Telematics and Informatics 68 (2022) 101782

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

Lost in privacy? Online privacy from a cybersecurity expert perspective

Susanne Barth, Menno D.T. de Jong *, Marianne Junger

Faculty of Behavioural, Management and Social Sciences, University of Twente, Enschede, the Netherlands

ARTICLE INFO

Keywords:
Experts
Mobile apps
Online behavior
Privacy paradox
Privacy perceptions

ABSTRACT

Research on the privacy paradox shows that ICT users have serious concerns about their online privacy but often do not behave accordingly. Most insights, however, are based on research among lay users. It is unclear whether users with high expertise on online privacy and cybersecurity would show similar discrepancies between concerns and behavior. We therefore interviewed 20 privacy and cybersecurity experts about their views on online privacy regarding mobile apps. Despite their technical knowledge, results showed that the experts' perceptions and reported behaviors resembled those of lay users. A lack of specialized knowledge therefore does not seem to be a plausible explanation for the privacy paradox among mobile app users.

1. Introduction

Smartphones are omnipresent and have become an integral part of our daily lives. Applications ('apps') running on mobile devices support many of our daily activities, from providing information to pass time and entertainment, from maintaining social contacts to tracking physical activities, and from way-finding to buying products and services. By installing and using apps we provide vast amounts of personal data, which may either be stored on our phones or leave the local data storage. These data flows are not transparent and therefore difficult to understand. Research showed that 80% of the smartphone users have concerns about their personal data online (Deloitte, 2019). Despite these concerns, the number of app downloads is still on the rise and will probably exceed 250 billion by 2022 (Statista, 2019). Apparently, users' privacy concerns do not influence the adoption and usage of apps; instead, they often seem to be overridden by users' immediate practical, social, informational or entertainment needs and desires. The immediate benefits of downloading and using a particular app are salient and the possibility of privacy-compromising consequences in the future is easily accepted (Kehr et al., 2014; Pentina et al., 2016; Shklovski et al., 2014).

The discrepancy between privacy concerns and actual behavior is known as the privacy paradox: People say that they care about their online privacy but nevertheless disclose personal and sensitive information without hesitation (Acquisti, 2004; Barnes, 2006; Barth and De Jong, 2017). Most of our insights on privacy-related attitudes and behaviors are based on research with lay users, which implies that a lack of knowledge might play a role. Knowing about the exact privacy risks involved in downloading and using apps might raise people's privacy awareness and make them behave more cautiously, or give them the feeling that they can be in command and act appropriately, which would lower their privacy concerns.

Earlier research, however, suggests that experts' behaviors regarding online privacy often resembles lay users' behaviors. Barth et al. (2019) found that knowledgeable and privacy aware users—more specifically, advanced computer science students—take similar privacy risks when downloading and using mobile apps as lay users would do. Jorgensen et al. (2015) showed that experts and lay users

* Corresponding author.

https://doi.org/10.1016/j.tele.2022.101782
Received 30 April 2021; Received in revised form 25 November 2021; Accepted 18 January 2022
Available online 1 February 2022

have similar privacy concerns, but that experts may use different cues than lay users do (particularly permissions). Kang et al. (2015) and De Luca et al. (2016) showed that experts indeed have a better and more elaborate understanding of the conglomerate of privacy issues, but somehow do not put their knowledge into practice. Focusing on experts' and lay users' understanding of the Internet, Kang et al. (2015) showed that experts, like lay users, were often guided by their subjective feelings or by trustworthy cues on websites. Investigating the use of instant messaging apps, De Luca et al. (2016) found that experts, despite their privacy and security knowledge, still used insecure instant messagers for reasons of critical mass in their social network or ease of use considerations. In all, the previous research showed that expert knowledge on privacy issues may be unused or overruled in practice. These findings, however, are rather coarse-grained, as they do not differentiate between experts, and do not address possible feelings of dissonance, uncertainties, and dilemmas experts experienced when making privacy-related decisions.

