2019 IEEE European Symposium on Security and Privacy Workshops

Why Johnny Fails to Protect his Privacy

1st Nina Gerber
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
nina.gerber@kit.edu

2nd Verena Zimmermann
FAI
Technische Universität Darmstadt
Darmstadt, Germany
zimmermann@psychologie.tu-darmstadt.de

3rd Melanie Volkamer
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
melanie.volkamer@kit.edu

***Abstract*—Albeit people worldwide cry out for the protection of their privacy, they often fail to successfully protect their private data. Possible reasons for this failure that have been identified in previous research include a lack of knowledge about possible privacy consequences, the negative outcome of a rational cost-benefit analysis, and insufficient ability for protection on the users' side. However, these findings mainly base on theoretical considerations or results from quantitative studies, and no comprehensive explanation for users' privacy behavior has been found so far. We thus conducted an interview study with 24 participants to qualitatively investigate what are (1) users' mental models of privacy consequences, (2) obstacles for privacy protection, and (3) strategies for privacy protection. Our results provide evidence for all possible explanations: We find that most of our participants are indeed unaware of most consequences that could result from not protecting their privacy besides personalized advertisement and financial loss. We also identify several obstacles for privacy protection, such as protection being too much effort, too complicated, users lacking knowledge, or social aspects. Protection strategies mostly base on reducing the amount of data disclosed and most users refrain from using advanced PETs. We further identified additional factors which influence whether people adopt measures to protect their privacy and propose a model which subsumes all factors that are relevant for people's decision to apply protection measures.**

***Index Terms*—Privacy protection, Interviews, Privacy paradox, Privacy consequences, Protection obstacles**

I. Introduction

Albeit the ever evolving opportunities of smart technical devices offer many benefits in terms of convenience nowadays, they also come along with an overwhelming omnipresence of data capturing. It is therefore not surprising the majority of US-American adults (91%) think that consumers have lost control over how personal information is collected and used by companies [1] and half of the US-American Internet users worry about the amount of information available about them online [2]. Similar numbers apply for European, Asian, African and South American users [3]–[5]. It could therefore be concluded that privacy is a major issue for users worldwide and a considerable amount of users should make certain efforts to protect their private data.

However, if we take a closer look at most people's daily handling of their private data, we often find that this is not the case [3], [6]. Indeed, in many cases do people not only voluntarily give away these personal data by posting details of their private life in social networks or using fitness trackers and online shopping websites which include profiling functions, but also rarely make an effort to protect their data actively, for example through the deletion of cookies on a regular basis or the encryption of their email communication. But why is it that they fail to successfully protect their data?

This phenomenon is well known among privacy researchers and often referred to as "privacy paradox" [7]–[9]. It has been argued that people simply lack awareness of privacy threats which leads to their unconcerned handling of private data [10]. This is in line with threat avoidance theory, which states that in order to be motivated to avoid a threat in the IT context, people have to perceive this threat as malicious, i.e., that they are susceptible to this threat and that the negative consequences will be severe [11]. Our first research question thus is: **What are people's mental models of possible consequences arising from not protecting their privacy?**

Several other explanations for the privacy paradox have been proposed so far, one of the most popular being the weighting up of costs and benefits ("privacy calculus") [12], including social pressure [13]. We therefore aim to gain an understanding of what users consider to be the costs of privacy protection and benefits of using privacy-threatening devices and services by answering the following research question: **What are obstacles for privacy protection and for what reasons do people still use privacy-threatening devices and services?**

Other explanations suggest that people are aware of privacy problems and motivated to encounter them, but fail to do so because they lack knowledge about protection mechanisms (e.g., the Tor software or encryption tools) [14] or they suffer from an "illusion of control" when dealing with the privacy of their data [15]. In line with that, prior studies showed that people indeed seem to confuse the control over the publication of information with the control over the assessment of that information by third parties. According to this hypothesis, the paradoxical behavior is caused by the false feeling of control over the further usage of personal data, which occurs if users can initially decide over the publication of it (e.g., by posting in online social networks (OSN) and managing the privacy settings for the post). Hence, to investigate whether users simply lack knowledge about possible protection solutions or whether they apply strategies which are not effective but mainly make them feel like they have control over their data, we propose the third research question as follows: **What strategies do people apply to protect their data?**

DOI 10.1109/EuroSPW.2019.00019

The explanations proposed so far by other researchers either base on theoretical considerations or on empirical results from - often quantitative - studies, examining one or several aspects of people's privacy attitude and behavior. Despite the significant number of studies conducted in this filed, no comprehensive explanation has been found so far and user privacy remains a rather complex phenomenon that cannot be entirely explained yet [16]. The present study therefore aims to shed light on users' privacy beliefs and behavior by investigating how they protect their privacy, what are obstacles for privacy protection or reasons for still using privacy threatening services and devices, and what are their mental models of possible consequences arising from not protecting their privacy. To this end, we conducted semi-structured interviews with 24 participants.

We find that our participants are indeed unaware of most consequences that could result from data sharing and collection. Whereas nearly all mention personalized advertisement as a possible consequence, only half of our participants refer to the possibility of financial loss. Although other consequences are mentioned (e.g., spam mails, criminal and political prosecution, propaganda, safety threats, identity theft, or less favorable insurance tariffs), only very few participants were able to provide more than two or three consequences. We can therefore conclude that most people seem to be unaware of the rich set of possible consequences of data sharing and collection. Our participants mentioned several protection obstacles, such as protection being too much effort or too complicated, lacking knowledge about protection measures, social aspects, and ethical considerations. The most common reasons provided for still using privacy threatening services were social pressure and the desire to stay or keep others up to date. Other reasons include convenience and the wish to express and spread one's opinion. However, several participants reported to deploy certain protection strategies nonetheless, with most of them relating to the reduction of data disclosed, either by not using a particular service, not sharing certain types of data or limiting the amount of recipients.

II. Related Work

Our work relates to people's mental models of privacy consequences, obstacles for privacy protection, including reasons for continuing to use privacy-threatening devices and services, and strategies people apply to protect their privacy.

