Nina Gerber*, Benjamin Reinheimer, and Melanie Volkamer

Investigating People's Privacy Risk Perception

Abstract: Although media reports often warn about risks associated with using privacy-threatening technologies, most lay users lack awareness of particular adverse consequences that could result from this usage. Since this might lead them to underestimate the risks of data collection, we investigate how lay users perceive different abstract and specific privacy risks. To this end, we conducted a survey with 942 participants in which we asked them to rate nine different privacy risk scenarios in terms of probability and severity. The survey included abstract risk scenarios as well as specific risk scenarios, which describe specifically how collected data can be abused, e.g., to stalk someone or to plan burglaries. To gain broad insights into people's risk perception, we considered three use cases: Online Social Networks (OSN), smart home, and smart health devices. Our results suggest that abstract and specific risk scenarios are perceived differently, with abstract risk scenarios being evaluated as likely, but only moderately severe, whereas specific risk scenarios are considered to be rather severe, but only moderately likely. People, thus, do not seem to be aware of specific privacy risks when confronted with an abstract risk scenario. Hence, privacy researchers or activists should make people aware of what collected and analyzed data can be used for when abused (by the service or even an unauthorized third party).

Keywords: privacy risk perception, Online Social Networks, smart home devices, smart health devices

DOI 10.2478/popets-2019-0047
Received 2018-11-30; revised 2019-03-15; accepted 2019-03-16.

1 Introduction

Nowadays, there is a multitude of online services that are offered free of charge – at least at first glance. Instead of money, people are paying with the data that the service providers collect from them. Survey results indicate that the users of these services – including lay users – are indeed aware of this business model, i.e., that the service providers collect as much information about them as possible in return for the free services [10, 47, 59]. At the same time, the majority of users express concerns about such handling of their personal data [10, 47, 59].

Thus, it seems hard to believe people are actually surprised about the handling of their data every time they hear about a particularly bold privacy violation [8, 39, 51] when, at the same time, they continue to use privacy threatening online services and technologies exactly the same way they used to do prior to these revelations. The way people make (privacy) decisions gives us some insights into this paradoxical behavior [36]: The perceived risk determines how likely people are to protect their privacy. Yet, lay users have only a vague understanding of concrete consequences that can result from data collection [2, 26, 67]. When asked to name possible consequences, they often only refer to "personalized advertising", with some users even considering this beneficial [53]. This lack of understanding of possible consequences leads users to making intuitive risk judgments [4]. Garg, Benton and Camp [20] found that while the perceived risk of information sharing is the most important determinant of privacy behavior, users tend to share their personal data because they do not know about negative consequences that may arise and thus perceive the risk to be rather low.

Consequently, one could assume that the "holy grail" in motivating users to protect their privacy is to tell them about possible consequences that could result from data collection. However, research in the area of risk perception and communication tells us that people tend to base their decisions on perceived risk instead of actual risk [52, 62]. The goal of risk communication must therefore be to reduce, if not close, the gap between perceived risk and actual risk [54, 62]. The first step in achieving this goal is to evaluate how users perceive different privacy risks, either describing the general possibility of harm resulting from data collection or specifying how data collection might lead to negative consequences.

To this end, we conducted an online survey with 942 participants in which we asked them to rate nine differ-

***Corresponding Author: Nina Gerber:** SECUSO, Karlsruhe Institute of Technology, E-mail: nina.gerber@kit.edu
Benjamin Reinheimer: SECUSO, Karlsruhe Institute of Technology, E-mail: benjamin.reinheimer@kit.edu
Melanie Volkamer: SECUSO, Karlsruhe Institute of Technology, E-mail: melanie.volkamer@kit.edu

ent privacy risk scenarios (applying a between-subject design) according to their probability and severity. Since people often lack knowledge of potential privacy consequences [2, 20, 26, 67], which could lead them to grossly underestimate abstract risk scenarios in comparison to risk scenarios that state a particular consequence resulting from data collection [63], we included various abstract risk scenarios such as "data and usage patterns are collected" as well as various specific ones such as "the collected and analyzed information can be abused for targeted burglaries".

Additionally, early research on the awareness of online risks [17] has shown that unfamiliarity with a technology leads to lower risk perceptions, whereas other studies indicate that unknown technologies are considered to be more risky [15, 18]. Therefore, we included three different use cases of which one (Online Social Networks / OSN) is well-known to most people, while two (smart home and smart health devices) are, in comparison to OSN, a comparably new topic to the majority of people. All of these three technologies typically collect large amounts of sensitive data and they are either currently already used by a large amount of people or are likely to be used in the future by many people. This approach allows us to compare the risk evaluations for well-established and leading-edge technologies. Again, we implemented a between-subject design, i.e., each participant saw only one privacy risk scenario and was assigned to one use case.

Our results indicate that specific risk scenarios, e.g., stalking and targeted burglary, are considered to be more severe, but less likely compared to abstract risk scenarios. Specific risk scenarios are perceived to be most severe if they include a threat to one's physical safety or the possibility of financial loss. Concerning the abstract risk scenarios, the collection of data is perceived to be most likely and, in most instances, also most severe. Furthermore, the specific risk scenarios associated with the use of OSN are perceived as less severe than the specific risk scenarios associated with using smart home and smart health devices. Most of the risk scenarios related to the use of smart home devices are evaluated as most likely.

Our results provide several insights for privacy researchers or activists who aim to raise people's awareness of privacy risks by conducting privacy interventions or awareness campaigns: First, it is neither sufficient to focus on abstract nor on single specific privacy risks, since the former are considered to be less severe and the latter to be less likely. Hence, the most promising approach would be to mention the collection of data and also include a variation of specific privacy risks to account for different personal life situations. This should also raise people's evaluation of how likely the risks described will occur. Adequate candidates for such specific risks are those which comprise a physical safety component or the possibility of financial loss, since these are considered to be the most severe. Second, different use cases might call for different risks in terms of risk communication, with those risks which provide the best opportunity for an attacker to harm the user in a particular use case being the most promising.

2 Related Work

Our work relates to general risk perception, risk communication, and more specifically to the awareness and perception of privacy and IT security risks.

2.1 Risk Perception

Research on the perception of technological risks dates back to 1969, when Starr showed that the acceptance of risks is influenced by subjective dimensions such as the voluntariness of risk exposure [57]. Research in the following decades focused on the psychometric model paradigm to identify which factors influence risk perception. The most popular model is the canonical nine-dimensional model of perceived risk [16], which has been used extensively to study perceived risk offline for a diverse set of risks, e.g., health risks and environmental risks. According to Fischoff et al. [16], risk perception increases if risks are perceived as involuntary, immediate, unknown, uncontrollable, new, dreaded, catastrophic, and severe.

In the IT context, it has been used, e.g., to examine insider threats as well as security risks [15]. Yet the adoption of the Fischoff-model in the IT context has also been criticized. For example, a survey study on the perceived risk of several online threats revealed that the original risk dimensions only account for 13.07 % of the variance in people's risk perception, with severity alone explaining most of this variance. The authors reduced the model to four dimensions and found that these were able to explain 77% of the variance in risk perception with temporal impact (newness and common-dread) being the most important dimension for people's risk perception. New and uncommon threats were evaluated to be more risky, which is contrary to the results of Fried-

man et al. [17], who found that unfamiliarity with a technology leads to lower risk perceptions. We therefore look into three different use cases, of which one (OSN) is well-known to most people, whereas the other two (smart home and smart health devices) are rather new to the majority of lay users.

It has also been shown that, when it comes to technology, experts and lay users differ in the way they evaluate risks: Whereas experts base their judgments mainly on the objective probability and severity of a risk, lay users tend to rely on past experiences [13, 68], which can result in severe misjudgments that need to be addressed in awareness campaigns or other privacy interventions. Our main interest thus lies in investigating lay users' risk perceptions.

2.2 Risk Communication

Research on risk communication often refers to the "mental models approach", a framework according to which the mental models of the recipients of risk communication are supposed to be improved by adding missing knowledge, restructuring knowledge, or removing misconceptions [6]. Looking at lay users' mental models of privacy risks, we often find that they lack understanding of consequences that could result from data collection [2, 20, 26, 67]. We thus chose to include general risk scenarios and such describing particular consequences of data collection to investigate whether participants' risk evaluations increase when they are confronted with specific consequences. This is also in line with a seminal paper by Slovic [55], who suggests to mention possible adverse consequences when communicating risks to the public to increase their concerns.

Lay users were also found to focus on privacy consequences that happen online: For example, in a survey in which participants were prompted to name privacy consequences only 15% mentioned "real world" consequences such as stalking (3%) or employment risks (2%). On the other hand, 23% mentioned consequences associated with identity theft or financial loss (23%) [56]. According to the availability heuristic, people tend to overestimate the probability of risks that come easier to mind [63]. We thus included both kinds of consequences in our study in order to investigate whether they also differ in terms of perceived probability and security.

Camp [9] proposes the application of mental models for risk communication in the IT security and privacy context. She strongly argues for the use of physical and criminal metaphors in risk communication, e.g., by framing computer risks as risks of becoming victims of a crime. Although this approach aims at communicating security risks instead of privacy risks, we include these considerations in the phrasing of our risk scenarios by (1) telling the participants that the collection of their data could possibly harm them and thereby describing them as victims, and (2) referring to physical consequences such as stalking or burglary that happen in "the real world".

2.3 Privacy and IT Security Risk Awareness and Perception

There have been several studies on users' awareness of privacy risks in different contexts, e.g., eHealth [5], WiFi connections [32], RFID chips [31], or in general [21, 53]. These studies showed several misconceptions on the users' side, for example that hackers are considered to be the most serious threat in the WiFi context, that RFID chips could not be read without auditory or visual feedback, or that users are immune against most threats in the eHealth context. Overall, the results indicate that users are unaware and lack understanding of many possible privacy threats and consequences. We thus include a description of five different privacy consequences that could result from, e.g., identity theft, in our risk scenarios.

