Security and Privacy Awareness in Smart Environments – A Cross-Country Investigation

Oksana Kulyk[1,2], Benjamin Reinheimer[2], Lukas Aldag[2], Peter Mayer[2], Nina Gerber[3], and Melanie Volkamer[2]

[1] IT University of Copenhagen, Denmark, okku@itu.dk
[2] Karlsruhe Institute of Technology, Germany, {name.surname}@kit.edu
[3] Technische Universität Darmstadt, Germany,
n.gerber@psychologie.tu-darmstadt.de

Abstract. Smart environments are becoming ubiquitous despite many potential security and privacy issues. But, do people understand what consequences could arise from using smart environments? To answer this research question, we conducted a survey with 575 participants from three different countries (Germany, Spain, Romania) considering smart home and health environments. Less than half of all participants mentioned at least one security and privacy issue, with significantly more German participants mentioning issues than the Spanish ones and the Spanish participants in turn mentioning significantly more security and privacy issues than the Romanian participants. Using open coding, we find that among the 275 participants mentioning security and privacy issues, 111 only expressed abstract concerns such as "security issues" and only 34 mentioned concrete harms such as "Burglaries (physical and privacy)", caused by security and privacy violations. The remaining 130 participants who mentioned security and privacy issues named only threats (i.e. their responses were more concrete than just abstract concerns but they did not mention concrete harming scenarios).

1 Introduction

Smart environments are becoming increasingly popular for end users, with smart homes reaching a household penetration of 9.5% worldwide in 2019 and an expected increase to 22.1% by 2023 [21]. Smart environments offer a multitude of possible applications, one of them being the assistance of elderly people or those

Oksana Kulyk, Benjamin Maximilian Reinheimer, Lukas Aldag, Peter Mayer, Nina Gerber, Melanie Volkamer. Security and Privacy Awareness in Smart Environments – A Cross-Country Investigation, Proceedings of AsiaUSEC'20, Financial Cryptography and Data Security 2019 (FC). February 14, 2020 Kota Kinabalu, Sabah, Malaysia Springer, 2020.

suffering from a health impairment by equipping their households with connected health devices (e.g., blood pressure monitors) and sensors (e.g., drop sensors) - often referred to as smart health environments. However, such smart environments of home and health applications also introduce potential security and privacy issues [5,7,10,11,18]. While there is an increasing body of research on the security and privacy vulnerabilities of smart environments (and how to address these vulnerabilities), it remains an open question, to which extent end users are aware of these issues. A number of studies investigating user perception of security and privacy risks in smart environments have been conducted in the US, however, less is known about users' awareness in other countries. In this work we aim to gain broader insights into this topic by conducting a large-scale qualitative survey with 596 participants from three different countries (Germany, Romania, Spain). These countries were chosen based on previous research conducted in Europe, which showed different security and privacy conceptions for the southern, northern, eastern, and western parts of Europe [6, 15].

We considered two examples of smart environments (smart home and smart health). Smart homes as a smart environment which has been around for some years already, have a larger user base and have been more present in the media compared to smart health environments. On the other hand, smart health environments could be considered as handling even more sensitive data than smart homes. Moreover, we included both owners and non-owners of these environments in our sample.

We find that less than half of the participants mentioned any security and privacy issues in smart environments, and that most participants focused on threats (e.g., data collection, monitoring, and data theft) or expressed abstract concerns about their security and privacy. Only 34 out of 596 participants described a potential harm caused by security and privacy violations that could result from living in smart environments, such as being burgled, being influenced in one's behavior, or getting increased insurance rates. This suggests that most participants lack a thorough understanding of how living in smart environments could affect their lives. At the same time, our study has demonstrated significant differences between the countries in terms of awareness about security and privacy issues. As such, the German participants seem to be more aware of security and privacy issues associated with smart environments than the Spanish and Romanian participants, with 74% of them naming at least one security and privacy issue compared to 44% of Spanish participants and 22% of Romanian participants. Furthermore, the participants named more security and privacy issues associated with smart homes than with smart health. This is alarming, as particularly smart devices that are connected to the users' body have the potential to severely harm their health if these devices are compromised in a cyber-attack. We discuss the implication of our findings, concluding the need for taking the cultural context into account when designing measures for data protection such as general awareness campaigns or services providing information to the end users relevant for data protection.