A. Mental models of privacy consequences

There are many surveys assessing how people perceive different privacy risks, however, most of them present a set of risks and ask participants to rate their degree of concerns on a scale [17]–[20]. This approach is not sufficient to measure whether people are actually aware of these privacy risks without prompting them. Among the few who deployed a different approach are Harbach, Fahl and Smith [21], who asked German students and members of Amazon Mechanical Turk to name IT security and privacy risks and consequences in a survey. They found that participants usually overestimated the amount of risks they were aware of. This is in line with other studies, e.g., interviews conducted by Wash [22], which indicate that people are often not aware of threats and hence underestimate dangers. The consequence most frequently provided by both groups of participants in Harbach et al.'s study was financial loss, whereas the most salient risks were malware, hackers and the theft of account credentials.

The most comprehensive approach to accessing people's awareness of privacy consequences was conducted by Karwatzki et al. [23], who 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 on people's awareness of privacy consequences, Karwatzki et al. do not report the frequency of consequences mentioned in the different categories. Moreover, their participants mostly referred to consequences that could arise from using OSN. It is thus questionable which of their findings are application-specific and which generalize to other online services and technologies.

Other examples of assessing people's awareness of privacy risks are interviews conducted by Friedman et al. [24], who found that people were concerned about risks to their information and especially their privacy, but did not further specify these privacy risks, a survey on security and privacy risks of eHealth wearables [25], interviews combined with a field study concerning the risks of WiFi use [26], a comprehensive study on user regrets regarding Facebook posts [27], a survey assessing perceived risks of using mobile devices to conduct online transactions [28], and surveys and interviews concerning risks of cloud storage [29]. Shirazi and Volkamer [30] conducted interviews with 20 people on identification and tracking on the web, and found that their participants most often mentioned personalized advertising as a possible consequence, which some of them even considered to be beneficial. Melicher et al. [31] found that participants in their interview study were less comfortable with hidden outcomes of online tracking (e.g., price discrimination) than with more overt consequences (e.g., targeted advertisement). Although investigating specific privacy risks, Melicher et al. focused on online tracking and thus considered mainly risks specific to this application.

B. Obstacles for privacy protection

A few qualitative studies have been conducted on what obstacles users face when aiming to protect their privacy in several contexts. Shirazi and Volkamer [30], for example, conducted interviews with 20 people, most of them lay users, to investigate why most people do not use tools to protect themselves against identification and tracking on the web. They identified seven different explanations: (1) people mainly worry about privacy issues other than identification and tracking, (2) people are not aware of the assessment of meta-data, (3) people are not aware of the possibility to use meta-data for identification and tracking, (4) people are not concerned

because of several misconceptions such as being not aware of consequences or the feeling that they have nothing to hide, (5) people are not aware of protection tools, (6) people are not able to use protection tools properly, (7) people become side-tracked. Renaud, Volkamer and Renkema-Padmos [32] combined semi-structured interviews, a survey, and a literature review to identify obstacles to the adoption of end-to-end (E2E) encrypted email. Their final list of seven explanations includes lack of awareness, concern, and knowledge about how to protect oneself, as well as misconceptions of how to protect oneself, no perceived need to act, inability to use E2E encryption and becoming side-tracked. In a more recent study, Abu-Salma et al. [33] interviewed sixty users of different communication tools to identify factors that influence the adoption of secure messaging tools. Like Renaud et al. [32], they found that usability is not the major obstacle for the adoption of secure communication tools. In the messaging context, other factors like fragmented user bases, along with interoperability of the different messaging services are significant adoption obstacles. Participants also reported not to use a communication tool if they evaluate its message and voice call functionality to be of low quality.

C. Strategies for protecting one's privacy

Several studies have been conducted on how people protect their privacy by deploying a set of strategies. Most of these studies focus on a particular context, e.g., managing photos which are shared with other people [34], managing privacy in OSN in general [35], [36] or with respect to others revealing information about oneself [37], or when using WiFi [26]. Other studies describe strategies people deploy to address specific problems, e.g., identity theft [38], or online harassment [39]. Further, there are also studies dealing with a specific protection strategy, like webcam covering [40], or lying for privacy reasons [41].

A few studies focus on the general deployment of privacy protection strategies. Oomen and Leenes [17] differ between three sets of privacy protection strategies: (1) behavioral, such as providing incorrect information, using anonymous email addresses or pseudonyms, (2) employment of security measures and use of PETs, such as spam filters, firewalls, and anti spyware, and (3) use of more advanced PETs, such as encryption tools, anonymous remailers, trust certificates, and cookie crunchers. In a survey with Dutch students, they found that about half of their participants employed behavioral protection strategies, whereas the majority (between 74 and 89%) took standard security measures and used PETs, and about a third used some of the more advanced protection strategies, with trust certificates being the most (31%) and anonymisers (3%) the least frequently used.

In a lab study with corresponding interviews, Coles-Kemp and Kani-Zabihi [42] found that in an online registration task, when participants where not comfortable providing their information, most of them chose to give false information, discontinue with the registration or continue the registration and provide accurate information, but reduce their engagement with the service. In their interview study, Abu-Salma et al. [33] also asked their participants about strategies they applied if they wanted to protect their communication data. The most common strategy was to deliver sensitive information in person, or using video-chat and voice-mails if a personal meeting was not possible. Other practices include sending information by post, using a foreign language for voice messages, and cutting a message into several chunks which were then send via different communication channels. Some participants also reported to use a "code" to exchange sensitive information with others, regardless of the communication channel used.