Regarding the actual perception of privacy risks, some studies only consider rather abstract privacy risks:

Oomen and Leenes [43] conducted a study with 5,541 Dutch students in which they asked them how concerned they were about different privacy risks. Participants were least concerned about unjust treatment and most about the invasion of their private sphere. However, the authors focused on rather abstract risks like "Loss of freedom" or "Invasion of the private sphere" and did not find much difference between the ratings. We investigate whether describing more specific consequences leads to more distinguished ratings.

Skirpan et al. [54] conducted a survey study with experts and lay users and identified identity theft, account breach, and job loss as the top rated tech-related risk scenarios. Whereas Skirpan et al. provided a list of rather abstract technological risks associated with emerging technologies without describing how and which consequences could result from these risks, we include abstract risks and particular privacy risks stating how, e.g., identity theft could lead to harassment in OSN. Furthermore, we investigate participants' perception of these risks in three different use cases.

Other studies do not allow us to draw conclusions about participants' risk perception due to methodological factors: Karwatzki et al. [30] ran a total of 22 focus groups in which they asked their participants directly to name all privacy consequences they are aware of. The authors derive seven categories of privacy consequences based on the responses: physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related consequences. Albeit providing valuable insights into peoples' awareness of privacy consequences, Karwatzki et al. do not investigate how risky these consequences are evaluated. Since this is the most extensive study that has been conducted so far on people's awareness of privacy consequences, we base our selection of privacy risk scenarios on the categories of different privacy risks identified by Karwatzki et al. (see section 3.4).

Woodruff et al. [66] conducted a survey study in which they asked participants to indicate for 20 different privacy-related scenarios with varying (positive and negative) outcomes whether they would provide their data if they knew this would be the outcome. Their participants were more or less completely unwilling to provide information in any of the negative scenarios. Considering that participants have no reasonable motivation to share their data if they know something negative will result from this, we decided not to ask whether they are willing to share their data in a particular scenario, but to assess their evaluation of a risk by asking them to rate the probability and severity of this risk.

Again, other studies focus on the perception of risks in the IT and online context in general, albeit without considering privacy risks: LeBlanc and Biddle [34] conducted a survey study on the risk perception of different Internet and non-Internet related activities with 94 participants using Amazon Mechanical Turk. Their results show that activities carrying the possibility of financial loss were evaluated as most severe, whereas potentially embarrassing activities were considered to be most likely.

In two survey studies, Harbach, Fahl and Smith [26] prompted Amazon MTurk panelists and German students to provide risks and consequences they associate with using the Internet. Participants were also asked to rate the severity and likelihood of the provided risks and consequences. Loss of privacy was rated to be by far the most likely consequence. Damage to one's health and large financial loss were rated as most severe. However, most people were only able to provide a few consequences and were unaware of the majority of possible consequences. Thus, we deploy a similar approach by asking our participants to rate the severity and probability of privacy risks, but provide participants with different privacy risks.

Conducting a survey study at their university, Garg and Camp [18] found that most of the variance in their participants' evaluation of IT security risks was explained by how new and common these risks are, with new and uncommon risks receiving higher risk ratings. Further, risks that have an analogue in the physical world were rated as being riskier than those who lack physical analogues.

We aim to close this research gap by evaluating lay users' perception of abstract as well as specific privacy risks describing particular consequences that could harm the user. To this end, we deploy the established definition of risk perception as the perceived probability of adverse consequences and the perceived severity of those [37, 62].

3 Methodology

This section describes our methodological approach. We describe our research question, the recruitment process and the sample, the study material and design, and ethical considerations.

3.1 Research Question

We conducted a survey study with 942 participants to answer the following research question:

RQ: How do lay users evaluate privacy risks that are associated with the use of established and new technologies, i.e., Online Social Networks (OSN), smart home and smart health devices?

3.2 Recruitment and Participants

We recruited our participants using the German panel "clickworker" [11], which is similar to Amazon Mechanical Turk, but focuses on European users, with German-speaking people being the largest user group [12]. We only recruited German-speaking users for our survey in order to prevent methodical artifacts resulting from participants evaluating the risk scenario texts in a foreign language (see 5.4 for a discussion about cultural influences). We used the clickworker IDs of those panelists who had participated in the pilot study to dismiss them from the main study in order to prevent participation

Table 1. Participants' age.

Age	<20	20 – 25	26 – 35	36 – 45	46 – 55	56 – 65	66 – 75	76 – 85
N	51	188	315	186	120	65	15	1
%	5.4	20.0	33.5	19.8	12.8	6.9	1.6	0.1

in both studies. Participants of the pilot and the main study both received a compensation of 2.10€.

A total of 942 participants completed our study. We used the exploratory data analysis function in SPSS 24.0 to check for answer patterns and whether participants took at least 3 minutes to complete the questionnaire (this value was chosen based on pretests). Note that the average time needed to complete the study is higher, as the study also included a part with open answer questions [22], which took participants much longer to complete than the quantitative questions that are described in this paper. None had to be excluded from the analysis due to technical problems or invalid answers. This seems surprising, but might be due to the fact that all questions were mandatory and thus needed to be answered in order to proceed with the study. Thus, participants who were not sufficiently motivated to complete the study adequately were likely to have dropped out before finishing the questionnaire. Due to technical restrictions of the clickworker panel, we unfortunately have no record of how many participants dropped out before finishing the questionnaire.

The final sample includes 942 participants (417 female, 517 male, 3 others, 5 chose not to answer this question). Participants' age is listed in Table 1. Most participants reported to use OSN often or sometimes, whereas only about one third stated to use smart home or smart health devices frequently. Participants reported a median of 0 years for IT security expertise and are thus considered to be lay users. According to the IUIPC questionnaire [38], participants were rather concerned about their privacy with an average of 3.51 (the scale ranging from 1, indicating low levels of concern, to 5, indicating high levels of concern; SD=0.75, med=3.5).

3.3 Use Cases

We investigate three different use cases one of which is well-known to most people (OSN) and two are a rather new topic to the majority of lay users (smart home and smart health devices). This approach allows us to draw conclusions about lay users' risk perception of already established and emerging technologies, as prior research has provided evidence for novel technologies being perceived as less risky [17], as well as more risky [15, 18] than well-known technologies.

We decided to include OSN in our study since this kind of technology is used by a considerably large number of people (with 2.46 billion users in 2017 [14]). Furthermore, the topic of OSN privacy risks is relatively well-covered in media reports [40, 46, 60]. Smart home and smart health devices, on the other hand, should be new ground for most lay users. Hence, it is possible that they did not put much thought on potential privacy risks emerging from the use of these devices so far. However, smart home and smart health devices combine several sensors and thus collect and analyze a multiplicity of – often sensitive – data, in the case of smart home devices in an environment deemed to be most private, and in the case of smart health devices about a highly sensitive data type. As both technologies are constantly spreading, this makes them interesting candidates for studying users' evaluation of privacy risks.

3.4 Privacy Risk Scenarios

We chose to include four scenarios in our study which describe abstract privacy risks and thus leave it to the participant to interpret what actual consequences could arise from the collection and analysis of their data. We further included five specific risk scenarios with each of them focusing on a particular consequence of data collection and analysis. Those were based on categories of privacy risks lay users associate with the access to their personal data identified by Karwatzki et al. [30]. This combination allows us to compare how users perceive scenarios with different levels of specificity, as prior research has shown that users often lack knowledge about possible privacy consequences [2, 20, 26, 67], which could lead them to underestimate the risk of abstract privacy risk scenarios but make better judgments when confronted with a concrete consequence resulting from a risk scenario.

We refer to "the manufacturer" (for the smart home and smart health use case[1]) and "the service provider" (for the OSN use case) as the one who collects the data. This decision was based on prior research, which has

1 We chose the manufacturer for these use cases as there are often multiple devices from various manufacturers in a smart home or smart health setting and the term "service provider" thus might have confused our participants for it is not clear who is the service provider in this setting.

shown that people are almost always scared of criminals (e.g., hackers) accessing their data, whereas data collection by the manufacturer or service provider is sometimes considered to be acceptable [23]. Yet, taking a look at the privacy policies and terms of use of popular OSN, smart home, and smart health devices, it can be assumed that manufacturers collect at least some kind of data. According to the concept of contextual integrity [41], people's evaluation of data collections depends on whether (1) this collection and processing is appropriate in the given context, and (2) meets governmental regulations. We were thus interested in how people perceive potential threats arising from this data collection, which describe inappropriate as well as illegal processing of their data. The texts used in the study to describe the privacy risks are presented below. All texts were presented in German and translated for the paper.

Abstract Privacy Risk Scenarios. Abstract risk scenarios vaguely refer to an unspecific risk, without stating how the user could be harmed. The first privacy risk scenario, (R1), focuses on the "collection" of information and usage patterns, thereby reflecting a phrase typically used in the media to talk about data assessment in the digital context [25, 44]. The following risk scenarios (R2) and (R3) successively add more information by also saying that the collected data are analyzed and explaining the concept of meta data. Finally, (R4) more straightforwardly points at an unspecific risk by saying that the results of the analysis could be utilized to harm the user. The actual texts we used in the study are the following ones:

- (R1) Your entered data and usage patterns are collected by the various manufacturers of [use case[2]].
- (R2) Your entered data and usage patterns are collected and analyzed by the various manufacturers of [use case].
- (R3) Your entered data and usage patterns* are collected and analyzed by the various manufacturers of [use case].
  *Usage patterns are defined as how one behaves with regard to special services or devices. The behavior occurs repeatedly and does not necessarily involve conscious behavior. Examples for usage patterns are switching the light on at certain times or ordering certain food on certain days.
- (R4) Your entered data and usage patterns* are collected and analyzed by the various manufacturers of [use case]. The results of the analysis can harm you.
  *Usage patterns are defined [...][3]

Specific Privacy Risk Scenarios. The idea of specific privacy risks is to describe a particular consequence of data collection and analysis, thereby clarifying how the data can be used to harm the participant. To identify possible consequences, i.e., specific privacy risk scenarios, we used the categorization of Karwatzki et al. [30], who conducted a set of 22 focus groups on privacy risks. They identified seven categories of risk scenarios their participants are aware of: Freedom-related, physical, resource-related, social, career-related, psychological and prosecution-related. We aimed to include a mix of more and less obvious examples for these categories. We did, however, not include the categories "Psychological" (negative impact on one's peace of mind owing to access to individuals' information) and "Prosecution-related" (legal actions taken against an individual owing to access to individuals' information), as we considered the former one would be too hard to grasp for some participants and the latter describes a risk that does likely not apply to most users.