2 Background and Related Work

Although there are several studies on *users' awareness and perception of security and privacy threats*, in most of these studies participants were shown lists with different threats and asked to evaluate these. Few researchers, however, asked users to provide security and privacy threats on their own. Some studies e.g., Harbach et al. [9] or Stadion et al. [20] had a slightly different context in their study and asked the participants about the dangers of the primary use of the Internet. The participants could name only very few consequences and were not aware of most of the possible ones. Similar studies e.g. Bellekens et al. [4], Oomen and Leenes [17] or Aktypi et al. [1] with lists of various security and/or privacy risks found that people are unaware of concrete privacy and security risks and mainly worried about general privacy issues. In their study, Zeng et al. [23] focused on the group of smart home users and their knowledge of security and privacy threats. Unfortunately, the study comprises only very few participants, and therefore the significance of the dissemination of the knowledge of consequences is only limited here. Therefore, we have chosen the approach of questioning both users and non-users within the framework of a large-scale online study. Karwatzki et al. [12] had in their study 22 focus groups in which they asked the participants about possible privacy consequences. Whereas this is probably the most extensive study that has been conducted so far on people's awareness of privacy issues, Karwatzki et al. do not report how many participants referred to a particular issue. Moreover, their participants mostly referred to consequences that could arise from using online social networks, a well-established technology, while we focus on two emerging technologies, i.e., smart home and smart health environments. Garg [8] conducted a survey with 834 US-American IoT users, of which 115 reported to no longer use IoT devices due to privacy concerns. Another survey with experts and lay users [19] shows that if people care about concrete security and privacy issues, these are often of a financial or social nature, identifying identity theft, account breach, and job loss as the top rated tech-related risk scenarios.

Further studies focused on *influence of culture* on security and privacy risk perception. As such, Lancelot Miltgen et al. [15] conducted focus groups with participants from seven EU countries. The countries were chosen based on cultural differences and internet usage. Europe was divided into four major blocks: Northern, Eastern, Western, and Southern Europe. The findings suggest a difference between North and South with respect to responsibility versus trust. Also, people in the Southern countries perceive data disclosure as a personal choice, whereas people from Eastern countries feel forced to disclose personal data. A study by Cecere et al. [6] relying on a data set collected in 2009 by the EU Commission in 27 different European countries showed comparable outcomes to Lancelot Miltgen et al. [15]. Northern and Eastern European countries seem to be less concerned by potential misuse of personal data. People living in Southern and Central Europe, at the same time, tend to be more worried about their personal data. They explain their findings by the institutional legacy of former

collectivistic countries. Eastern countries are seen as more collectivistic, therefore are accustomed to government control, which reflects fewer privacy concerns.

3 Methodology

We conducted a qualitative survey with open answer questions to investigate people's understanding of potential security and privacy issues associated with the use of two different instances of smart environments – namely smart home and smart health environments – while considering people from different cultural backgrounds (i.e., from Germany, Spain, and Romania).

3.1 Smart Environments

Smart environments are a rather broad area as this can be any environment with any types of interconnected devices and sensors. We consider the transformation of people's homes into smart environments most relevant and thus decided to focus on our research on these smart environments in people's homes. Firstly, this includes all classical smart home devices (ranging from smart TVs to other smart household appliances, to various sensors e.g., for light and temperature) which have been around for several years. Secondly, this also includes smart health environments, i.e., equipping households with connected health devices (e.g., blood pressure monitors) and sensors (e.g., fall detectors) which are connected to the attending physician and/or various health services. We consider it worthwhile to study both of these smart environments, as (1) smart homes are likely to be more frequently used, but also more discussed in the media compared to smart health households; and (2) smart health data may be considered more sensitive than smart home data, but also might bring more advantages as it helps saving lives while smart homes are mainly for one's convenience. All these different characteristics might make a difference with respect to people's awareness of security and privacy issues.

We used the following definition of smart home and smart health devices for our study considering descriptions from other researchers such as used in [2, 14] while providing examples for the various types of connected devices:

A smart home is an environment in which household appliances (e.g., refrigerator, washing machine, vacuum cleaner), integrated devices (e.g., lights, windows, heating) and entertainment electronics (e.g., TV, game consoles) are networked and can be controlled via the Internet.

Smart health comprises health care devices (e.g., blood pressure monitors, scales, thermometers) and special sensors (e.g., drop-sensors, sensors in the toilet, heat sensors) which are connected to the Internet.

The actual descriptions used in the survey are provided in the supplementary materials A. These texts were pre-tested regarding their understandability and iteratively improved. One of our aims with the texts was to clearly emphasise the unique selling proposition for smart homes in the one case and smart health devices in the other.