A number of studies have dealt with the deployment of different privacy protection strategies by Facebook users. Young and Quan-Haase [43] found that university students mainly adopted privacy protection strategies that restricted access to their personal data for different members of the Facebook community, rather than strategies that would allow them to control data access for third parties. Furthermore, they showed that university students do not use fictitious information as protection strategy, since this would lead to confusion among friends and peers. Another study by Staddon, Acquisti and LeFevre [44] showed that users who value privacy features most generally show more privacy actions such as not providing certain information, limiting post visibility or deleting posts. Concerning cultural differences, the results of Peters, Winschiers-Theophilus and Mennecke [45] indicate that US users would rather remove friends from their contact list than change their privacy settings to restrict the visibility of their data, whereas Namibian users refuse from the deletion of friends due to the concern of being rude. When it comes to teenagers, Feng and Xie [46] found that older teenagers tend to implement more privacy protection strategies (e.g., deleting someone from their friends list, deleting older posts), whereas Litt [47] showed that younger adults are more likely to show a wider use of technological privacy tools than older adults, maybe due to greater knowledge of and skills in using these technologies. Using interviews, user diaries and surveys, Wang et al. [27] identified three different sets of protection strategies, namely proactive (e.g., rejecting friend requests, managing privacy settings), in-situ (e.g., self-censoring), and reactive (e.g., deleting content, untagging photos), with the last being the most frequently used strategy in their study.

III. Methodology

We conducted an exploratory study consisting of semi-structured interviews with 24 participants and subsequent qualitative analysis to evaluate their mental models of privacy consequences, obstacles for privacy protection, and protection strategies. The interviews were conducted in German, questions and quotations were translated for this paper.

A. Recruitment and Enrollment

We aimed for a heterogeneous sample, i.e., interviewing people with different professional and sociodemographical backgrounds, experiences, and expertise regarding online privacy. Therefore, we asked our student research assistants to

invite friends and family members of whom they thought would be interested in participating in our study. These were then contacted to make an appointment without telling them about the research topic. Instead, they were told the interviews would focus on their "use of digital applications". Additionally, we send a corresponding invitation email via the mailing list used to advertise studies among our university's undergraduate psychology students. We proceeded to recruit new participants until data saturation was reached, i.e., there came no new themes up during the interviews. Undergraduate students received course credits for participating, however, non-student participants did not receive any compensation but participated voluntarily. We conducted several pilot interviews to check the soundness of the questions and structure of the interview guidelines. Based on the feedback of the participants and our own impression during these pilot interviews, we improved the interview guidelines iteratively.

B. Study design

The interview guidelines can be accessed at https://secuso.aifb.kit.edu/english/889.php. The interviews took between 27 and 91 minutes, with an average of 48, and comprised the following sections:

1) Welcome and general instructions: First, participants were welcomed and informed about the study procedure and purpose[1]. They were further informed about the study conditions (see section III-D) and asked whether they consented to the recording of their interview.

2) Use of digital communication channels: In the first part of the interview, participants were asked to explain how they used technology, i.e., hard- and software, to communicate with other people. We did not ask actively about privacy, but if participants mentioned privacy-related issues on their own, we encouraged them to explain these in more detail.

3) Use of privacy-relevant applications and services: Afterwards, we asked participants whether they used (and if yes, which) OSN, messengers, navigation apps, shopping apps, cloud services, online banking, electronic pay services, loyalty programs, digital assistants, and game consoles. We further asked whether they owned a smart TV and whether they had already gotten the new version of the German ID card. Again, we did not ask about privacy issues actively, but encouraged participants to talk about their privacy beliefs if they had mentioned them first. Where applicable, we asked participants to justify their decisions not to use certain applications or products.

4) Data privacy attitude and behavior: The final part focused on participants' privacy beliefs and behavior. We asked them about their attitude towards data privacy, what their social and professional environment thought about data privacy, how they experienced the media coverage of this topic and what they thought about personalized services like Amazon's product recommendations. They were asked to explain which negative consequences could possibly arise from data sharing and whether they had already experienced such consequences in the past.

[1]Note that in order not to bias participants towards privacy, we told them the interview topic would be their use of digital applications instead of telling them we were interested in their privacy beliefs and behavior.

C. Participants

The interview group consisted of 24 participants (15 female, 9 male). Participants ranged between 17 and 53 years of age (M=26.29, SD=6.90). Nineteen participants were students, the other five participants' professional backgrounds included online journalist, event manager, office clerk, media manager, and researcher. None of the participants had a professional background in the computer sciences.

D. Ethical considerations

Ethical requirements for research involving human participants are provided by an ethics commission at our university. All relevant ethical requirements regarding research with personal data were met. Participants were informed about the procedure of the study, after which they could decide to proceed or stop the interview. They were told that they could stop the interview at any time without stating reasons and in this case all data collected so far would be deleted. We further assured them that the collected data would only be used for research purposes, their identity would not be linked to their responses, and their data would only be handled by members of our research group and never passed on to third parties.

E. Evaluation methodology

We used open coding [48], [49] for the analysis to account for the exploratory nature of our study. Thus, we were able to only consider such themes and issues that were highly relevant for our participants, which had not been possible by using pre-defined codings. First, we reviewed the transcripts and audio files to identify relevant themes and sub-categories from the participants' responses. Our final codebook included four meta themes and 31 sub-categories. Based on these, two authors independently coded all transcripts. Differences in the coding were solved through discussion afterwards. We report the number of participants who mentioned a theme or sub-category in the following section. Where applicable, we add (translated) quotes.

IV. Results

In this section, the results of the data analysis are presented. RQ1 is addressed in section IV-A, RQ2 in section IV-B, and RQ3 in section IV-C. Section IV-D describes additional findings about common privacy misconceptions. Where applicable, we provide the corresponding number of participants who made a statement and add the quotes from the participants that we translated from German.

A. Mental model of privacy consequences

A few participants (7) thought even if they provided all their data, nothing bad would happen at all: "Well, many people are pretty skeptical and say they don't want to be under surveillance in any case [...] and make a huge scandal out of it. I can't really understand why...on the one hand I think I

feel a bit...almost threatened, if some data of me is found, but then I have...because at the moment I lack the idea of how you could use this against me, that's why." (P9)

1) Personalized advertisement: Almost all participants (20) mentioned that they would be shown or sent personalized advertisement as a possible consequence of disclosing data. Most participants did not like the idea of receiving personalized ads, but did not worry too much about it. A few participants, however, reported to look favorable upon being shown personalized ads: "And of course it's in my interest to get advertisement for products I'm potentially interested in and not just for ladies' underwear [...] I think it's a good thing it's tailored to me, since I'm actually interested in the products that I am shown." (P19).