The specific texts we used in the study are the following ones (please note that the order of presentation is random and does not reflect any assumptions about a hierarchy in terms of severity and probability evaluation of the described risk):

- (R5) [Freedom-related] Your entered data and usage patterns* are collected and analyzed by the various manufacturers of [use case]. The results of the analysis can harm you by passing the results on to your insurance company. This can restrain you in the choice of your nutrition if you do not want to get a worse premium rate.
  *Usage patterns are defined [...]
- (R6) [Physical] Your entered data and usage patterns* are collected and analyzed by the various manufacturers of [use case]. The results of the analysis can harm you since from the analysis it is known where you are at what time. That way you can become a victim of stalking.
  *Usage patterns are defined [...]
- (R7) [Resource-related] Your entered data and usage patterns* are collected and analyzed by the var-

2 Depending on the use case, the text contained either "smart home devices", "smart health devices", or "Online Social Networks".

3 The same text presented in (R3) about usage patterns was contained in (R4) and in all the specific privacy risk scenarios.

Fig. 1. Study procedure.

ious manufacturers of [use case]. The results of the analysis can harm you since from the evaluation it is known when you are at home. That way targeted burglaries can be planned.
*Usage patterns are defined [...]

– (R8) [Social] Your entered data and usage patterns* are collected and analyzed by the various manufacturers of [use case]. The results of the evaluation can harm you by unauthorized people taking over your identity. That way inappropriate content can be published on your behalf.
*Usage patterns are defined [...]
– (R9) [Career-related] Your entered data and usage patterns* are collected and analyzed by the various manufacturers of [use case]. The results of the evaluation can harm you by passing on the results to your potential future employer. This can result in worse chances of getting a new job.
*Usage patterns are defined [...]

3.5 Study Procedure

We used a 9x3-between-subject design, randomly assigning participants to one of the three considered technologies and one of the nine different risk scenarios. All questionnaires were presented in German and implemented in SoSciSurvey [35]. It took participants 13.68 minutes on average to complete the study (SD=7.38). The presented study is part of a larger study on the perception and awareness of privacy risks [22]. Those parts of the study procedure which are relevant for the presented research question are described below and displayed in Figure 1 (see section 7.3 in the appendix for the whole questionnaire).

We first thanked participants and provided them with information about our study. 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". We then asked participants to indicate whether they used the three considered technologies, and if not, whether they liked to use them in the future. Participants were then randomly assigned to one specific technology which was introduced to them in a brief descriptive text (see section 7.3 in the appendix). In case they did not use the assigned technology, participants were prompted to imagine they would actually use it in order to answer the questionnaires. We then showed the participants one of the nine randomized texts (R1)-(R9) describing potential privacy risk situations, with four texts describing rather abstract privacy risk situations (section 3.4) and five texts focusing on specific risk scenarios (section 3.4). Participants were asked to answer two questionnaires assessing their evaluation of the privacy risk. We used a scale consisting of four items to assess the perceived probability of the privacy risk and one item to assess the perceived severity of the privacy risk. We decided to use a VAS, that is, a continuous line with labels at both ends (e.g., "stongly agree" and "strongly disagree"). Several researchers have proposed to use Visual Analogue Scales (VAS) to overcome the limitations of Likert scales, such as the data being ordinally distributed (e.g., [48, 58]). In SoSciSurvey, which we used to implement our questionnaire, these VAS assess data between 1 and 100. The participants, however, only saw the labels without the corresponding numbers. Still, we think it is sensible to use these values for the analysis, as it is common to talk about probabilities on a percent basis, which ranges from 1 (or 0) to 100. To maximize validity and reliability, we based our items upon a previously validated instrument [36]. However, as we adjusted the wording of the items to fit our research purpose, we ran a pilot study to check whether the adjusted items still achieve sufficient psychometric values (see section 3.6). We further asked participants to complete the IUIPC questionnaire's global information privacy concern scale [38]. Finally, we asked participants to provide demographic information. On the last page, we thanked the participants and provided them with contact details in case any questions would occur, as well as the code they needed to receive their compensation from the panel.

3.6 Pilot Study

We conducted a pilot study with 45 participants (16 female, 28 male, 1 other, aged between 18 and at least

56 years) to check the quality of our adjusted items. Participants were randomly assigned to one of the three use cases. Thus, every use case was considered by 15 participants. Internal consistency was checked for every subscale and item-total correlation for every item to ensure the reliability and validity of the measures. As all items showed satisfactory values (see section 7.2 in the appendix), no items had to be omitted.

3.7 Ethics

All relevant ethical preconditions given for research with personal data by our university's 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 [35] for the survey implementation, which stores all the data in Germany and is thus subject to strict EU data protection law.

4 Results

This section describes our survey results, starting with the perceived probability of the nine risk scenarios, which is followed by the perceived severity. Finally, we take a look at the relationship between both scales.

4.1 Perceived Probability

The data distribution for perceived probability of the nine risk scenarios is displayed as box plots in Figure 2 on the left side. Whereas (R1) *Collection* (of data) is considered to be very likely (with a median between 80% and 90%), participants are not so sure when it comes to the specific risk scenarios (i.e., (R5) *Nutrition*, (R6) *Stalking*, (R7) *Burglary*, (R8) *Inappropriate content*, (R9) *Job application*), which are located around a median of 50%. Generally, the abstract risk scenarios were considered to be more likely than the specific risk scenarios. While our participants are quite certain that their data are collected, they are undecided about how this data collection could harm them. Apparently, around half of the participants felt that chances were good for any of the specific risk scenarios to happen, whereas the other half thought it rather unlikely.

Table 2. Results of the MANOVA regarding the comparison of perceived probability of the risk scenarios (DV) between the different risk scenarios (IV).

	df	F-value	Sig.	partial η^2
Social Network	8, 311	14.78	<.001**	0.28
Smart Home	8, 302	9.75	<.001**	0.21
Smart Health	8, 297	5.43	<.001**	0.13

The vast majority of our participants thought that chances were at least 50% that the analysis of the collected data could harm them, which reflects the high level of privacy concerns usually expressed in this context [10, 47]. There are no notable differences regarding the use cases, except for (R3) *Usage patterns*, which are evaluated to be more likely when using OSN. Interestingly, the collection and analysis of usage patterns is rated as more likely than the mere collection and analysis without referring to usage patterns in the OSN and smart health devices use case, suggesting that participants believe that their actual usage content (e.g., posts in OSN, health data) is less likely to be analyzed than their usage patterns.

The risk scenario that is perceived as least likely in all three use cases is worse chances regarding (R9) *Job applications* due to data sharing with possible future employers. Yet, the specific risk scenarios do not differ much among each other in as how likely participants evaluate them.

We ran a MANOVA with the privacy risk scenario and the use case as independent variables (IV) and the mean of the perceived probability and severity of the different risk scenarios as dependent variables (DV). All assumptions for conducting a MANOVA were met. We checked normality using Q-Q-Plots, and homoscedasticity using the Levene-Test. The analysis showed significant differences regarding the perceived probability of the different risk scenarios in all three use cases. In summary, the abstract risk scenarios were considered to be more likely than the specific ones, with the collection of data (R1) being the most and worse chances regarding job applications (R9) being the least likely. Table 5 in the appendix provides an overview of the results of the post-hoc pairwise comparisons, Table 2 shows the results of the MANOVA regarding the perceived probability.

Social Network. Post-hoc tests using Sidak correction (as implemented in IBM SPSS 24.0) showed that all of the specific risk scenarios (R5)-(R9) were consid-