3.2 Country Selection

The participants of our study were inhabitants of Spain, Romania, and Germany. The original concept included participants from Norway, which had to be abandoned due to a lack of participants (see supplementary materials for more details). Various factors led to the decision for the countries mentioned above. First of all, most studies referring to privacy and security are conducted in the US. In combination with the findings that national culture influences privacy and security concerns studying European countries seemed as an obvious extension of existing research. Studies concerning Internet privacy tend to split Europe into four major parts – namely northern, central/western, eastern, and southern Europe [6, 15]. This separation is based on cultural differences and equalities as well as Internet usage. Therefore, we decided to include participants from each of these major parts of Europe. Spain representing the Southern European states, Romania representing the Eastern states, and Germany representing Central/Western states. Norway would have been the representative for the Northern part of Europe.

3.3 Study Procedure

We used a between-subject design, randomly assigning participants to one of the considered technologies. All questionnaires were presented in participants' native language (i.e., German, Romanian, and Spanish) and implemented in SoSciSurvey [13]. The study procedure is:

Welcome and Informed Consent. We first thanked participants and provided them with information about our study (i.e., length, purpose, compensation, anonymity of their data, opportunity to withdraw from participation at any time). Participants were asked to provide their consent for participation and processing of their data by clicking on a button which was labeled with "I agree".

Introduction of Smart Environment. Participants were randomly assigned to one of the smart environments which was introduced to them in a brief descriptive text (see appendix A).

Open Question on Consequences of Smart Environment Usage. We used an open answer format inspired by Harbach et al. [9] to ask participants about possible consequences. In order to encourage the participants to list as many consequences as they are aware of, the questionnaire included ten text boxes and participants were instructed to enter one consequence per box, beginning with the most severe one: "Please enter all the consequences that may arise when using [smart home/health]. Please begin with the most severe possible consequence and leave the additional boxes empty if you do not know any further consequences." Participants also had the opportunity to provide as many additional consequences as they wanted in an extra text box at the end of the site.

Demographics and Thanks. At the end of the study, we asked the participants for demographic information. On the last page, we thanked the participants and provided contact details in case any questions would occur as well as the code they needed to receive their compensation from the panel.

3.4 Recruitment and Participants

We recruited our participants using the European panel "clickworker"[4], which is similar to Amazon Mechanical Turk (MTurk), but focuses on European users.

Participants received a compensation which corresponds to minimum wage in the respective country at the time the survey [5] was conducted, i.e., 1.50€ in Germany and 0.80€ in Spain. In Romania, we started with minimum wage, but since we had trouble finding Romanian participants with this low payment, we raised the compensation from 0.30 to 1€).

All relevant ethical preconditions given for research with personal data by our universities' ethics committee were met. On the start page, all participants were informed about the purpose and procedure of the present study. Participants had the option to withdraw at any point during the study without providing any reason and we informed them that in this case all data collected so far would be deleted. Participants were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Furthermore, we used SoSciSurvey [13] for the survey implementation, which stores all data in Germany and is thus subject to strict EU data protection law.

3.5 Data Analysis

First, as the questionnaires were presented in the main language of each country, the responses were cross translated, i.e., the responses were translated to English and then back to the original language to ensure the quality of the translation. Both translation processes were done by researchers who are used to work in a bilingual environment. The translated responses were then analysed using three rounds of coding.

In a first coding round, we used a closed coding approach, to identify those responses related to privacy and/or security. To that end, two researchers independently coded the responses. Differences in the codings were resolved using codings from a third independent researcher with a majority decision. Responses that were not clearly related to security and privacy were sorted out in this round as well.

In a second coding round, we then further analysed the responses clearly related to privacy and/or security. To that end, two researchers independently reviewed a subset of the responses using an open coding methodology to create a code book of security- and/or privacy-related themes from the responses. Open coding is a bottom-up method to structure qualitative data, based on participants' responses, rather than using pre-selected categories to code the responses. The codes were then discussed between the two original and an additional researcher, resulting in a final code book.

Using this process, a hierarchical code book arose, distinguishing between *abstract concerns* (i.e. responses such as "security issues" that do not specify a

[4] `https://www.clickworker.com/`, visited March 01, 2019

[5] Which took, according to our pretests, about 10 minutes to complete.

concrete result of a security and privacy violation), *threats* (i.e. responses such as "data theft" that specify a security and privacy violation but not necessarily mention a concrete harm resulting from it) and *harms* (i.e. responses that specify the concrete effect on one's well-being as a result of security and privacy violation, e.g. "home burglary"). The complete code book including codes in these three categories is provided in the supplementary materials (Appendix A.1). This code book was then used in a third round of coding by the two original researchers to perform selective coding of the responses.