2) Financial loss: About half of the participants (12) talked about financial loss as a consequence of disclosing data, particularly banking details. Whereas some participants were mainly worried about passwords to their online banking accounts, others were concerned about their IBANs as well because they were not sure if it was possible to use this to debit money: "I am always...I don't know if that works, but if somebody could debit a sum just having your IBAN, that would actually be the fear. But I don't know if that would really work." (P7)

3) Job applications: A few participants (8) stated to be worried about a potential future employer getting access to their postings on social media and thus limiting their chances of getting a job they had applied to: "[...] when you provide your actual data and start posting things which are rather less favorable in terms of employers being able to find you easily and see what a person you are socially, if you are trustworthy or not...and that could easily backfire." (P4)

4) Safety threats: A few participants (7) were worried about becoming victims of harassment or stalking due to disclosure of their current location: "[...] that somebody shows up at your home and bothers you" (P7)

5) Spam mails: A few participants (6) were worried about receiving spam mails if their email address got disclosed.

6) Identity theft: A few participants (6) mentioned the risk of identity theft, either as an abstract threat: "Maybe somehow on the Internet, a doppelganger, e.g., that someone collects every information about me and somehow creates a new identity, which then is another me." (P7) or with regard to specific actions, like financial transactions, crime commitment or social interaction: "[...] that criminals could possibly take your identity to buy things or commit crimes and so on." (P3)

7) Exposure: Few participants (6) thought data disclosure could result in being exposed because they had done something they did not want their friends and family to know about: "[...] because there could be data that I would be embarrassed of if friends would find out about it. Because I suppose they wouldn't approve to certain behaviors or because I suppose they would make fun about it, if they'd know it." (P1)

8) Criminal prosecution: The few participants (5) who talked about the possibility of being criminally prosecuted mostly stated that only people committing crimes should be worried about this: "If I'd be a criminal. Then there would be information about me. Either where I am, what I buy, whom I contact. That I don't what to become public. But that does not apply in my case. I don't care who knows where I am at what time, how much I bought." (P2)

9) Political prosecution: Few participants (5) talked about possible consequences that could result from governmental surveillance. Those who did mostly stated to trust the current German government, but were concerned about possible implications regarding future governments: "Many people say they don't give a damn whether someone eavesdrops on them, why should someone care about their issues. But overall, I think that's not quite that simple. We currently live in a democracy, the constitutional state works in that our personal rights are protected rather well - so far. But that could change one day and if the government can access all communication channels then it could exploit this." (P8)

10) Monopolization: A few participants (5) expressed concerns about the monopoly of certain organizations through control over a great amount of consumer data: "And I think we are disclosing more and more about ourselves due to reasons of security or convenience and hence, certain organizations are getting more and more powerful, and those may dictate us a lot of things in the future. [...] And organizations are not always interested in the common welfare, but in their own profits and if they have such a great power they could use this to restrict our freedom one day." (P3)

11) Data abuse: Few participants (4) were worried about the unintended use of their data: "That happened to some comedian, the AfD [german political party] canvassed with his photo. That's...that can be misused. [...] And suddenly you appear as a dessous model in the US and have never heard about that before." (P11)

12) Burglary: Only very few participants (3) talked about burglary as a potential risk of disclosing one's location data. Those who did, however, rated the risk as rather low.

13) Propaganda: Very few participants (2) reported to be worried about their data being used to influence their opinion in some way. Statements to this topic mainly referred to the recent US election: "Um, recently in the US elections the way the Republicans run their election campaign and there was a media report about it. About an analytic software, how you categorize certain groups of people. To break it down, they knew which people they should address and what would be reasonable, what groups of people should be addressed to suceed with the election campaign." (P8)

14) Less favorable insurance tariffs: Location and health data were mentioned by very few participants (2) in association with the risk to get a less favorable health insurance tariff: "Or, if we're getting on with these fitness and health trackers that store various data, that, e.g., a health insurance company could say 'Well, we saw via your app or fitness tracker that you don't work out very much. No wonder you're sick now, that's your own fault. We're not paying you anything."' (P3)

15) Not being granted a credit: Only one participant mentioned the possibility of being refused a credit: "Well then, it could be possible that not just the employer uses the data, but

also banks if they grant credits. That they can access what you bought at Rewe [a German supermarket] in the past and then infer from this you're not able to handle money well and then refuse to grant you the crucial credit." (P1)

B. Protection obstacles

We identified five obstacles that prevent our participants from protecting their data, with three concerning their skills and motivation, and one concerning other people and ethical considerations, respectively.

1) Too much effort: Some participants (9) reported to refrain from reading security policies since these were too cumbersome to understand. The same seems to apply regarding the use of privacy-friendly applications: "Because after all it [Threema] is rather cumbersome. And because only a few people use it and I think you can still share everyday things via WhatsApp." (P16)

2) Too complicated: Very few participants (2) complained about privacy policies being too complicated to understand.

3) Lack of knowledge: This is in line with a few participants (4) stating lack of knowledge about protection possibilities and processing of their released data as one reason for not protecting themselves more: "I wish I'd know which data I should protect better and how. Maybe I also would take better care if I'd know. If I'd concentrate more on this I'd probably know why it is important to protect these data, but it's just too hard for me to access these information." (P12)

4) Behavior of other people: A few participants (8) referred to other people who refrained to use alternative privacy-friendly messengers or even shared data about third people: "In my opinion, if you have the opportunity to use a secure service, why shouldn't you do it, I think. The only thing speaking against it is, for example Telegram, it's just not spread that much. If you delete WhatsApp and only use Telegram, you simply don't reach a huge amount of your friends." (P8) "With social networks like Facebook [...] as soon as anybody posts something or tags you, it's already gotten out where you are or where you were or anything." (P4)

5) Ethical considerations: One participant also explained that s/he thought it would be unethical to use free services that build on the processing of personal data as their business model without proving personal data: "The thing is, the anonymous search engines use Google's data, more or less...I think, in terms of ethics, that's kind of...not perfectly ethical, with the anonymous search engines using Google's servers, since they cost and not giving something in exchange to Google for this...to use it for free...actually the deal is that Google shows ads for this." (P13)

Furthermore, participants stated four different reasons for using applications or devices that could possibly harm their privacy, with all but one being related to social factors.

