersecurity challenges of the smart home will be no less prominent, if not more, in the years to come.

Appendix A. Interview questions guide

Awareness

1. What do you think the IoT means to the public?

2. What do you think "smart home" means to the public?

Risks and benefits of IoT

For the organization

3. Can you summarize the business opportunity that these products and/or services represent for your company? What is your company's business model? (BUSINESS)

4. How easy has it been to promote IoT products and/or related services to the British public? (BUSINESS)

5. How big do you expect the market for your company's products and/or services to be in the future a) 5 years, b) 10 years' time? (BUSINESS)

6. How easy has it been for your organization to achieve your objectives in the IoT sector? (NGO)

For consumers

7. Why should consumers adopt a smart home device? What do you think are the key benefits of your product and/or service that make it desirable to adopt?

8. Why might they not adopt it?/What do you think are the main issues that might make people reluctant to adopt your company's products and/or services?

9. Is your organization taking any steps to deal with these issues? Which ones?

10. Are there new risks for the public specifically related to (your) IoT (products)?

Trust

11. Should consumers trust smart home devices?

12. Do you think the risks for privacy and security posed by smart home devices are acceptable?

13. What kind of actions would be necessary to improve public trust in smart home devices?

Digital divide/technology rejection

14. Are you aware of which groups are less likely to adopt smart home technology? What can your organization do about it?

15. These are some of the results of our survey. Do any of these come as a surprise? If so, why?

    i. Overall fairly low levels of trust

    ii. Overall, levels of satisfaction are still uncertain despite the prolonged presence of IoT in society

    iii. Younger respondents' low-risk awareness

    iv. Older respondents' resistance to IoT

    v. Less-educated respondents' resistance to IoT

16. Would these results be a concern for your company/organization and, if so, how might it respond?

Future and change

17. Do you think your company's business model/organization's strategy may need to adapt to deal with any of the challenges of IoT adoption?

18. If your organization was in charge of the whole sector, what would you change?

19. Are there any actions that the IoT industry as a whole should take to be able to encourage the adoption of IoT products and services?

20. Does your company welcome new policies and regulations for IoT products and services?

Author details

Sara Cannizzaro[1]* and Rob Procter[2]

1 Department of Computer Science and WMG, University of Warwick, Coventry, UK

2 Department of Computer Science, University of Warwick, Coventry, UK

*Address all correspondence to: sara.cannizzaro@warwick.ac.uk

References

[1] Armstrong, M. The Market for Smart Home Devices Is Expected to Boom over the Next 5 Years, 2022, Available from https://www.weforum.org/agenda/2022/04/homes-smart-tech-market/

[2] Kling R, Rosenbaum H, Hert C. Social informatics in information science: An introduction. Journal of the American Society for Information Science. 1998;**49**(12):1047-1052

[3] Cannizzaro S, Procter R, Ma S, Maple C. Trust in the smart home: Findings from a nationally representative survey in the UK. PLoS One. 2020;**15**(5):e0231615

[4] Zubiaga A, Procter R, Maple C. A longitudinal analysis of the public perception of the opportunities and challenges of the internet of things. PLoS One. 2018;**13**(12):1-18

[5] Consumers International. The Trust Opportunity: Exploring Consumers' Attitudes to the Internet of Things, 2019. Available from https://www.consumersinternational.org/media/261950/thetrustopportunity-jointresearch.pdf

[6] Zhang W, Liu L. How consumers' adopting intentions towards eco-friendly smart home services are shaped? An extended technology acceptance model. The Annals of Regional Science. 2022;**68**(2):307-330

[7] Jalali MS, Kaiser JP, Siegel M, Madnick S. The internet of things promises new benefits and risks: A systematic analysis of adoption dynamics of IoT products. IEEE Security & Privacy. 2019;**17**(2):39-48

[8] Tanczer L, Brass I, Elsden M, Carr M, Blackstock JJ. The United Kingdom's emerging internet of things (IoT) policy landscape. In: Ellis R, Mohan V, editors. Rewired: Cybersecurity Governance. New Jersey: John Wiley & Sons; 2019. pp. 37-56

[9] DDCMS Guidance. Code of Practice for Consumer IoT Security. 2018. Available from https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security

[10] DDCMS and Warman, M. Policy Paper: Proposals for Regulating Consumer Smart Product Cyber Security—Call for Views, 2020. Available from https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views

[11] Taebi B. Bridging the gap between social acceptance and ethical acceptability. Risk Analysis. 2017;**37**(10):1817-1827

[12] Meyer ET, Shankar K, Willis M, Sharma S, Sawyer S. The social informatics of knowledge. Journal of the Association for Information Science and Technology. 2019;**70**(4):307-312

[13] Kling R. What is social informatics and why does it matter? The Information Society. 2007;**23**(4):205-220