All statistical analyses based on these three rounds of coding were conducted using the R statistics software environment.

4 Results

A total of 596 participants completed our study. Of them, 21 were excluded from further analysis because they provided at least one obvious nonsense-answer, e.g., "ahdjhdg". Out of the remaining 575 participants, 196 were from Germany, 185 from Romania and 196 from Spain. 206 participants reported to use their assigned smart environment (i.e., smart home or smart health) often or sometimes. Participants from age groups "<20" to "66–75" were represented in the sample, with the majority of the participants being from the age group "26–35". Further details on the demographics of the sample are provided in the supplementary materials.

4.1 Total Responses

Overall, we analysed 1117 responses (excluding two duplicate responses)[6]. Of them, 38 stated that the respective participants do not know any consequences that could result from using smart environments. 387 responses (stated by 275 participants) described negative aspects of smart environment usage that clearly referred to privacy and/or security issues (e.g, hacking or increased insurance rates due to access to medical information). Out of the participants mentioning at least one security and privacy issue, 147 were from Germany, 86 from Spain and 42 from Romania; 164 of them were assigned the smart home scenario, and 111 the smart health scenario.

4.2 Security and Privacy Issues

We categorized the security and privacy issues named by the participants on the three axes introduced in section 3.5, namely, whether the response describes abstract concerns, threats, or the harm on themselves (see section 4.2). Of all the participants mentioning at least one security and privacy issue, 111 mentioned

[6] Note that as described in Section 3.3, each participant was encouraged to list as many consequences as they could think of, having a total of 11 open questions which they could fill in.

only abstract concerns (of them, 43 participants from Germany, 46 from Spain and 22 from Romania; 72 assigned to smart home and 39 to smart health scenario), 34 mentioned at least one concrete harm (19 from Germany, 11 from Spain, 4 from Romania; 22 assigned to smart home and 12 to smart health scenario) and 130 mentioned at least one threat but no concrete harm (85 from Germany, 29 from Spain, 16 from Romania; 70 assigned to smart home and 60 to smart health scenario).

Table 1. Number of participants mentioning "only abstract concerns", "at least one concrete harm", "at least one threat but no concrete harm" (from left to right - Germany, Romania, Spain, smart home, smart health).

						Total
Only abstract concerns	43	46	22	72	39	111
At least one concrete harm	19	11	4	22	12	34
At least one threat but no concrete harm	85	29	16	70	60	130

Overall, more German participants named security and privacy issues than Spanish or Romanian ones. The German participants also named threats more

Table 2. Number of participants mentioning each of the detailed security and privacy issues (from left to right - Germany, Romania, Spain, smart home, smart health).

						Total
Abstract concerns						
Concerns about attacks	27	31	23	59	22	81
Concerns related to data abuse	17	3	0	7	13	20
General privacy concerns	33	22	4	38	21	59
General security concerns	11	9	3	17	6	23
Other	1	0	0	0	1	1
Threats						
Being spied on	44	4	3	34	17	51
Manipulation of functionality	0	2	1	3	0	3
Data being shared	25	5	1	12	19	31
Data collection	27	6	4	24	13	37
Data theft	20	14	9	20	23	43
Profiling	9	3	0	7	5	12
Transparency	11	2	0	8	5	13
Other	0	1	0	1	0	1
Harms						
Being blackmailed	2	0	1	2	1	3
Being influenced	3	4	0	4	3	7
Burglary	4	2	1	5	2	7
Financial loss	5	3	1	6	3	9
Health impairment	2	1	1	1	3	4
Identity theft	2	0	1	3	0	3
Other	2	1	0	1	2	3
Personalised ads	2	0	0	2	0	2

often and were more likely to describe the harm on themselves than participants from other countries. Moreover, German participants not only mentioned somewhat more security issues than Spanish participants, but also more of the German participants mentioned more threats and described the harm on themselves. In contrast, more of the Spanish answers described abstract concerns. Romanian participants provided the least responses referring to each category of security and privacy issues.