6) Social pressure: Most (19) participants reported to use certain messenger or OSNs, even if they are skeptical towards them in terms of privacy protection, because most of their friends also use them: "Well, I actually view WhatsApp with skepticism due to reasons of data privacy. However, since all of my friends use WhatsApp I also use it, for you won't get very far with an alternative messenger that might be more suitable but that nobody uses." (P1) Accordingly, they stated that they would transfer to other messengers or OSN if their friends would do so. However, this effect also applies to the use of such applications that are considered as privacy-friendly: "Friends of mine started with this and then all of them had it and then we had a group chat and then everyone transferred to Threema and then I thought 'Come on, then you're also going to Threema'." (P11)

7) To keep oneself and others up-to-date: Many participants stated to use OSN to keep themselves informed of what happens in the life of their friends and family or to inform others about what is going on in their own life: "Once in a while you wonder about what friends with whom you don't meet very often do at the moment. [...] I don't get an email, I don't get a WhatsApp message, I get all information via Facebook what happens in my surroundings." (P8) "[...] I want my family - because we live so far apart...sometimes I like it to communicate with them. [...] so they know where I am, where I was on the weekend, I don't know, stuff like this and I want to show it, because they want to know how I am and they want to know what I did." (P17)

8) Convenience: Some participants (7) admitted to use certain applications out of convenience: "Anyhow you have an easy opportunity to contact a large amount of people and invite to something, who have then the opportunity to discuss things like who brings what, when does it start, what's the address again in this group or event. And that simplifies a lot of things." (P5)

9) Express one's opinion: Very few participants (2) referred to the opportunity to express and spread their own opinion about a certain topic: "But when I post something then often with the idea to let people in my social surroundings know something, either what I do or what I like. [...] Last year at Christmas I found out about gift coupons offered by the Oxfam company that supported charitable projects. That's something I want more people to know of and maybe support it, and so I spread it." (P2)

C. Protection strategies

Most of the strategies participants described to deploy for protecting their data relied on reducing data disclosure, either by not using certain services, not sharing certain data or limiting the amount of recipients. Some participants, however, also reported to actively provide false or misleading information to "confuse the system".

1) Refrain from using services that could infringe upon one's privacy: Some participants (8) deliberately decided not to use certain services to prevent these from accessing their data. The list of these "critical" services does not only comprise apps demanding extensive permissions and OSN, but also game consoles, Google's search engine, loyalty programs, cookies and applications that gather certain kinds of data (e.g., one's location). Some participants reported not to use those privacy-critical services right from the start, whereas

others have used them for some time but then decided to abandon the use. In their choice of an alternative service, participants mainly relied on the service provider's reputation: "Well, regarding the phone, that I use an iPhone and not an Android, of which...You know both share information with the NSA, but as far as I know only Google also uses it for marketing purposes [...]." (P13) Another strategy is to rely on the opinion of experts: "For example, Signal is recommended by Edward Snowden [...] it helps in the decision to use it if someone like Edward Snowden recommends it." (P13)

2) Do not share sensitive data: Some participants (13) stated to not share certain kinds of data, e.g., their name, email address, phone number, location, and bank data. However, only one participant mentioned his/her sharing behavior in OSN in this regard: "If you have liked 'ZEIT ONLINE' [a German newspaper], you always get their news feed and some things there are interesting every once in a while, where you think it would be worthwhile to promote it a little and it could interest someone, e.g., a pal, but instead of liking it or tagging my pal, I leave it be and think 'whatever'." (P8)

3) Limit the amount of data recipients: A few participants (2) reported to share data, but limit the amount of recipients, for example by reducing the number of Facebook friends or not posting something on Facebook at all because they have so many friends there: "Maybe because so many are watching. Back then you had about 30 friends, it didn't matter what you posted on your timeline. And now it's, I don't know for sure, like 400. Thus you think twice before you post something." (P8) Others use Facebook's privacy settings to keep their postings away from unwanted readers.

4) Provide false or misleading information: A few participants (6) reported to act according to the principle "security through obscurity" by providing false information on purpose, mainly by using a false identity: "Well, depending on the service provider, quasi depending on the importance, I also provide false data, I don't simply use false data but instead I have set up a fake profile which I always use." (P10)

D. Common privacy (mis)conceptions

We also identified certain (mis)conceptions about data privacy in our participants' responses that have already been observed by other privacy researchers in prior studies.

1) I have nothing to hide: Some participants stated they were not interested in privacy very much because their data was not sensitive at all: "Yes, well, I must say I don't get the whole hype about this...I always think those who have nothing to hide don't have to be so upset about it. [...] if someone would intercept me, I'd say he wouldn't find anything or it wouldn't be relevant [...]" (P15)

2) I am not important enough: Accordingly, a few participants also thought they were too unimportant to be intercepted: "[...] but I have a lot of confidence. On the one hand in the systems, on the other hand that I am too ordinary. That it wouldn't be worthwhile to spy on my data." (P2)

3) It is not possible to protect my data: A few participants said even if they wanted to do so, it would not be possible to protect their data from being accessed in one way or another: "I think it is like the lock at my apartment, if someone really wants to get in he can break it open. If someone really wants to have my data, he gets it. Once I use smartphones and notebooks, that's a truth I have to deal with...or that I have to accept, respectively." (P18)

V. Discussion

We conducted an interview study with 24 participants to shed light on why and how users' do protect or refrain from protecting their privacy.

A. Mental models of privacy consequences

Regarding RQ1, we found that while most participants named personalized advertisement as a possible consequence of not protecting one's privacy and about half of our participants also fear financial losses, most participants lack awareness of further possible privacy consequences. This is in line with the results from Harbach et al. [21] and Shirazi and Volkamer [30], who also identified financial loss and personal advertisement as the most salient privacy consequences. However, individual participants provided additional possible consequences besides personalized advertisement and financial loss. The list of resulting consequences also relates to the results of Karwatzki et al. [23], since all consequences named by our participants could be categorized as either physical, social, resource-related, psychological, prosecution-related, career-related, or freedom-related. However, most consequences provided by our participants are more specific than the broad categories of consequences identified by Karwatzki et al. [23], and some refer to more than one category. The resulting list of consequences could thus be better suited to complete people's mental models of possible data collection consequences, e.g., in interventions and campaigns than Karwatzki et al.'s categories.