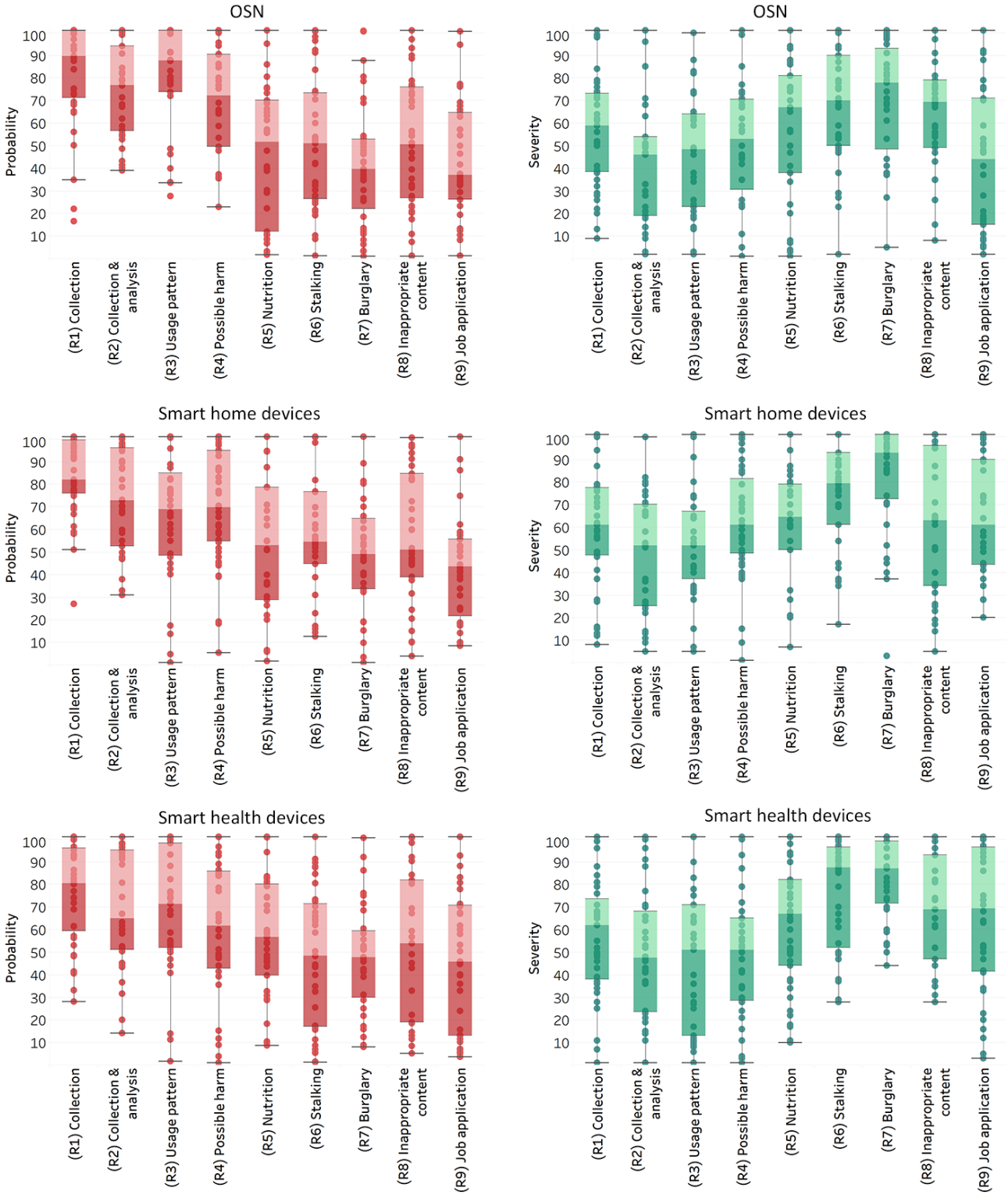

Fig. 2. Boxplots of the privacy risk evaluation data showing the medians and ranges for the probability ratings (left) and severity ratings (right).

ered to be less likely than the abstract ones (R1)-(R3) (with p<.01). (R4) *Possible harm* was further considered to be more likely than (R5) *Nutrition*, (R7) *Burglary* and (R9) *Job application* (p<.05).

Smart Home. All of the specific risks (R5)-(R9) were considered to be less likely than (R1) Collection (p<.01). (R2) *Collection & analysis* and (R4) *Possible harm* were further considered to be more likely compared to (R7) *Burglary* and (R9) *Job application* (p<.01). (R3) *Usage patterns* was considered to be more likely than (R9) *Job application* and less likely than (R1) *Collection* (p<.05).

Smart Health. (R1) *Collection* was considered to be more likely than (R6) *Stalking*, (R7) *Burglary*, (R8) *Inappropriate content*, and (R9) *Job application* (p<.05). (R2) *Collection & analysis* was considered to be more likely than (R6) *Stalking*, (R7) *Burglary*, and (R9) *Job application* (p<.05). (R3) *Usage patterns* was considered to be more likely than (R9) *Job application*.

The MANOVA showed no significant differences regarding the perceived probability of the different risk scenarios between the three use cases (with p>.05), indicating that the technology has no significant effect on the perceived probability of the considered risk scenarios. There was also no significant interaction effect between risk scenario and use case (p>.05).

4.2 Perceived Severity

Figure 2 shows the data distribution for perceived severity of the nine risk scenarios on the right side. Generally, the specific risk scenarios were evaluated to be more severe than the abstract risk scenarios, which provides evidence for the assumption that people are generally unaware of specific consequences that could result from data collection and analysis but adjust their evaluation when confronted with specific consequences. (R1) *Collection* (of data) was perceived to be more severe than the other abstract risk scenarios, including the combination of (R2) *Collection & analysis*. This is surprising, considering that the potential for negative effects increases if data are not only collected but also analyzed. Since (R2) *Collection & analysis* also comprises the collection of data, this scenario should be considered as at least equally severe than (R1) *Collection*. Regarding the specific risk scenarios, participants perceived (R7) *Burglary* as most severe in all three use cases. This matches previous research [26, 34], which has shown that people dread risks associated with financial loss.

Table 3. Results of the MANOVA regarding the comparison of perceived severity of the risk scenarios (DV) between the different risk scenarios (IV).

	df	F-value	Sig.	partial η^2
Social Network	8, 311	5.60	<.001**	0.13
Smart Home	8, 302	5.21	<.001**	0.12
Smart Health	8, 297	7.51	<.001**	0.17

The perceived severity of the abstract risks hardly differed between the three use cases, except for (R4) *Possible harm* with a median of 50 regarding the use of OSN and smart health devices, and a median of 60 regarding the use of smart home devices. This suggests that our participants had a slightly worse unspecific bad feeling about the use of smart home devices, which is, however, not reflected in their attitude regarding specific adverse consequences of smart home device usage. How severe the specific risk scenarios were evaluated also depends on the use context, with risk scenarios associated with OSN use being considered as less severe.

The statistical analysis further showed significant differences regarding the perceived severity of the different risks in all three use cases (see Table 3). In summary, participants mostly dread (R6) *Stalking* and (R7) *Burglary*, whereas the (R2) *Collection & analysis* of data is considered as least severe. Table 6 in the appendix provides an overview of the results of the post-hoc pairwise comparisons.

Social Network. Post-hoc tests using Sidak correction showed that (R6) *Stalking* was considered to be more severe than (R2) *Collection & analysis* and (R9) *Job application* (p<.05). (R7) *Burglary* was considered to be more severe than (R2) *Collection & analysis*, (R3) *Usage patterns* and (R9) *Job application* (p<.01). (R8) *Inappropriate content* was considered to be more severe than (R2) *Collection & analysis*, and (R9) *Job application* (p<.05).

Smart Home. (R6) *Stalking* was considered to be more severe than (R2) *Collection & analysis* (p<.01). (R7) *Burglary* was considered to be more severe than all of the abstract risk scenarios (R1)-(R4), as well as (R8) *Inappropriate content* (p<.05).

Smart Health. (R6) Stalking was considered to be more severe than (R2) *Collection & analysis*, (R3) *Usage patterns*, and (R4) *Possible harm* (p<.01). (R7) *Burglary* was considered to be more severe than all of the abstract risks (R1)-(R4) (p<.01).

The MANOVA also showed significant differences regarding the perceived severity of (R4) *Possible harm*

Table 4. MANOVA results regarding the comparison of the perceived severity (DV) between the different use cases (IV).

	df	F-value	Sig.	partial η^2
(R1) Collection	2, 112	0.24	.78	0.004
(R2) Collection & analysis	2, 103	0.78	.46	0.020
(R3) Usage patterns	2, 91	0.61	.55	0.010
(R4) Possible harm	2, 104	3.75	.03*	0.070
(R5) Nutrition	2, 98	0.22	.80	0.005
(R6) Stalking	2, 100	1.83	.17	0.040
(R7) Burglary	2, 102	3.00	.05	0.060
(R8) Inappropriate content	2, 97	0.56	.57	0.010
(R9) Job application	2, 103	6.12	.003*	0.110

and (R9) *Job application* between the three use cases (see Table 4).

(R4) Possible Harm. Post-hoc tests using Sidak correction showed that the risk of possible harm was considered to be more severe in the smart home device than in the smart health device use case ($p<.05$).

(R9) Job Application. Post-hoc tests showed that the risk of worst chances regarding job applications was considered to be less severe regarding the use of OSN than smart home ($p<.05$) and smart health devices ($p<.01$).

There was no significant interaction effect between risk scenario and use case ($p>.05$).

4.3 Relationship Between Both Scales

The median values for perceived probability and severity are plotted in Figure 3 to display the relationship between both scales. Overall, participants indicated a higher probability for the abstract risk scenarios than for the specific ones. The specific risk scenarios, on the other hand, tend to be perceived as more severe, although worse chances for (R9) *Job applications* received lower values of perceived severity in the OSN and smart home use case, whereas restricted freedom of (R5) *Nutrition* choice and the publication of (R8) *Inappropriate content* were considered to be less severe or equal to the collection of data and usage patterns in the smart home devices use case.

In spite of these particular cases, the abstract and the specific risk scenarios seem to build two clusters, with the abstract ones, e.g., the collection of data being perceived as very likely but only of medium severity, and the specific ones ranging between medium and high severity, but at the same time are considered to be less likely than the abstract ones (see Figure 3). We conducted a hierarchical cluster analysis on the median values for likelihood and severity (using the Ward method and squared euclidean distance) to test this hypothesis and found two clusters for each use case, with cluster 1 including the abstract and cluster 2 the specific risk scenarios. Using Mann-Whitney-U-tests, we found that the clusters differed significantly in terms of likelihood and severity for all use cases ($p<.05$), except for likelihood in the OSN use case with $p=.19$. This finding provides some further insights into earlier work on risk perception and communication, which suggests that specific consequences of a risk should be communicated in order to increase people's perception of a risk [6, 55].

Regarding the median values, (R7) *Burglary* is perceived to be the most severe risk scenario in all use cases, but fails to exceed the 50% mark in probability. In contrast, (R6) *Stalking* related to the use of OSN and smart home devices is perceived as somewhat more likely, but at the same time less severe, except for the smart health devices use case. Figure 4 combines all use cases in one graph. Figure 5 displays the relationship between the scales using scatterplots, R^2 indicates the linear correlation between the two scales.

The MANOVA showed no significant interactions between the perceived probability and severity of the nine risk scenarios (with $p>.05$).

5 Discussion

We conducted a survey study with 942 German participants to investigate how lay users perceive different privacy risks associated with the use of common (OSN) and new technologies (smart home and smart health devices). In this section, we discuss what these results imply for future approaches of risk communication implemented in awareness campaigns or privacy interventions.

5.1 Abstract Privacy Risk Scenarios

The high values for perceived probability of the abstract risk scenarios are not surprising, as abstract risks like data collection comprise a large amount of possible scenarios and thus should carry a high probability. However, one could assume that all participants take the collection of their data for a fact when using technologies like OSN, smart home, and smart health devices.