The most responses in the abstract concerns category described the possibility of a cyber-attack, while at the same time the most of the concerns mentioned by the German participants referred to privacy and data protection. The general privacy concerns were also mentioned more prominently in the smart health context than in relation to smart homes. Most of the responses mentioning a threat referred to privacy-related issues as well, such as the possibility of being monitored or spied on in one's own home, one's data being collected, or information about oneself getting disclosed or passed on to somebody else. The responses in the smart health context furthermore focused more on data being shared with third parties or stolen via unauthorised access, compared to the smart home context that focused on data collection or overall surveillance. Although only very few participants described the harm from the consequences that could result from living in smart environments on themselves, those who did, mostly named financial loss as both direct (e.g. via unauthorised access to one's financial accounts) and indirect (e.g. as increased insurance rates due to leakage of personal data), burglary due to both access to one's security system as well as to private information about when one is (not) at home and the possibility of being influenced in one's opinion or behavior.

4.3 Statistical Analysis

In order to investigate the differences in security and privacy risk perception among the participants in our sample, we looked at the awareness of security- and privacy risks, which we measured as a binary outcome, whether a participant mentioned at least one security- or privacy-related issue. In addition to looking at country of the participant and the smart environment to which they were assigned, we included age, gender and their smart environment usage (as actual users, potential users or non-users) as predictor variables. The logistic regression analysis has shown the country of the participant, the smart environment (either smart home or smart health) to be a significant factor ($p < .001$), as well as, to a lesser extent, smart environment usage ($p = .003$) and age ($p = .036$) (see the ouput of the analysis in the supplementary materials). The gender of the participant was not shown to be significant ($p > .05$). The post-hoc tests furthermore have shown significant differences between all the three countries ($p < .001$), with participants from Germany naming security and privacy issues most frequently, followed by Spain and Romania. Significantly more participants mentioned security and privacy issues for smart homes than for smart health devices, and significantly more potential than actual smart home and smart health users named security and privacy issues ($p = .002$).

5 Discussion

Several limitations apply to our study. Firstly, we chose a survey design, which prevented us from asking participants to further explain their answers if the meaning was unclear to us. Thus, some responses may have been related to security and privacy issues but were not considered in our final analysis. However, this study design allows us to compare the responses from a large sample of participants from three different countries, which would not have been possible with an interview study design. Furthermore, as we used a panel for recruitment, our sample might be biased in terms of age, academic background and technical expertise. However, if even younger, well-educated and tech-savvy people lack awareness of security and privacy issues associated with living in smart environments, the problems faced by the rest of the population might be even bigger.

Less than a half of the participants in our study mentioned at least one security or privacy-related issue of smart home usage, indicating that while there is some degree of awareness of these issues, for many users this awareness is still lacking. Our study furthermore shows that there are indeed differences between countries in terms of awareness about security and privacy risks. This might have an impact on data protection regulations and the success of their implementation and enforcement, especially if one aims to implement these on a global level given the cross-border nature of Internet-based services. Furthermore, as social factors are commonly recognized to play a role in the security and privacy behaviour of end users (e.g. resulting in reluctance to use security- and privacy-enhancing tools due to the fear of appearing overly paranoid, see e.g. [22]), it is worth investigating, how the different degree of awareness of security and privacy risks in various countries should be considered in developing security and privacy protection support methods.

The participants furthermore named security and privacy consequences of using smart health devices less often. When it comes to the differences in specific consequences, several differences between the two smart environments occur. As such, codes that imply transferring the data into the hands of third parties are mentioned more frequently in the context of smart homes than smart health. On the other hand, the issues mentioning data collection without referring to further sharing of the data are more prominently featured in the smart home context. A possible explanation is that while the participants understand the sensitivity of data collected by smart health devices, they are more likely to perceive the entity collecting the data as trustworthy (e.g., when consulting a physician) and therefore be more concerned about repurposing the data by other entities. As researchers stress the importance of context in determining privacy issues (see e. g. [3,16]), our findings provide a further confirmation for this approach, indicating the need to consider both cultural factors and context of a specific system or data exchange in order to support the end users with their security and privacy protection.

Acknowledgements

This work was partially funded by the European Unions Horizon 2020 Research and Innovation Programme through the GHOST project (`https://www.ghost-iot.eu/`) under Grant Agreement No. 740923. We specifically want to thank the project partners, Spanish Red Cross (`https://www.cruzroja.es`), TECSOS Foundation (`https://www.fundaciontecsos.es`), Televes (`https://www.televes.com`) and Kalos (`https://kalosis.com/`) for supporting our study with Spanish and Romanian translations. The research reported in this paper has furthermore been supported by the German Federal Ministry of Education and Research within the framework of the project KASTEL_SKI in the Competence Center for Applied Security Technology (KASTEL).