B. Obstacles for privacy protection

Regarding RQ2, we found that participants refrain from applying protection solutions or using privacy-friendly alternatives since these are too cumbersome to use, too complicated to understand, or due to the contradictory behavior of other people. In line with this, most participants reported to still use privacy-threatening services (e.g., OSN, messenger) in order to reach other people, participate in their life, or share their opinion with others. Another reason for using non-privacy-friendly services and devices is the convenience that these products offer. Contrary to prior studies (e.g., [30], [32], [50]), the major obstacles for privacy protection reported by our participants are related to usability and social factors, of which the latter were also identified to be crucial for the adoption of secure messengers by Abu-Salma et al. [33]. Whereas there are already many ongoing efforts to improve the usability of PETs (successful or not), social factors are harder to influence from the outside, i.e., as a privacy researcher or activist. Yet there also lies an opportunity in people's social suggestability, as some also report to having started to use a privacy-friendly

service because a significant other used this service as well. Hence, future attempts to motivate users to increase their privacy could focus on the social aspect, for example by letting other people invite their peers to privacy-friendly OSN, messengers, search engines etc.

C. Strategies for protecting one's privacy

Regarding RQ3, our participants reported to apply several privacy protection strategies, i.e., refrain from using privacy-threatening services, not share sensitive data, limit the amount of data recipients, or provide false information. These strategies indicate that our participants do not suffer from an "illusion of control", in the sense that they think their privacy is safe because they can decide what kind of information is shared with whom and have the possibility to change this decision later on, e.g., by editing their profile, while actually once an information is shared online users cannot control who already gained access to that information and how it is processed by third parties in the future. However, some participants reported a lack of knowledge about possible protection measures to be an obstacle for privacy protection, and some participants did not report on applying a successful protection strategy at all. Furthermore, all of the protection strategies our participants reported to use fall in the category of "behavioral" protection strategies described by Oomen and Leenes [17]. None of our participants reported to use standard security measures and PETs or more advances PETs. Whereas we suppose this is rather due to a lack of knowledge about what programs are running on their computer and how these are involved in the protection of their private data than an actual abandonment of standard security measures, it shows significant deficits in our participants' understanding of how data is processed on their computer. These results are contrary to those of Litt [47], who found that younger adults tend to apply more technically based protection strategies. Although our sample was rather young, our participants do not seem to be automatically more technically adept than older users.

Hence, it is not sufficient to hope that problems referring to a lack of technical expertise in the deployment of protection strategies will vanish on their own once most online users are digital natives. It seems thus crucial to further educate users about strategies for privacy protection, e.g., by developing trainings, campaigns, info material, or dedicated privacy assistants that provide information about possible protection solutions and help users to apply these solutions successfully.

Overall, our results suggest that there is no single factor determining whether people protect their private data or not, as our results provide evidence for all possible explanations for people failing to protect their data proposed in the introduction (i.e., lack of awareness regarding consequences, costs outweight benefits in a rational analysis, lack of knowledge about protection solutions or illusion of control about the handling of shared data). Since we further identified additional factors which influnce whether people adopt measures to protect their privacy, we propose a model which subsumes all factors that are relevant for people's decision to actually apply privacy protection measures. This model will be introduced in the following section.

D. Factors influencing the adoption of privacy protection measures

We identified four factors with various sub-categories that influence whether people are motivated and able to successfully protect their private data. The resulting model is displayed in figure 1.

In line with results from other studies [10], [30], [32], [33], [50], we found that usability is not the most important factor for the adoption of protection measures. Other factors, such as conceptions about being important, having something to hide, and the awareness of negative consequences that could arise from privacy violations also play an important role regarding people's motivation to think about the protection of their data. Once they are motivated, they also need to possess certain knowledge about how to protect their data, protection should not be too complicated and the people need to believe in the possibility of data protection. If people are motivated and able to deal with privacy issues, they will likely consider the costs of data protection in their decision for or against the adoption of data protection measures. Hence, people are more likely to adopt such protection measures if these are effortless, do not cause ethical concerns, and the functionalities of the services still support people in attaining their goals. Due to the social component of many data-capturing services like OSN or messengers, the behavior of other people also plays an important role. People are more likely to use encrypted, privacy-friendly messengers or encrypt their emails if their friends also do this. Moreover, people cannot sufficiently protect their data if other people share it, e.g., on OSN sites.

Our results verified all factors influencing privacy protection (or the lack thereof) identified in other studies [10], [30], [32], [33], [50] that are not dependent on the specific context investigated in the respective studies. We further identified three new sub-categories, namely: (1) Being ethically correct when protecting one's data, (2) keep oneself and others up to date, (3) other people not sharing one's data.

Consequently, in order to provide useful tools for privacy protection, developers of PETs have to consider the identified factors that influence the adoption of privacy protecting measures. The results indicate that this could be done by raising awareness of privacy issues on the one hand and providing knowledge on the other hand via PETs. Further, PETs have to be easy and effortless to use, and not affect the core functionalities of online services that motivate people to share their data in the first place, such as contacting other people. Last but not least, other people have to support privacy protective behavior by also using protection solutions, such as end-to-end encryption, and refrain from sharing other people's data. This issue could possibly be addressed by implementing a feature to easily invite other people to use certain protection solutions one wants to use, for example for communication, as it is already implemented in popular services like Facebook.