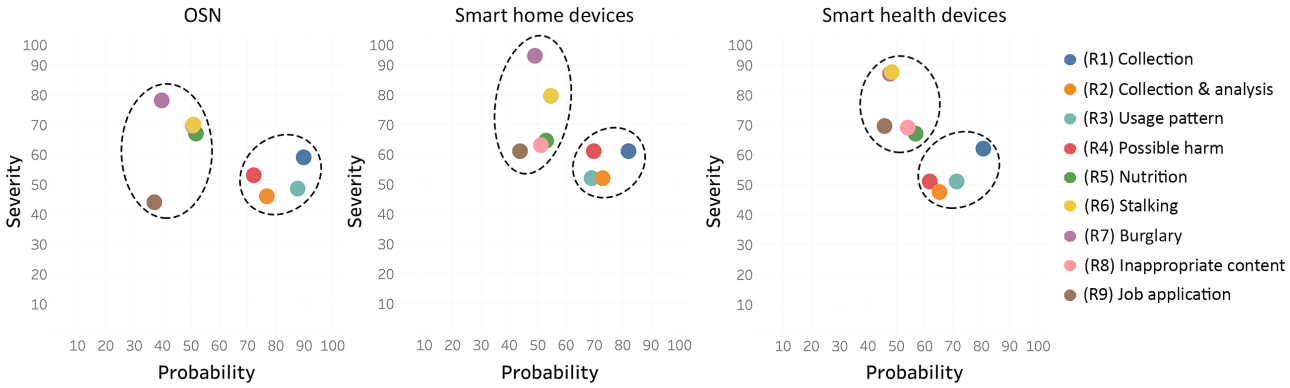

Fig. 3. Relationship between the probability and severity rating scale displayed separately for each use case.

Yet, the mean and median values for this risk scenario range between 75 and 90, implying that some lay users still think their data might not be collected.

Considering the lower values for perceived severity, lay users seem to not have specific risk scenarios or adverse consequences in mind when confronted with an abstract risk scenario. Moreover, the perceived severity does not increase notably when adding more information about the data processing, i.e., the analysis of the data and an explanation of usage patterns. Even when confronted with the possibility of personal harm due to data collection and analysis, lay users do not seem to consider serious consequences, probably because they lack the imagination of what their data could be used for. This is in line with previous research (e.g., [53]), which has shown that lay users are often not aware of specific privacy risks. Since privacy disclaimers generally only refer to the "collection and analysis" of data, lay users need to be made aware of specific adverse privacy risks in order to consider them in their risk evaluation and make an informed decision about using a technology or service. Otherwise, their evaluation will be biased regarding the severity of possible risks.

Most surprising are the results for the most abstract risk scenario (R1) *Collection*, which is rated as somewhat more severe than the other abstract risk scenarios, except for (R4) *Possible harm* in the smart home devices use case. As all of the other abstract risk scenarios also include a reference to data collection, these should at least reach equal values of perceived severity. A possible explanation for this seemingly paradoxical result might be the ubiquity of the "data collection" phrase in the media, which is usually linked to negative statements, leading to a "data collection is bad" heuristic. Likewise, people could feel obliged to judge "data collection" harshly to follow social norms.

Yet, people could actually be bothered by the extensive collection of data nowadays and thus believe data collection is in general a serious issue, without referring to the extent of harm that could result from this collection. The vague description also leaves more room for interpretation like the possibility of the technology's developer passing on the data to third parties, while the more concrete phrase "Your data are collected and analyzed" may imply that nothing further happens with the data. Finally, the well-known "collection" phrase might trigger an intuitive evaluation, whereas other expressions (analysis, a comprehensive explanation of usage patterns, possible harm) lead to a more thorough analysis of the possible risk and its severity. This is consistent to the dual-process theory [28], which has also been drawn on to explain the privacy paradox [1, 42] by stating that people sometimes judge intuitively when asked about their privacy concerns, and sometimes base their evaluation on rational cost-benefit analyses [45].

It could thus be a promising approach to combine the "collection" of data with specific privacy risk scenarios in order to increase users' privacy risk awareness.

5.2 Specific Privacy Risk Scenarios

When presented with a single particular specific privacy risk, lay users appraise it to be quite severe, but consider it to be an individual case which is not likely to apply to themselves. Renaud et al. [49] attribute this lack of problem awareness to the way people inform themselves, namely, by listening to stories told by others and their personal experience. Likewise, research has shown that media coverage of risks affects people's perception of how likely this risk is (a phenomenon also referred to as "availability heuristic" [7, 63]). Garg et al. [19] there-

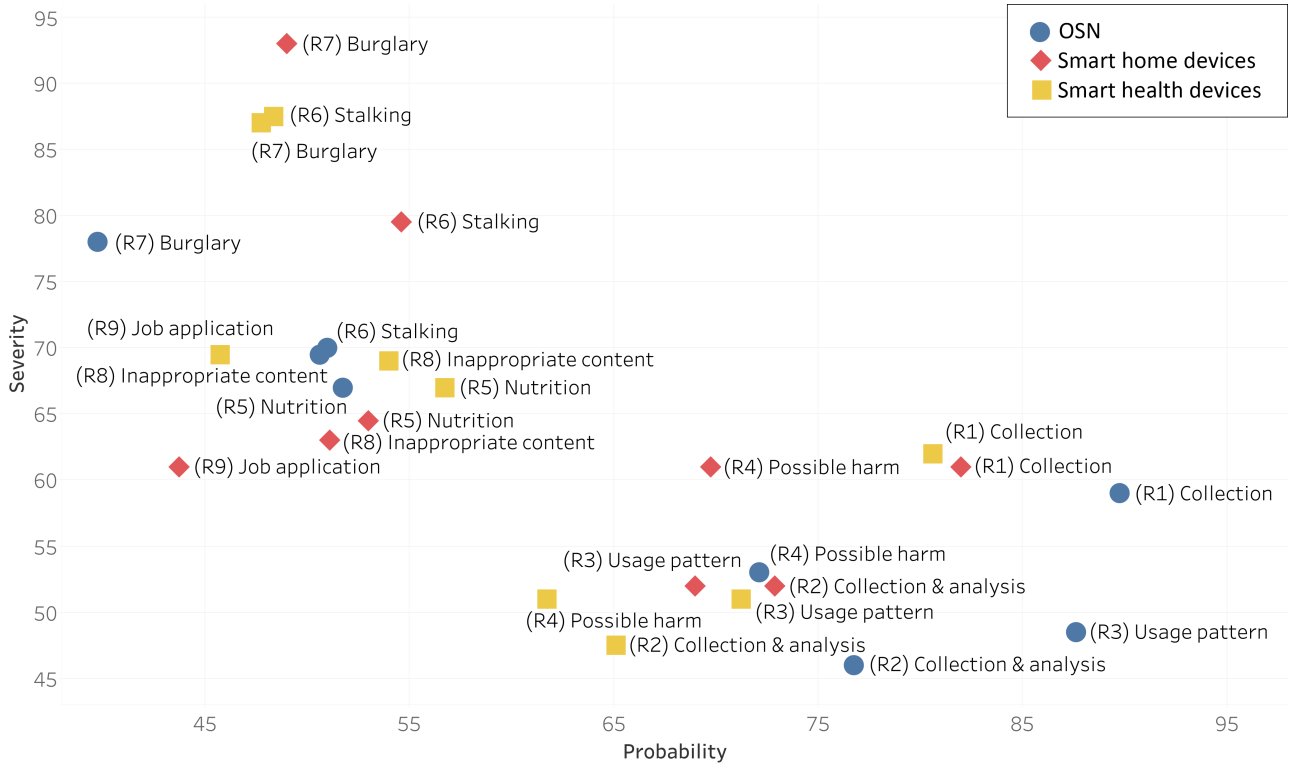

Fig. 4. Relationship between the probability and severity rating scale for all use cases combined.

fore suggest to include reports on privacy risks like job loss due to data sharing on Facebook in public campaigns in order to discourage users from sharing their information on Facebook. Besides the inclusion in public campaigns, this approach could also be implemented in interventions and trainings which aim to raise privacy awareness. A first attempt to this can be found at https://www.teachingprivacy.org, a privacy awareness project which includes media reports on privacy incidents in their lessons about privacy issues.

Taking a closer look on the risk evaluations for severity, our results suggest that risks with a physical safety component (stalking, burglary) are perceived to be most severe. This is in line with previous results [26]. The risk of burglaries is further associated with a financial loss, a circumstance which also contributed to high values of perceived severity in earlier survey studies [26, 34]. Another contributing factor could be that people's understanding of burglary should be rather similar, whereas the idea of restricted freedom in nutrition choice or the publication of inappropriate content probably differs to a greater extent between the participants. Hence, the consequences of burglary should be easier to grasp, whereas other risks relate to a multiplicity of consequences, with several of them being rather harmless.

In previous studies, career-related risks have been found to be among the top-rated risks (for job loss [54]), as well as being less serious than other risks (for not getting promoted [66]) or coming not as easily to mind as other risks [56]. According to our results, worse chances for job applications are also considered to be less severe than other risks in the OSN context.

Regarding probability, worse chances for job applications are perceived to be least likely in all three use cases. This is in line with the availability heuristic, which states that risks that are less present in people's mind are also considered to be less risky [63]. However, this finding could also be due to the fact that people think this risk does not apply to them, either because they are not looking for a new job at the moment and not planning to do so in the near future, or because they assume none of the content they share would worsen their chances in an application for a new job.

Contrary to earlier research [34], embarrassing content was not found to be more likely than other risks. However, our example described embarrassment due to identity theft, and thus also referred to impersonation, which may be considered as rather less likely.

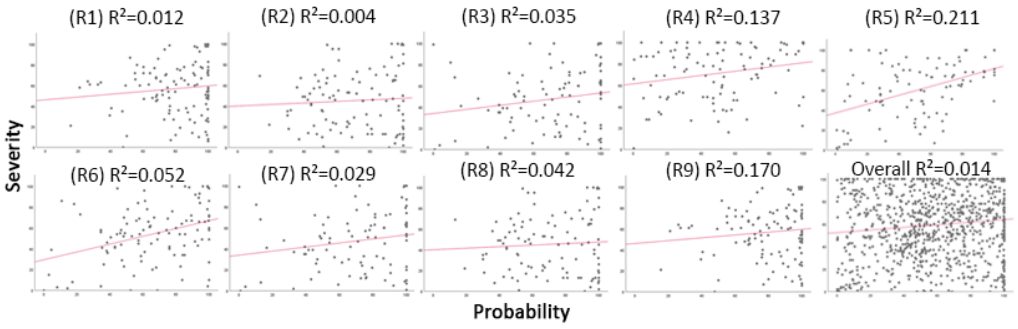

Fig. 5. Relationship between the probability and severity rating scale, depicted as scatterplots.