References

1. Angeliki Aktypi, Jason R.C. Nurse, and Michael Goldsmith. Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In *Workshop on Multimedia Privacy and Security (MPS)*, pages 1–11. ACM, 2017.
2. Mirza Mansoor Baig and Hamid Gholamhosseini. Smart health monitoring systems: an overview of design and modeling. *Journal of medical systems*, 37(2):9898, 2013.
3. Louise Barkhuus. The mismeasurement of privacy: using contextual integrity to reconsider privacy in hci. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 367–376. ACM, 2012.
4. Xavier Bellekens, Andrew Hamilton, Preetila Seeam, Kamila Nieradzinska, Quentin Franssen, and Amar Seeam. Pervasive ehealth services a security and privacy risk awareness survey. In *Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, pages 1–4. IEEE, 2016.
5. Niklas Buescher, Spyros Boukoros, Stefan Bauregger, and Stefan Katzenbeisser. Two Is Not Enough: Privacy Assessment of Aggregation Schemes in Smart Metering. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017(4):198–214, 2017.
6. Grazia Cecere, Fabrice Le Guel, and Nicolas Soulié. Perceived internet privacy concerns on social networks in europe. *Technological Forecasting and Social Change*, 96:277–287, 2015.
7. Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. Security Analysis of Emerging Smart Home Applications. In *Symposium on Security and Privacy (SP)*, pages 636–654. IEEE, 2016.
8. Radhika Garg. An analysis of (non-)use practices and decisions of internet of things. In David Lamas, Fernando Loizides, Lennart Nacke, Helen Petrie, Marco Winckler, and Panayiotis Zaphiris, editors, *Human-Computer Interaction – INTERACT 2019*, pages 3–24, Cham, 2019. Springer International Publishing.
9. Marian Harbach, Sascha Fahl, and Matthew Smith. Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In *Computer Security Foundations Symposium (CSF)*, pages 97–110. IEEE, 2014.
10. Weija He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *Symposium on Usable Privacy and Security (SOUPS)*, pages 255–272. USENIX, 2018.

11. Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. Smart Locks: Lessons for Securing Commodity Internet of Things Devices. In *Asia Conference on Computer and Communications Security (ASIACCS)*, pages 461–472. ACM, 2016.
12. Sabrina Karwatzki, Manuel Trenz, Virpi Kristiina Tuunainen, and Daniel Veit. Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, pages 688–715, 2017.
13. D. J. Leiner. Sosci survey (version 2.5.00-i), 2017. Retrieved March 01, 2019 from `https://www.soscisurvey.de/`.
14. A Lymberis. Smart wearable systems for personalised health management: current r&d and future challenges. In *Engineering in Medicine and Biology Society*, volume 4, pages 3716–3719. IEEE, 2003.
15. Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. Cultural and generational influences on privacy concerns: a qualitative study in seven european countries. *European Journal of Information Systems*, 23(2):103–125, 2014.
16. Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.
17. Isabelle Oomen and Ronald Leenes. Privacy risk perceptions and privacy protection strategies. *Policies and research in identity management*, 261:121–138, 2008.
18. Eyal Ronen and Adi Shamir. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. In *Symposium on Security and Privacy (SOUPS)*, pages 3–12. IEEE, 2016.
19. Michael Warren Skirpan, Tom Yeh, and Casey Fiesler. What's at stake: Characterizing risk perceptions of emerging technologies. In *Conference on Human Factors in Computing Systems (CHI)*, page 70. ACM, 2018.
20. Jessica Staddon, David Huffaker, Larkin Brown, and Aaron Sedley. Are privacy concerns a turn-off?: Engagement and privacy in social networks. In *Symposium on Usable Privacy and Security (SOUPS)*, page 10. ACM, 2012.
21. Statista. Smart home worldwide, 2018. Retrieved March 01, 2019 from `https://www.statista.com/outlook/279/100/smart-home/worldwide`.
22. Melanie Volkamer, Karen Renaud, Oksana Kulyk, and Sinem Emeröz. A socio-technical investigation into smartphone security. In *International Workshop on Security and Trust Management*, pages 265–273. Springer, 2015.
23. Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 65–80. USENIX, 2017.

A Supplementary Materials

Appendix A.1

A.1 Code book

The following code book was used to analyse the responses in the survey. The responses could be assigned multiple codes as follows. If multiple abstract concerns, but no concrete issues (that is, no threats or harms) were named in a response, the respective codes were simply assigned to the responses. However, if codes from both, the concrete and the abstract categories would have been coded in

a response, only the concrete codes were assigned, since the response specifies either the threat or the harm related to the concern, hence, it is no longer seen as abstract.

Abstract concerns The response mentions an abstract concern, without specifying either the threat that the adversary poses or the concrete harm that can result from the threat.