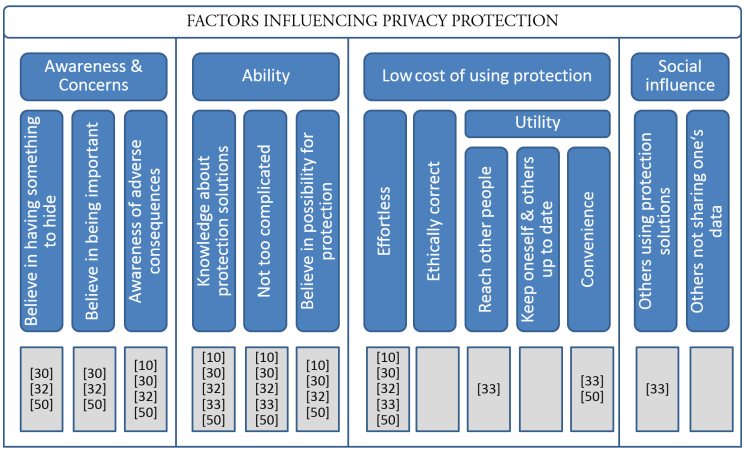

Fig. 1. Model of factors influencing privacy protection. The references in the gray boxes indicate what factors have also been identified in previous studies.

E. Limitations

The study suffers from several limitations that should be kept in mind when drawing conclusions based on the results. We used a convenience sample, which resulted in the majority of our participants being students, thus our sample is most likely skewed (i.e., younger, higher educated and eventually over averagely tech-savvy) compared to the general population. Furthermore, it would be recommendable to validate the results with a greater number of participants. Also, although we aimed to investigate the general privacy behavior of people across different contexts, some online services, such as online social networks and messengers, are very well-known to most people, unlike new devices and services like smart home systems. Hence, it is likely that these contexts are over-represented in the answers of our participants.

ACKNOWLEDGEMENTS

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

REFERENCES

[1] M. Madden, L. Rainie, K. Zickuhr, M. Duggan, and A. Smith, "Public Perceptions of Privacy and Security in the Post-Snowden Era," *Pew Research Center*, pp. 3–57, 2014. [Online]. Available: www.pewresearch.org

[2] L. Rainie, S. Kiesler, R. Kang, and M. Madden, "Anonymity, privacy, and security online," http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/, accessed: 2017-10-20.

[3] Symantec, "State of privacy report 2015," https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf, Symantec, Tech. Rep., 2015, accessed: 2017-10-20.

[4] I. . C. for International Governance Innovation, "83% of global internet users believe affordable access to the internet should be a basic human right," https://www.cigionline.org/sites/default/files/documents/internet-survey-2014-factum.pdf/, Tech. Rep., 2014, accessed: 2017-03-01.

[5] I. MORI, "Global trends: personalisation vs. privacy," http://www.ipsosglobaltrends.com/personalisation-vs-privacy.html/, Tech. Rep., 2014, accessed: 2017-03-01.

[6] B. I. with Kaspersky Lab, "Consumer security risks survey. From scared to aware: digital lives in 2015," https://press.kaspersky.com/files/2015/07/Kaspersky_Lab_Consumer_Security_Risks_Survey_2015_ENG.pdf/, Tech. Rep., 2015, accessed: 2017-03-01.

[7] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security and Privacy*, vol. 3, no. 1, pp. 26–33, Jan. 2005. [Online]. Available: https://doi.org/10.1109/MSP.2005.22

[8] D. M. Boyd and N. B. Ellison, "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication*, vol. 13, no. 1, pp. 210–230, 2007. [Online]. Available: http://dx.doi.org/10.1111/j.1083-6101.2007.00393.x

[9] P. Norberg, D. R.Horne, and D. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," vol. 41, pp. 100 – 126, 2007.

[10] V. Garg, K. Benton, and L. J. Camp, "The privacy paradox: A facebook case study," in *Proceedings of the 42nd Research Conference on Communication, Information and Internet Policy*, 2014.

[11] H. Liang and Y. Xue, "Avoidance of information technology threats: A theoretical perspective," *MIS Q.*, vol. 33, no. 1, pp. 71–90, 2009. [Online]. Available: http://dl.acm.org/citation.cfm?id=2017410.2017417

[12] N. Lee and O. Kwon, "A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2764–2771, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.eswa.2014.11.031

[13] M. Taddicken, "The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure," *Journal of Computer-Mediated Communication*, vol. 19, no. 2, pp. 248–273, 2014. [Online]. Available: http://dx.doi.org/10.1111/jcc4.12052

[14] Y. M. Baek, "Solving the privacy paradox: A counter-argument experimental approach," *Computers in Human Behavior*, vol. 38, pp. 33 – 42, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563214002842

[15] L. Brandimarte, A. Acquisti, and G. Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social Psychological and Personality Science*, vol. 4, no. 3, pp. 340–347, 2013. [Online]. Available: https://doi.org/10.1177/1948550612455931

[16] S. Kokolakis, "Privacy attitudes and privacy behaviour," *Computers & Security*, vol. 64, no. C, pp. 122–134, 2017. [Online]. Available: https://doi.org/10.1016/j.cose.2015.07.002

[17] I. Oomen and R. Leenes, *Privacy Risk Perceptions and Privacy Protection Strategies*. Boston, MA: Springer US, 2008, pp. 121–138.

[18] D. Sarathchandra, K. Haltinner, and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in *2016 Cybersecurity Symposium (CYBERSEC)*, 2016, pp. 68–73.

[19] V. Garg and J. Camp, "End user perception of online risk under uncertainty," in *2012 45th Hawaii International Conference on System Sciences*, 2012, pp. 3278–3287.

[20] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns," in *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ser. SPSM '12. New York, NY, USA: ACM, 2012, pp. 33–44. [Online]. Available: http://doi.acm.org/10.1145/2381934.2381943

[21] M. Harbach, S. Fahl, and M. Smith, "Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness," in *2014 IEEE 27th Computer Security Foundations Symposium*, 2014, pp. 97–110.

[22] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ser. SOUPS '10. New York, NY, USA: ACM, 2010, pp. 11:1–11:16. [Online]. Available: http://doi.acm.org/10.1145/1837110.1837125

[23] S. Karwatzki, M. Trenz, V. K. Tuunainen, and D. Veit, "Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence," *European Journal of Information Systems*, pp. 1–28, 2017.