5.3 Use Cases

Earlier research indicates that the newness of a risk contributes to a higher risk perception and thus new technologies should be perceived to be more risky [15, 18], although there is also evidence for the opposite, with novel technologies being considered to be less risky [17]. In line with this, our descriptive results suggest that this relationship might be complicated: The abstract risk scenarios are considered to be more likely, but approximately equally severe when related to the use of a well-known technology (OSN) compared to two relatively new technologies (smart home and smart health devices). The specific risk scenarios, on the other hand, are considered to be equally likely, but less severe when associated to the use of OSN compared to the use of smart home and smart health devices. This implies that in some cases the differences in risk perceptions between new and common technologies might be reasoned in different perceptions of severity regarding specific risks, whereas in others people might be referring to differences in how likely an abstract risk is.

Our results provide some further insights into the severity perception of lay users. Actually, the severity perception should not differ between the considered use cases, as the severity of stalking, burglary or worse chances in job applications is supposed to be the same, regardless of what has caused them. As the severity evaluations differ between the three use cases, however, people seem to consider factors beneath the actual risk, e.g., to what extent a stalker or thief could benefit from the data shared in an OSN compared to those shared by using a smart health device.

(R6) *Stalking*, for example, is evaluated as most severe when related to the use of smart health devices. If a stalker gains access to the data collected with a fitness tracker which collects GPS data, s/he would have the possibility of tracking the user's location almost twenty-four-seven. Smart home devices, on the other hand, only provide information about whether the user is at home (or probably when s/he's going to come home or leave the apartment/house). OSN usually leave the decision about when and what content should be shared up to the user, so the publication of one's location can be controlled more easily when using OSN than the other two considered technologies and thus is attributed lower values of severity for stalking. The risk of burglaries, on the other hand, does not depend on the knowledge of one's location but only on the information about whether somebody is at home at a certain time. Accordingly, the perceived severity of this risk reaches nearly equal values for the use of smart home and smart health devices, but is considered as less severe when using OSN.

Overall, the abstract risks associated with using smart home devices are perceived as slightly more severe than those relating to the use of smart health devices or OSN. This could be due to the diverse functionalities of smart home devices. Since many people lack experience with this new and complicated technology, they might be uncertain what risks could actually arise from its usage, but feel like there is quite a great possibility for adverse consequences, as reflected in the high value of perceived severity for the "possible harm" risk scenario. Smart health devices, on the other hand, collect data that are easier to grasp (e.g., location, nutrition, physical activity) and are thus associated with higher severity concerning specific privacy risks. OSN, finally, provide other levels of control about what kind of data are shared when and with whom.

Hence, the data shared on OSN are less valuable for attackers and thus specific privacy risks relating to the use of OSN are rated as least severe. This also fulfills people's desire to control how they present themselves when others are watching [24].

5.4 Influence of Culture

The possible influence of cultural specifics should be kept in mind when drawing conclusions based on our results. There are a number of studies on cultural differences regarding privacy perception and behavior, with conflicting results regarding differences, for example, between German and US-American users. Whitman [65], argues that Europeans (and mainly German and French people) define privacy protection as the protection of their dignity, whereas US-Americans associate privacy with the freedom to manage their own life without interference from the government, especially in their home. Based on these considerations, the (R5) *Nutrition* scenario, in which participants are restricted in their choice of nutrition, should be more severe for US-Americans than for Germans. Since US-Americans also strongly demand to be left alone in their own home, they should also consider (R7) *Burglary* to be particularly severe. For Germans, on the other hand, those risk scenarios that imply a loss of face, such as the distribution of (R8) *Inappropriate content* should be considered as increasingly severe. Further studies are needed to determine whether the aforepostulated cross-cultural difference for those scenarios indeed holds.

Empirical results from other studies [33] indeed suggest that Germans consider the possibility of someone using their posts on social media to embarrass them to be considerably more severe than US-Americans, though this also holds true for their posts being used against them by somebody or being shared with third parties. On the contrary, US-Americans considered it somewhat more likely that the information will by used by someone to harm or embarrass them.

Concerning the general assessment of privacy risks, some researchers claim that Europeans might be less concerned about their privacy since the use of their data is closely protected by law – an effect that has already been demonstrated in a 2008 survey regarding the Safe Harbour Agreement [3] and should be strengthened with the introduction of the new GDPR in May 2018.

Yet others argue that Germans are more aware of potential consequences of data misuse, as the violation of strict European data protection laws usually come along with extensive coverage of this topic by the media [50]. In line with this, study results indicate that Germans are more worried about their privacy in OSN than US-Americans [29, 33]. Drawing on the seminal concept of Hofstede's cultural dimensions [27], Trepte et al. [61] show that Facebook users from countries with high values of uncertainty avoidance, such as Germany, place higher importance on the avoidance of privacy risks, as these are often unspecific and hard to grasp and, therefore, associated with uncertainty. An overview of cultural differences regarding privacy in social media is provided by Ur and Wang [64]. However, further research is needed to decide whether Europeans or US-Americans are more aware of and worried about privacy issues, or if they just pursue different concepts of privacy, as indicated by Whitman [65].

5.5 Implications for Risk Communication

The present study provides several insights for privacy researchers or activists who aim to raise lay users' awareness of privacy risks. First, neither abstract nor specific risk scenarios alone will succeed in raising people's privacy risk awareness, since the former are considered to be less severe and the latter to be less likely. Hence, a combination of different specific risk scenarios held together by the notion of data collection (as in R1) is needed in order to increase people's evaluation of how likely the described scenarios will occur. Introducing additional concepts like the analysis of data (as in R2), usage patterns (as in R3), and personal harm (as in R4) do not seem to add substantial value to the communication. Specific risk scenarios that are perceived to be most severe are those describing the possibility of financial loss (e.g., (R7) *Burglary*) or threats to one's physical safety (e.g., (R6) *Stalking*). Moreover, specific risk scenarios which leave little room for interpretation were considered to be more severe in our study and are thus most appropriate to increase people's severity perception. Yet, since specific risk scenarios do not apply to the same extent to all people, it might also be necessary to include several specific risk scenarios to address, for example, people whose nutrition is rather unhealthy, people who are currently looking for a new job and people whose nutrition is perfectly healthy or who are not going to look for a new job in the near future alike.

Second, the use case to which the risk communication refers to should also be taken into account. The more an attacker can benefit from the data provided by using a particular technology in order to harm the user in a specific risk scenario, the higher are the values for perceived severity and probability. Hence, which risk scenarios work best depends on which data are provided by the user and collected by the manufacturer or service in the considered use case. Third, whenever it is unclear which specific scenarios might fit the intended use case of a specific instance of risk communication or when-

ever the target population cannot be clearly specified, (R1) might be the best choice. Users perceived (R1) in all use cases as the most likely scenario. Furthermore, it was generally perceived as of medium severity and in all use cases achieved the highest severity rating found among the abstract scenarios. Last but not least, especially researchers should be aware that while cross-cultural influences in privacy risk communication are a logical extension of taking the use case into account, the field leaves many open questions.

5.6 Limitations and Future Work

Several limitations apply to our study. First, since we only included participants who currently lived in Germany, our results may not be generalizable to other cultures. However, we are currently planning to conduct a follow-up study with participants from other European countries to allow for comparison of the results across a wider range of cultural backgrounds. Second, we used a panel to recruit our participants, thus it is likely that our sample is biased in terms of age, academic background and technical expertise, as it might be younger, higher educated and overly tech-savvy. We do also not know how many and which participants dropped out before finishing the questionnaire due to technical restrictions of the clickworker panel. Third, we only considered a selection of possible privacy risks in three use cases. We aimed to include a mix of more and less obvious examples for the categories of privacy risks identified by Karwatzki et al. [30]. However, this might have biased our results, as more obvious examples could have lead to different evaluations of the risk scenarios. It would thus be worthwhile to conduct another follow-up study to check whether the results also apply to other risk scenarios and use cases. Forth, we applied a between-subject design. The results are expected to be (at least slightly) different if we had used a within-subject design. However, since one of our goals was to investigate how people perceive different privacy risks in the context of risk communication, we decided to show them only one risk scenario to evaluate their perception of these individual risks, independent of other potential risks, to allow for conclusions about whether the individual risk scenarios are appropriate for risk communication. Also, with a within-subject design, it would have been hard to prevent a bias due to sequence effects.

6 Conclusion

We investigated lay users' risk perception of different privacy threats that could arise from using OSN, smart home and smart health devices. Our results suggest that there might be two clusters of privacy risks, with abstract risks (e.g., collection and analysis of data) being evaluated as likely but only of mediocre severity. Specific privacy risks, like stalking or targeted burglary, on the other hand, reach higher values of perceived severity, but are perceived as less likely. As our participants consider the abstract risk scenarios to be less severe than the specific ones, it is possible that they are not aware of specific serious consequences that could result from data sharing. Hence, it is necessary to raise their awareness of specific privacy risks in order to enable an informed decision about using potentially privacy-threatening technologies. Yet, if confronted with particular specific privacy risks, lay users consider them to be less likely than the abstract ones. A possible solution could thus be to combine several risk scenarios and report on real world examples to increase the perceived probability of specific privacy risks. The present study further provides insights into the severity perception of lay users in general: Since specific risks, like stalking or burglary should be evaluated as equally severe across different usage contexts, lay users seem to take other factors into account when assessing the severity of privacy risks, e.g., how much a possible attacker could benefit from the data users provide when using the respective technologies. Hence, different use cases might call for different risk scenarios in terms of risk communication, with those risks scenarios which provide the best opportunity for an attacker to harm the user in a particular use case being most promising.

Acknowledgements

This paper is supported by European Union's Horizon 2020 research and innovation programme under grant agreement No 740923, project GHOST (Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control). This work was also supported by the German Federal Ministry of Education and Research in the Competence Center for Applied Security Technology (KASTEL).