- General security concerns
  - Description: The response explicitly mentions security
  - Example: "security issues"
- General privacy concerns
  - Description: The response explicitly mentions privacy or data protection
  - Example: "Lack of privacy"
- Concerns related to data abuse
  - Description: The response explicitly mentions misuse or abuse of data
  - Example: "Possible misuse of personal data"
- Concerns about attacks
  - Description: The response explicitly mentions hackers or cyber-attacks.
  - Example: "They could hack into my data"

Threats The response a specific way one's security and privacy might be violated, without also necessarily mentioning the concrete harm a violation might cause.

- Data theft
  - Description: The response explicitly mentions data theft or someone stealing the data, or otherwise makes clear that the issue is with non-legal means of getting access to the data
  - Example: "If my data is stolen"
- Manipulation of functionality
  - Description: The response describes how unauthorised access or control to the system interferes with the functioning of the system.
  - Example: "Deactivation of the burglar alarm"
- Data collection
  - Description: The response mentions data being collected and stored
  - Example: "Smart home appliances collect information"
- Being spied on
  - Description: The response explicitly mentions spying, surveillance, monitoring or eavesdropping, or otherwise makes clear that the issue is about external observation of some kind
  - Example: "increased risk of monitoring in the personal environment"
- Being transparent
  - Description: The response explicitly mentions transparency (in a sense of users of smart environment being transparent to observation) or otherwise makes clear that the issue is about being totally exposed (as opposed to the codes "Data collection" or "Being spied on" where there is no such focus on total character of the exposure)

  - Example: “My way of life would not be private, but would be almost anytime x-rayed”
- Profiling
  - Description: The response explicitly mentions profiling or analysis or otherwise makese clear that the collected data is further processed
  - Example: “A profile is created which allows conclusions about my person”
- Data being shared
  - Description: The response makes clear that the collected data is shared with others, also referring to legal transfer to third parties.
  - Example: “Transmission of my data not only to the doctor, but also to the health insurance company”

Harms The response mentions an impact on one’s well-being that is the result of a security and privacy violation.

- Burglary
  - Description: The response mentions being robbed as either the result of manipulating the smart system or by learning the habits of the household members (i.e. times when no one is at home)
  - Example: “Being connected to the internet, intelligent devices can be hacked and can indicate whether they are at home or not, then causing a break”
- Financial loss
  - Description: The response mentions financial loss, either direct (e.g. someone hacking into one’s financial accounts) or indirect (e.g. insurance companies raising rates as the result of access to one’s health data)
  - Example: “Automated internet-connected systems can be remotely accessed by unauthorized people who could steal any amount from the user’s account”
- Being blackmailed
  - Description: The response mentions blackmail, either via controlling the smart home or threatening to expose sensitive information leaked from the smart system.
  - Example: “Takeover of the flat / the house by hackers for the purpose of extortion”
- Personalised ads
  - Description: The response mentions being targetted with personalised ads
  - Example: “My personal data is recorded in detail. As a consequence I will be targeted with ‘tailored’ advertisements”
- Being influenced
  - Description: The response mentions decision or opinion manipulation as the result of access to data
  - Example: “That companies get too much information about my preferences and use it to try to modify my opinions or habits, as has happened with Facebook and Trump”

- Health impairment
  - Description: The response mentions using smart health devices to harm one's health
  - Example: "Someone hack into your service and cause you a serious health problem by sending false information"
- Identity theft
  - Description: The response mentions identity theft or fraud as the result of access to personal data
  - Example: "Theft of identity"

A.2 Description of Smart Environments as stated in the questionnaire

Smart Home Smart home refers to a household in which household appliances (e.g., refrigerator, washing machine, vacuum cleaner), integrated devices (e.g. lights, windows, heating), and entertainment electronics (e.g., TV, voice assist, game consoles) are networked and can be controlled via the Internet.

This new technology delivers several conveniences:

- Increased quality of life e.g. concerning the refrigerator by detecting low supplies of important products and automatic ordering of these
- Building protection e.g. concerning lights by individual profiles for switching on and off
- Simplified ordering processes e.g instructing voice assistants such as Alexa via simple verbal orders

Smart Health Smart health describes a household in which health equipment (e.g. blood pressure monitor, scales, thermometer), special sensors (e.g., drop sensors, sensors in the toilette, heat sensors), and wearables (e.g. smartwatches, fitness trackers or smartphones) are connected.