[14] Renaud K, Van Biljon J. Predicting technology acceptance and adoption by the elderly: a qualitative study. In: Proceedings of the 2008 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries: Riding the Wave of Technology. 2008. pp. 210-219. DOI:

10.1145/1456659.1456684. Available from: https://dl.acm.org/

[15] Oye ND, Aiahad N, Abrahim N. Awareness, adoption and acceptance of ICT innovation in higher education institutions. International Journal of Engineering Research and Applications. 2011;**1**(4):1393-1409

[16] Velmurugan MS, Velmurugan MS. Consumer behaviour toward information technology adoption on 3G Mobile phone usage in India. The Journal of Internet Banking and Commerce. 1970;**19**(3):1-8

[17] Sudhir K, Pandey M, Tewari I. Mobile Banking in India: Barriers and Adoption Triggers, 2012. Available from https://som.yale.edu/news/news/mobile-banking-india-barriers-and-adoption-triggers

[18] Lipford HR, Tabassum M, Bahirat P, Yao Y, Knijnenburg BP. Privacy and the internet of things. In: Modern Socio-Technical Perspectives on Privacy. Cham: Springer; 2022. pp. 233-264

[19] Guhr N, Werth O, Blacha PP, Breitner MH. Privacy concerns in the smart home context. SN Applied Sciences. 2020;**2**(2):1-2

[20] Rogers EM. Diffusion of Innovations. New York: Free Press; 1983

[21] Hsu CW, Yeh CC. Understanding the factors affecting the adoption of the internet of things. Technology Analysis & Strategic Management. 2017;**29**(9):1089-1102

[22] Hsu CL, Lin JC. Exploring factors affecting the adoption of internet of things services. Journal of Computer Information Systems. 2018;**58**(1):49-57

[23] Kim Y, Park Y, Choi J. A study on the adoption of IoT smart home service: Using value-based adoption model. Total Quality Management & Business Excellence. 2017;**28**(9-10):1149-1165

[24] Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019. New York: PublicAffairs, Profile books; 2019

[25] Helbing D, Caron H. Towards Digital Enlightenment. Cham, Switzerland: Springer International Publishing; 2019

[26] Sorwar G, Aggar C, Penman O, Seton C, Ward A. Factors that predict the acceptance and adoption of smart home technology by seniors in Australia: A structural equation model with longitudinal data. Informatics for Health and Social Care. 2022:1-5

[27] Cavallo F, Aquilano M, Arvati M. An ambient assisted living approach in designing domiciliary services combined with innovative technologies for patients with Alzheimer's disease: A case study. American Journal of Alzheimer's Disease & Other Dementias®. 2015;**30**(1):69-77

[28] Poel IV. A coherentist view on the relation between social acceptance and moral acceptability of technology. In: Philosophy of Technology After the Empirical Turn. Cham: Springer; 2016. pp. 177-193

[29] Shahrestani S. Internet of Things and Smart Environments. Cham: Springer International; 2018

[30] Taylor P, Allpress S, Carr M, Lupu E, Norton J, Smith L, et al. Internet of Things: Realising the Potential of a Trusted Smart World. London: Royal Academy of Engineering; 2018

[31] Porch.com. Swearing by Smart Homes. Analysing Trust in Smart Home Technology. 2017. Available from https://porch.com/resource/smart-home-trust

[32] TechUK. The State of the Connected Home. Edition 2 ed2018 Available from https://www.techuk.org/connected-home/our_report

[33] Van de Poel I, Verbeek PP. Ethics and engineering design. Science, Technology, & Human Values. 2006;**31**(3):223-236

[34] Misra S, Maheswaran M, Hashmi S. Vulnerable features and threats. In: Security Challenges and Approaches in Internet of Things. Cham: Springer; 2017. pp. 19-38

[35] Zeng E, Mare S, Roesner F. End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). USENIX Association; 2017. pp. 65-80

[36] Hove SE, Anda B. Experiences from conducting semi-structured interviews in empirical software engineering research. In: 11th IEEE International Software METRICS Symposium (METRICS'05). Como, Italy: IEEE; 2005. p. 10

[37] Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;**3**(2):77-101

[38] Khastgir S, Birrell SA, Dhadyalla G, Jennings PA. The science of testing: An automotive perspective. In: SAE World Congress Experience, WCX 2018, Detroit, United States; 10-12 April 2018. SAE Technical Papers; 2018. ISSN: 0148-7191. DOI: 10.4271/2018-01-1070

[39] Pliatsikas P, Economides AA. Factors influencing intention of Greek consumers to use smart home technology. Applied System Innovation. 2022;**5**(1):26

[40] Freeman C. Technology, Policy, and Economic Performance: Lessons from Japan. London: Pinter Pub Ltd; 1987