7 Appendix

7.1 Results of the Pairwise Comparisons

Table 5. Results of the post-hoc tests regarding the comparison of perceived probability of the risk scenarios (DV) between the different risk scenarios (IV). A ↑ with the corresponding p-value indicates a significantly greater value of perceived probability for the risk scenarios (R1) – (R4) displayed in the horizontal rows than for the risk scenarios displayed in the columns.

		(R1) Collection	(R2) Collection & analysis	(R3) Usage patterns	(R4) Possible harm	(R5) Nutrition	(R6) Stalking	(R7) Burglary	(R8) Inappropriate content	(R9) Job application
OSN	(R1)					$< .001$ ↑	$< .001$ ↑	$< .001$ ↑	$< .001$ ↑	$< .001$ ↑
	(R2)					$< .001$ ↑	$= .003$ ↑	$< .001$ ↑	$= .003$ ↑	$< .001$ ↑
	(R3)					$< .001$ ↑	$< .001$ ↑	$< .001$ ↑	$< .001$ ↑	$< .001$ ↑
	(R4)					$= .015$ ↑		$< .001$ ↑		$= .004$ ↑
Smart home devices	(R1)					$< .001$ ↑	$= .001$ ↑	$< .001$ ↑	$< .001$ ↑	$< .001$ ↑
	(R2)							$= .005$ ↑		$< .001$ ↑
	(R3)	$= .045$ ↑								$= .02$ ↑
	(R4)							$= .007$ ↑		$< .001$ ↑
Smart health devices	(R1)						$= .001$ ↑	$= .001$ ↑	$= .044$ ↑	$< .001$ ↑
	(R2)						$= .029$ ↑	$= .047$ ↑		$= .015$ ↑
	(R3)									$= .031$ ↑
	(R4)									

Table 6. Results of the post-hoc tests regarding the comparison of perceived severity of the risk scenarios (DV) between the different risk scenarios (IV). A ↑ with the corresponding p-value indicates a significantly higher value of perceived severity for the risk scenarios (R5) – (R9) displayed in the horizontal rows than for the risk scenarios displayed in the columns.

		(R1) Collection	(R2) Collection & analysis	(R3) Usage patterns	(R4) Possible harm	(R5) Nutrition	(R6) Stalking	(R7) Burglary	(R8) Inappropriate content	(R9) Job application
OSN	(R5)									
	(R6)		$= .005$ ↑							$= .012$ ↑
	(R7)		$< .001$ ↑	$= .008$ ↑						$< .001$ ↑
	(R8)		$= .009$ ↑							$= .024$ ↑
	(R9)									
Smart home devices	(R5)									
	(R6)		$= .003$ ↑							
	(R7)	$= .009$ ↑	$< .001$ ↑	$< .001$ ↑	$< .032$ ↑				$= .019$ ↑	
	(R8)									
	(R9)									
Smart health devices	(R5)									
	(R6)		$= .001$ ↑	$< .001$ ↑	$= .001$ ↑					
	(R7)	$= .005$ ↑	$< .001$ ↑	$< .001$ ↑	$< .001$ ↑					
	(R8)									
	(R9)									

7.2 Results of the Item Analysis

The results of the item analysis are displayed in Table 7 for the pilot study and in Table 8 for the main study.

Table 7. Results of the item analysis for the pilot study. Cronbach's α for the probability scale=.977.

Item	Item-total correlation	Cronbach's α if item is left out
Prob_1	.962	.964
Prob_2	.961	.964
Prob_3	.880	.986
Prob_4	.963	.963

Table 8. Results of the item analysis for the main study. Cronbach's α for the probability scale=.936.

Item	Item-total correlation	Cronbach's α if item is left out
Prob_1	.871	.910
Prob_2	.910	.897
Prob_3	.786	.937
Prob_4	.837	.922

7.3 Survey Questionnaire

Welcome & Informed Consent

Dear participant, we are pleased that you are taking part in our study related to the use of digital services. Your opinion is very important to us. First, we ask you to answer some questions about your ownership of different devices and services. You will be given information about the devices and services we are going to use later in the study and you will be asked to provide an assessment on these devices. Then we will present you with a number of fictional cases and statements to which your consent or rejection is requested. The survey ends with a few demographic questions. This survey will take approximately 10 minutes to complete.

Please read the following text carefully before proceeding.

There will be no physical safety risks during the study. The responses you enter during the course of the study are recorded. Other than this, no data are collected. The recorded data are evaluated and further processed in the course of the data analysis and published in project reports. It will be impossible to trace the source of the information back to you. The study can be terminated at any time, without providing reasons and without any negative consequences. Your decision to approve the use, and dissemination, of your information is completely voluntary. However, if you do not give permission, it will not be possible for you to participate in the study and you will not receive the promised remuneration. You will receive 2.10€for your participation. You only have to sign to confirm receipt of the remuneration. An additional benefit is increased knowledge of security and applications within the "Internet of Things". By participating you will make a valuable contribution to our research.

By pressing the "I agree" button, you authorize us to use your answers and access them till the end of the project. Please note that you can withdraw the authorization at any time during the study. In that case, all your data will be deleted.

Technology Use

- Do you use social networks (e.g., Facebook, Xing, Google+)?
- Do you use smart home devices (e.g., a refrigerator that is connected to the internet, light that is controlled by movements, digital assistants like Alexa)?
- Do you use smart health devices (e.g., measuring devices for blood pressure connected to the internet, fall detectors, fitness tracker)?

Answer options: Yes, I often use [use case], Yes, I sometimes use [use case], I never use [use case] but I'd like to in the future, I never use [use case] and I don't like to in the future

Presentation of Use Case

Note: 1 out of 3 use cases is presented, it is randomized which participant is presented which use case.

OSN. A social network refers to an online service which allows users to share their opinions, experiences and information, and offers the opportunity to communication easily with other users. Social networks display relationships (e.g., friendships, acquaintanceships, etc.) between the users. Often, social networks focus on a particular context (e.g., professional or private). The advantages for users are the opportunity to effortlessly stay in touch with other users from the respective context (e.g., friends) and exchange news. Popular social networks are, for example, Facebook or Google+.

Smart Home Devices. 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 Devices. 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

Presentation of Risk Scenario

Note: 1 out of 9 risk scenarios is presented, it is randomized which participant is presented which risk scenario. See section 3.4 and 3.4 for the risk scenario texts.

Evaluation of Risk Scenario

- It is extremely likely that the situation described above will occur
- The chances of the situation described above occurring are great
- There is a good possibility that the situation above will occur
- I feel that the situation described above will occur

Scale: strongly disagree (1) to strongly agree (100)

- Assuming that the situation described above would occur, this would be...

Scale: innocuous (1) to extremely devastating (100)

Privacy Concerns

[Items taken from the IUIPC questionnaire's global information privacy concern scale [38]]

Demographics

- Gender: male, female, other
- Age: <20, 20–25, 26–35, 36–45, 46–55, 56–65, 66–75, 76–85, >85
- Profession / course of study:
- How many years have you been working in the field of IT security, e.g., as a student, researcher or practitioner?

End

Thank you very much for your participation! We would like to thank you very much for your help. If you have any questions about the study, please send an e-mail to nina.gerber@kit.edu. Your confirmation code is [...]. Your answers have been saved and you can now close the browser window.

7.4 Availability of Data

Anyone who is interested in receiving the (anonymized) data should feel free to contact us at any time.

References

[1] A. Acquisti and J. Grossklags. Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[2] Angeliki Aktypi, Jason R.C. Nurse, and Michael Goldsmith. Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In *Proceedings of the 2017 on Multimedia Privacy and Security (MPS)*, pages 1–11, New York, NY, USA, 2017. ACM.

[3] Annie I. Antón, Julia B. Earp, and Jessica D. Young. How Internet Users' Privacy Concerns Have Evolved Since 2002. *IEEE Security & Privacy*, 8(1):21–27, 2010.

[4] Gökhan Bal, Kai Rannenberg, and Jason I. Hong. Styx: Privacy risk communication for the android smartphone platform based on apps' data-access behavior patterns. *Computers & Security*, 53:187–202, 2015.

[5] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, and A. Seeam. Pervasive eHealth services a security and privacy risk awareness survey. In *Proceedings of the International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, London, UK, 2016.

[6] Ann Bostrom, Cynthia J Atman, Baruch Fischhoff, and M Granger Morgan. Evaluating risk communications: completing and correcting mental models of hazardous processes, Part II. *Risk Analysis*, 14(5):789–798, 1994.

[7] William Bottom, Thomas Gilovich, Dale Griffin, and Daniel Kahneman. Heuristics and Biases: The Psychology of Intuitive Judgment. *The Academy of Management Review*, 29, 2004.

[8] Carole Cadwalladr. 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower. https:

//www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump. Accessed: 2019-03-12.

[9] L. J. Camp. Mental models of privacy and security. *IEEE Technology and Society Magazine*, 28(3):37–46, 2009.

[10] Pew Research Center. Public Perceptions of Privacy and Security in the Post-Snowden Era. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/. Accessed: 2019-03-11.

[11] clickworker GmbH. clickworker panel. https://www.clickworker.com/. Accessed: 2017-09-20.

[12] Xuefei Deng, Robert D. Galliers, and Kshiti D. Joshi. Crowdworking - a New Digital Divide? Is Design and Research Implications. In *Proceedings of the 2016 European Conference on Information Systems (ECIS)*, Istanbul, Turkey, 2016.

[13] C. Digmayer and E. Jakobs. Risk perception of complex technology innovations: Perspectives of experts and laymen. In *2016 IEEE International Professional Communication Conference (IPCC)*, Austin, TX, USA, 2016. IEEE.

[14] eMarketer. Number of social network users worldwide from 2010 to 2021 (in billions). https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/. Accessed: 2019-03-12.

[15] Fariborz Farahmand and Eugene H. Spafford. Understanding insiders: An analysis of risk-taking behavior. *Information Systems Frontiers*, 15(1):5–15, 2013.

[16] Baruch Fischhoff, Paul Slovic, Sarah Lichtenstein, Stephen Read, and Barbara Combs. How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, 9(2):127–152, 1978.