This new technology delivers several conveniences:

- Improved information for doctors, e.g., blood pressure measuring instruments reporting and transmitting regular measurements
- Improved emergency response, e.g., drop detectors sending a direct emergency message to the rescue service
- Improved health, e.g., fitness trackers analyzing your sleep patterns

A.3 Questionnaire

Do you use smart home devices (e.g. refrigerator, automated light, voice assistants like alexa connected to the internet)/smart health devices (e.g. blood pressure measuring devices, case sensors, fitness tracker connected to the internet)?
Yes, I often use use smart home devices/smart health devices.
Yes, I sometimes use use smart home devices/smart health devices.
I do not use smart home devices/smart health devices, but I would like to use

them in the future.
I do not use social networks/use smart home devices/smart health devices and I do not want to use them in the future.

Please enter all the consequences that may arise from using [smart home/health]. Please begin with the most severe possible consequence and leave the additional boxes empty if you do not know any further consequences.

Gender: *m / f / other*
Age:
<20, 20-25, 26-35, 36-45, 46-55, 56-65, 66-75, 76-85, >85

A.4 Demographics of the sample

The following tables describe the demographics of our sample (excluding the participants who provided nonsense answers) in terms of age, gender and smart environment usage distributed between the three countries and the two smart environments.

Table 3. Demographics from left to right - Germany, Romania, Spain, smart home/health.

						Total
Female	88	61	97	123	123	246
Male	108	124	97	182	147	329
<20	11	50	14	43	32	75
20–25	28	56	56	77	63	140
26–35	65	59	55	98	81	179
36–45	33	14	57	49	55	104
46–55	36	5	9	26	24	50
56–65	20	1	2	11	12	23
66–75	3	-	1	1	3	4

Table 4. Usage frequency of smart environments from left to right - Germany, Romania, Spain, smart home/health.

						Total
Often	27	24	31	48	34	82
Sometimes	32	34	58	55	69	124
Never, but I would like to in the future	88	109	89	169	117	288
Never, and I would not like to in the future	49	18	16	33	50	83

We also aimed to include Norwegian participants in our study, but had trouble recruiting them. Initially, we chose the clickworker panel since they assured us to have a large enough user base in all four countries considered in our study. We started to recruit with minimum wage (3€) in Norway, but after a month only 17 participants had completed the questionnaire, compared to less than one week in Germany and Spain. We thus raised the compensation to 4.50€, which lead to another 73 completed questionnaires after 2,5 month. Since the Norwegian sample was still too small compared to the other samples, we asked several Scandinavian researchers for their advice. Unfortunately, none of them was aware of a platform like MTurk reaching Norwegians; also searching in Norwegian it was not possible to find an alternative Scandinavian panel (via internet and by asking other research colleagues). The contacted researchers further told us that finding Scandinavian participants for studies is a well-known problem, as most Scandinavians are not interested in participating in research studies for a small or moderate compensation, and Scandinavian researchers thus often rely on students or use foreign panels like MTurk. Finally, we decided not to include the 90 Scandinavian participants in our analysis, due to the small sample size, the long recruiting period and the Scandinavian researchers' experience with recruitment, all of which lead us to worry about the 90 participants in our sample being hardly representative for the Norwegian population.

A.5 Output of the statistical analysis

The following tables describe the results of the statistical analysis, investigating the effect of country of the participant, the smart environment they were assigned to, their usage habits of smart environment and their age and gender on security and privacy awareness, measured as naming at least one security and privacy issue.

Table 5. Analysis of deviance output for whether a participant named at least one security or privacy issue (factors ordered by p-value)

	LR Chisq	Df	Pr(>Chisq)
country	108.54	2	0.0000
environment	12.63	1	0.0004
user	11.50	2	0.0032
age	13.43	6	0.0367
gender	0.49	1	0.4828

Table 6. Post-hoc tests for comparison between the countries

contrast	estimate	SE	df	z.ratio	p.value
DE - RO	2.7108	0.2903	Inf	9.336	<.0001
DE - ESP	1.4535	0.2528	Inf	5.749	<.0001
RO - ESP	-1.2573	0.2574	Inf	-4.884	<.0001

Results are given on the log odds ratio (not the response) scale.

Table 7. Post-hoc tests for comparison between the usage habits

contrast	estimate	SE	df	z.ratio	p.value
non-user - potential user	-0.2432	0.3033	Inf	-0.802	0.4225
non-user - user	0.4853	0.3181	Inf	1.526	0.1271
potential user - user	0.7286	0.2179	Inf	3.343	0.0008

Results are given on the log odds ratio (not the response) scale.