[41] Grint K, Woolgar S. The machine at work. Technology, Work and Organization. Cambridge, UK: Polity Press; 1997:65-94

[42] Pinch TJ, Bijker WE. The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. Social Studies of Science. 1984;**14**(3):399-441

[43] Orlikowski WJ. The duality of technology: Rethinking the concept of technology in organizations. Organization Science. 1992;**3**(3): 398-427

[44] Williams R, Stewart J, Slack R. Social Learning in Technological Innovation: Experimenting with Information and Communication Technologies. Cheltenham: Edward Elgar Publishing; 2005

[45] Yousefikhah S. Sociology of innovation: Social construction of technology perspective. AD-minister. 2017;**30**:31-43

[46] Humphreys L. Reframing social groups, closure, and stabilization in the social construction of technology. Social Epistemology. 2005;**19**(2-3):231-253

[47] Elle M, Dammann S, Lentsch J, Hansen K. Learning from the social construction of environmental indicators: From the retrospective to the pro-active use of SCOT in technology development. Building and Environment. 2010;**45**(1):135-142

[48] Rowland W. Recognizing the role of the modern business corporation in the "social construction" of technology. Social Epistemology. 2005;**19**(2-3):287-313

[49] Burns TR, Machado N, Corte U. The sociology of creativity: Part I: Theory: The social mechanisms of innovation and creative developments in selectivity environments. Human Systems Management. 2015;**34**(3):179-199

[50] van Baalen PJ, van Fenema PC, Loebbecke C. Extending the social construction of technology (SCOT) framework to the digital world. In: ICIS Thirty Seventh International Conference on Information Systems. 2016

[51] Burns TR, Corte U, Machado N. The sociology of creativity: PART III: Applications–The socio-cultural contexts of the acceptance/rejection of innovations. Human Systems Management. 2016;**35**(1):11-34

[52] Wellman B, Quan-Haase A, Boase J, Chen W, Hampton K, Díaz I, et al. The social affordances of the internet for networked individualism. Journal of Computer-Mediated Communication. 2003;**8**(3):JCMC834

[53] Sharov AA. Functional information: Towards synthesis of biosemiotics and cybernetics. Entropy. 2010;**12**(5):1050-1070

[54] ISO. ISO/PC 317. Consumer protection: Privacy by Design for Consumer Goods and Services, 2018. Available from https://www.iso.org/committee/6935430.html

[55] Zeng E, Roesner F. 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). 2019. pp. 159-176

[56] Bartel AP, Lichtenberg FR. The comparative advantage of educated workers in implementing new technology. The Review of Economics and statistics. 1987;**69**:1-1

[57] Cannizzaro, S. Procter, R. Ma, S., Maple, C., Trust in the Smart Home Dataset. 2020. Available from https://figshare.com/articles/Trust_in_the_smart_home_findings_from_a_nationally_representative_survey_in_the_UK_dataset_/12068379

[58] Wilson C, Hargreaves T, Hauxwell-Baldwin R. Benefits and risks of smart home technologies. Energy Policy. 2017;(103):72-83

[59] Mayer RC, Davis JH, Schoorman FD. An integrative model of organizational trust. Academy of Management Review. 1995;**20**(3):709-734

[60] Emami Naeini P, Degeling M, Bauer L, Chow R, Cranor LF, Haghighat MR, et al. The influence of friends and experts on privacy decision making in IoT scenarios. Proceedings of the ACM on Human-Computer Interaction. 2018;**2**(CSCW):1-26

[61] Zheng S, Apthorpe N, Chetty M, Feamster N. User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction. 2018;**2**(CSCW):1-20

[62] Brass I, Tanczer L, Carr M, Elsden M, Blackstock J. Standardising a moving target: The development and evolution of IoT security standards. Living in the Internet of Things: Cybersecurity of the IoT—2018;**2018**:1-9. DOI: 10.1049/cp.2018.0024

[63] Gordon LA, Loeb MP, Lucyshyn W, Zhou L. Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity. 2015;**1**(1):3-17

[64] Bell S. Cybersecurity is not just a 'big business' issue. Governance Directions. 2017;**69**(9):536-539

[65] Vakakis N, Nikolis O, Ioannidis D, Votis K, Tzovaras D. Cybersecurity

in SMEs: The smart-home/office use case. In: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE; 2019. pp. 1-7

[66] Kent C, Tanner M, Kabanda S. How south African SMEs address cyber security: The case of web server logs and intrusion detection. In: 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech). Balaclava, Mauritius: IEEE; 2016. pp. 100-105. Available from: https://ieeexplore.ieee.org/document/7737319

[67] Fairclough N. Language and Power. Edinburgh: Routledge; 2001