[17] Batya Friedman, David Hurley, Daniel C. Howe, Helen Nissenbaum, and Edward Felten. Users' Conceptions of Risks and Harms on the Web: A Comparative Study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, pages 614–615, New York, NY, USA, 2002. ACM.

[18] V. Garg and J. Camp. End User Perception of Online Risk under Uncertainty. In *Proceedings of the 45th Hawaii International Conference on System Sciences (HICCS)*, pages 3278–3287, Maui, HI, USA, 2012. IEEE.

[19] V. Garg and J. Camp. Heuristics and Biases: Implications for Security Design. *IEEE Technology and Society Magazine*, 32(1):73–79, 2013.

[20] Vaibhav Garg, Kevin Benton, and L. Jean Camp. The Privacy Paradox: A Facebook Case Study. In *Proceedings of the 42nd Research Conference on Communication, Information and Internet Policy*, Arlington, VA, USA, 2014.

[21] Vaibhav Garg, L. Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber. Risk Communication Design: Video vs. Text. In Simone Fischer-Hübner and Matthew Wright, editors, *Privacy Enhancing Technologies (PETS 2012). Lecture Notes in Computer Science, vol 7384*, pages 279–298, 2012.

[22] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats. In *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP)*, Baltimore, MD, USA, 2018. USENIX Association.

[23] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. Exploring Consumers' Attitudes of Smart TV Related Privacy Risks. In Theo Tryfonas, editor, *Human Aspects of Information Security, Privacy and Trust (HAS). Lecture Notes in Computer Science, vol 10292*, pages 656–674. Springer, Cham, 2017.

[24] E. Goffman. *The Presentation of Self in Everyday Life*. Anchor Books/Doubleday, 1999.

[25] Darien Graham-Smith. How to escape the online spies. https://www.theguardian.com/technology/2017/may/13/how-to-get-privacy-digital-life-data-monitoring-gathering-amazon-facebook-google, 2018. Accessed: 2019-03-12.

[26] M. Harbach, S. Fahl, and M. Smith. Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In *Proceedings of the IEEE 27th Computer Security Foundations Symposium (CSF)*, pages 97–110, Vienna, Austria, 2014. IEEE.

[27] Geert H. Hofstede. *Cultures and organizations: Software of the mind*. McGraw-Hill, London and New York, 1991.

[28] Daniel Kahneman. A Perspective on Judgment and Choice: Mapping Bounded Rationality. *The American psychologist*, 58:697–720, 2003.

[29] Katherine Karl, Joy Peluchette, and Christopher Schlaegel. Who's Posting Facebook Faux Pas? A Cross-Cultural Examination of Personality Differences. *International Journal of Selection and Assessment*, 18(2):174–186, 2010.

[30] 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*, 26(6):688–715, 2017.

[31] Jennifer King and Andrew McDiarmid. Where's The Beep? Security, Privacy, and User Misunderstandings of RFID. In *Proceedings of Usability, Security, and Psychology (UPSEC)*, San Francisco, CA, USA, 2008. USENIX Association.

[32] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. "When I Am on Wi-Fi, I Am Fearless": Privacy Concerns & Practices in Everyday Wi-Fi Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 1993–2002, New York, NY, USA, 2009. ACM.

[33] H. Krasnova and N. F. Veltri. Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. In *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences (HICSS)*, Honolulu, HI, USA, 2010. IEEE.

[34] D. LeBlanc and R. Biddle. Risk perception of internet-related activities. In *Proceedings of the Tenth Annual International Conference on Privacy, Security and Trust (PST)*, pages 88–95, Paris, France, 2012. IEEE.

[35] D. J. Leiner. SoSci Survey (Version 2.5.00-i). https://www.soscisurvey.de/, 2017. Accessed: 2017-09-20.

[36] Huigang Liang and Yajiong Xue. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, 11(7):394–413, 2010.

[37] Ragnar Löfstedt and Åsa Boholm. The study of risk in the 21st century. In *The Earthscan Reader on Risk*, pages 1–23. Earthscan, 2009.

[38] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet Users' Information Privacy Concerns (IUIPC): The

Construct, the Scale, and a Causal Model. *Information systems research*, 15(4):336–355, 2004.

[39] BBC News. Edward Snowden: Leaks that exposed US spy programme. http://www.bbc.com/news/world-us-canada-23123964, 2014. Accessed: 2019-03-12.

[40] BBC News. Facebook to exclude billions from European privacy laws. http://www.bbc.com/news/technology-43822184, 2018. Accessed: 2019-03-12.

[41] Helen Nissenbaum. Privacy As Contextual Integrity. *Washington Law Review*, 79, 2004.

[42] P. A. Norberg, D. R. Horne, and D. A Horne. The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, 41(1):100–126, 2007.

[43] Isabelle Oomen and Ronald Leenes. Privacy Risk Perceptions and Privacy Protection Strategies. In Elisabeth de Leeuw, Simone Fischer-Hübner, Jimmy Tseng, and John Borking, editors, *Policies and Research in Identity Management*, pages 121–138, 2008.

[44] George Packer. Can You Keep a Secret? The former C.I.A. chief Michael Hayden on torture and transparency. https://www.newyorker.com/magazine/2016/03/07/michael-hayden-comes-out-of-the-shadows, 2016. Accessed: 2019-03-12.

[45] Chanda Phelan, Cliff Lampe, and Paul Resnick. It's Creepy, But It Doesn't Bother Me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI)*, pages 5240–5251, New York, NY, USA, 2016. ACM.

[46] Eduardo Porter. The Facebook Fallacy: Privacy Is Up to You. https://www.nytimes.com/2018/04/24/business/economy/facebook-privacy.html, 2018. Accessed: 2019-03-12.

[47] Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden. Anonymity, Privacy, and Security Online. http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/#. Accessed: 2019-03-12.

[48] Ulf-Dietrich Reips and Frederik Funke. Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator. *Behavior Research Methods*, 40(3):699–704, 2008.

[49] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why Doesn't Jane Protect Her Privacy? In Emiliano De Cristofaro and Steven J. Murdoch, editors, *Privacy Enhancing Technologies (PETS 2014). Lecture Notes in Computer Science, vol 8555*, pages 244–262, 2014.

[50] Carsten Röcker. Information Privacy in Smart Office Environments: A Cross-Cultural Study Analyzing the Willingness of Users to Share Context Information. In David Taniar, Osvaldo Gervasi, Beniamino Murgante, Eric Pardede, and Bernady O. Apduhan, editors, *Computational Science and Its Applications – ICCSA 2010. Lecture Notes in Computer Science, vol 6019*, pages 93–106, Berlin, Heidelberg, 2010. Springer.

[51] Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr. How Trump Consultants Exploited the Facebook Data of Millions. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Accessed: 2019-03-12.

[52] Bruce Schneier. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Springer-Verlag, Berlin, Heidelberg, 2003.

[53] Fatemeh Shirazi and Melanie Volkamer. What Deters Jane from Preventing Identification and Tracking on the Web? In *Proceedings of the 13th Workshop on Privacy in the Electronic Society (WPES)*, pages 107–116, Scottsdale, Arizona, USA, 2014. ACM.

[54] Michael Warren Skirpan, Tom Yeh, and Casey Fiesler. What's at Stake: Characterizing Risk Perceptions of Emerging Technologies. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI)*, pages 70:1–70:12, New York, NY, USA, 2018. ACM.

[55] Paul Slovic. Informing and Educating the Public About Risk. *Risk Analysis*, 6(4):403–415, 1986.

[56] Jessica Staddon, David Huffaker, Larkin Brown, and Aaron Sedley. Are Privacy Concerns a Turn-off?: Engagement and Privacy in Social Networks. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS)*, pages 10:1–10:13, New York, NY, USA, 2012. ACM.

[57] Chauncey Starr. Social Benefit versus Technological Risk. *Science*, 165(3899):1232–1238, 1969.

[58] Yao-Ting Sung and Jeng-Shin Wu. The Visual Analogue Scale for Rating, Ranking and Paired-Comparison (VAS-RRP): A new technique for psychological measurement. *Behavior Research Methods*, 50(4):1694–1715, 2018.

[59] Symantec. State of Privacy Report 2015. Technical report, Symantec, 2015.

[60] Nitasha Tiku. Facebook Is Steering Users Away From Privacy Protections. https://www.wired.com/story/facebook-is-steering-users-away-from-privacy-protections/?mbid=BottomRelatedStories, 2018. Accessed: 2019-03-12.

[61] Sabine Trepte, Leonard Reinecke, Nicole B. Ellison, Oliver Quiring, Mike Z. Yao, and Marc Ziegele. A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society*, 3(1), 2017.

[62] Monique Turner, Christine Skubisz, and Rajiv Rimal. Theory and practice in risk communication: A review of the literature and visions for the future. In Teresa L. Thompson, Roxanne Parrott, and Jon F. Nussbaum, editors, *Handbook of Health Communication (2. ed.)*, pages 146–164. Routledge, 2011.

[63] Amos Tversky and Daniel Kahneman. Judgment under Uncertainty: Heuristics and Biases. *Science*, 185(4157):1124–1131, 1974.

[64] Blase Ur and Yang Wang. A Cross-cultural Framework for Protecting User Privacy in Online Social Media. In *Proceedings of the 22nd International Conference on World Wide Web (WWW)*, pages 755–762, New York, NY, USA, 2013. ACM.

[65] James Q. Whitman. The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal*, 113, 2004.

[66] Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Laura Brandimarte, and Alessandro Acquisti. Would a Privacy Fundamentalist Sell Their DNA for $1000...If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS)*, pages 1–18, Menlo Park, CA, USA, 2014. USENIX Association.

[67] Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security and Privacy Concerns with Smart Homes. In

Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS), pages 65–80, Santa Clara, CA, USA, 2017. USENIX Association.

[68] Pei Zhang and A. Jetter. Understanding risk perception using Fuzzy Cognitive Maps. In *Proceedings of the 2016 Portland International Conference on Management of Engineering and Technology (PICMET)*, pages 606–622, Honolulu, HI, USA, 2016. IEEE.