[24] B. Friedman, D. Hurley, D. C. Howe, H. Nissenbaum, and E. Felten, "Users' conceptions of risks and harms on the web: A comparative study," in *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '02. New York, NY, USA: ACM, 2002, pp. 614–615. [Online]. Available: http://doi.acm.org/10.1145/506443.506510

[25] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, and A. Seeam, "Pervasive ehealth services a security and privacy risk awareness survey," in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, 2016, pp. 1–4.

[26] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall, ""When I Am on Wi-Fi, I Am Fearless": Privacy Concerns & Practices in Eeryday Wi-Fi Use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '09. New York, NY, USA: ACM, 2009, pp. 1993–2002. [Online]. Available: http://doi.acm.org/10.1145/1518701.1519004

[27] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor, ""I Regretted the Minute I Pressed Share": A Qualitative Study of Regrets on Facebook," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, ser. SOUPS '11. New York, NY, USA: ACM, 2011, pp. 10:1–10:16. [Online]. Available: http://doi.acm.org/10.1145/2078827.2078841

[28] S. Trewin, C. Swart, L. Koved, and K. Singh, "Perceptions of risk in mobile transaction," in *2016 IEEE Security and Privacy Workshops (SPW)*, 2016, pp. 214–223.

[29] J. W. Clark, P. Snyder, D. McCoy, and C. Kanich, ""I Saw Images I Didn't Even Know I Had": Understanding User Perceptions of Cloud Storage Privacy," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 1641–1644. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702535

[30] F. Shirazi and M. Volkamer, "What Deters Jane from Preventing Identification and Tracking on the Web?" in *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, ser. WPES '14. New York, NY, USA: ACM, 2014, pp. 107–116. [Online]. Available: http://doi.acm.org/10.1145/2665943.2665963

[31] W. Melicher, M. Sharif, J. Tan, L. Bauer, M. Christodorescu, and P. G. Leon, "(Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking." *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 2, pp. 135–154, 2016. [Online]. Available: http://dblp.uni-trier.de/db/journals/popets/popets2016.html#MelicherSTBCL16

[32] K. Renaud, M. Volkamer, and A. Renkema-Padmos, *Why Doesn't Jane Protect Her Privacy?* Cham: Springer International Publishing, 2014, pp. 244–262.

[33] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 137–153, 2017.

[34] J. M. Such, J. Porter, S. Preibusch, and A. Joinson, "Photo Privacy Conflicts in Social Media: A Large-scale Empirical Study," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: ACM, 2017, pp. 3821–3832. [Online]. Available: http://doi.acm.org/10.1145/3025453.3025668

[35] P. Wisniewski, H. Lipford, and D. Wilson, "Fighting for My Space: Coping Mechanisms for Sns Boundary Regulation," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '12. New York, NY, USA: ACM, 2012, pp. 609–618. [Online]. Available: http://doi.acm.org/10.1145/2207676.2207761

[36] F. Stutzman and J. Kramer-Duffield, "Friends Only: Examining a Privacy-enhancing Behavior in Facebook," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1553–1562. [Online]. Available: http://doi.acm.org/10.1145/1753326.1753559

[37] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in It Together: Interpersonal Management of Disclosure in Social Network Services," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '11. New York, NY, USA: ACM, 2011, pp. 3217–3226. [Online]. Available: http://doi.acm.org/10.1145/1978942.1979420

[38] G. R. Milne, A. J. Rohm, and S. Bahl, "Consumers' Protection of Online Privacy and Identity," *The Journal of Consumer Affairs*, vol. 38, no. 2, pp. 217–232, 2004. [Online]. Available: http://www.jstor.org/stable/23860547

[39] K. Mahar, A. X. Zhang, and D. Karger, "Squadbox: A Tool to Combat Email Harassment Using Friendsourced Moderation," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: ACM, 2018, pp. 586:1–586:13. [Online]. Available: http://doi.acm.org/10.1145/3173574.3174160

[40] D. Machuletz, S. Laube, and R. Böhme, "Webcam Covering As Planned Behavior," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: ACM, 2018, pp. 180:1–180:13. [Online]. Available: http://doi.acm.org/10.1145/3173574.3173754

[41] S. Sannon, N. N. Bazarova, and D. Cosley, "Privacy Lies: Understanding How, When, and Why People Lie to Protect Their Privacy in Multiple Online Contexts," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: ACM, 2018, pp. 52:1–52:13. [Online]. Available: http://doi.acm.org/10.1145/3173574.3173626

[42] L. Coles-Kemp and E. Kani-Zabihi, "Practice Makes Perfect: Motivating Confident Privacy Protection Practices," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, 2011, pp. 866–871.

[43] A. L. Young and A. Quan-Haase, "Privacy protection strategies on Facebook," *Information, Communication & Society*, vol. 16, no. 4, pp. 479–500, 2013.

[44] J. Staddon, A. Acquisti, and K. LeFevre, "Self-Reported Social Network Behavior: Accuracy Predictors and Implications for the Privacy Paradox," in *2013 International Conference on Social Computing*, 2013, pp. 295–302.

[45] A. N. Peters, H. Winschiers-Theophilus, and B. E. Mennecke, "Cultural influences on Facebook practices: A comparative study of college students in Namibia and the United States," *Computers in Human Behavior*, vol. 49, pp. 259 – 271, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563215001892

[46] Y. Feng and W. Xie, "Teens concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors," *Computers in Human Behavior*, vol. 33, pp. 153 – 162, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563214000144

[47] E. Litt, "Understanding social network site users privacy tool use," *Computers in Human Behavior*, vol. 29, no. 4, pp. 1649 – 1656, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563213000526

[48] A. L. Strauss and J. M. Corbin, *Basics of qualitative research: Grounded theory procedures and techniques.* Thousand Oaks, CA, US: Sage Publications, Inc., 1990.

[49] A. L. Strauss, *Qualitative analysis for social scientists*. New York, NY, US: Cambridge University Press, 1987.

[50] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz, "A socio-technical investigation into smartphone security," in *Security and Trust Management. STM 2015. Lecture Notes in Computer Science, vol 9331*, S. Foresti, Ed., 2015, pp. 265–273.