For a better understanding of the relationship between privacy knowledge and privacy-related behaviors, in-depth insights into how privacy and security experts use and reflect on their knowledge, deal with uncertainties, and make decisions would be a valuable next step. We therefore conducted a qualitative interview study investigating how privacy and cybersecurity experts (hereafter experts) deal with online privacy on their own smartphones. We addressed the following two research questions:

RQ1: How do privacy and security experts value their personal online privacy?
RQ2: How do privacy and security experts evaluate and use mobile apps?

2. Earlier research

With the rise of ICT, online privacy became an integral part of the interaction between humans and technology. It became more important than ever before that users define, preserve, and monitor their personal boundaries when it comes to the disclosure of data. With smartphones and apps, the privacy discussion became even more salient. As smartphones combine sensors, 24/7 connectivity, real-time tracking, data aggregation, and profiling with simple and limited interfaces, they are potentially even more intrusive and less transparent than desktop computers and notebooks. Users without expert knowledge on privacy and cybersecurity can easily be lost in privacy: A lack of knowledge about privacy threats, intimidating and ambigiously formulated privacy policies, hidden information, and complicated or intrusive tools for protecting personal data in online environments often lead to false assumptions about privacy protection, enacting the information and power asymmetry between users and online service providers (Acquisti, 2004; Acquisti et al., 2016; Martin, 2013; Reidenberg et al., 2015; Sundar et al., 2013). Therefore, users need support to make informed decisions on their valuation of privacy and to understand the terms and conditions when using online services.

2.1. *Experience of privacy: a user perspective*

From many studies, we know that users do not translate their general concerns about online privacy into actual behavior, a contradiction known as the privacy paradox (Acquisti, 2004; Barnes, 2006; Barth & De Jong, 2017; Deuker, 2010; Keith et al., 2013; Shklovski et al., 2014). The privacy paradox seems to be particularly applicable to smartphone contexts (Benenson et al., 2012). Various explanations for the privacy paradox have been given: (1) privacy threats and benefits are rationally weighed, whereby benefits outweigh privacy threats; (2) privacy threats and benefits are weighed, but the outcome is skewed by irrational factors or bounded rationality; and (3) privacy threats are not even included in users' considerations (Barth and De Jong, 2017).

In the context of e-mail encryption, Renaud et al. (2014) used the metaphor of a stairs to illustrate the stages users have to go through regarding the protection of their online privacy. The first step is privacy awareness: knowing that privacy may be an important issue in online activities. The second step involves privacy concerns: worrying about their own online privacy. This is followed by a full understanding of privacy threats, and, one step higher, a recognition of the need to actively protect their online privacy. The next steps are, respectively, knowing how to protect themselves and being able to do so. The highest step, not being side-tracked, accounts for irrational elements that may interfere. Interviews with users confirmed the first five steps; however, users did not reach the step in which usability of protection measures became an issue.

Although there is no consensus about the underlying mechanisms of the privacy paradox, it seems plausible that the human mind is bounded by nature and cognitive overload makes rational decision making highly unlikely (Simon, 1982; Veltri and Ivchenko, 2017). One can think of the mechanism of delay discounting, which refers to the tendency that outcomes that are remote in time have less impact than immediate outcomes (Odum, 2011). Long-term privacy threats are hard to estimate (Shklovski et al., 2014), while the costs of paying for secure and safe apps are salient and immediate. After all, abuse of personal data is often not visible and data breaches are relatively unlikely to happen.

Users might adjust their attitudes towards the value of their private data for reasons of pragmatism, as the wish to use apps seems to be stronger than the risks of data misusage (Debatin et al., 2009). They may, for instance, see themselves as not interesting enough for potential fraud attacks and therefore underestimate the risk probability or shift responsibilities to other parties such as the app store or the government (Volkamer et al., 2015) or erroneously assume to be less vulnerable to privacy than other people (Debatin et al., 2009). The higher the desirability of an app, the greater the willingness to disclose personal information will be. This may particularly apply to social networking apps, due to group dynamics (Taddicken, 2014) and their significance and ubiquity in people's lives (Debatin et al., 2009).

An additional important consideration is that processes running in the background of mobile apps are difficult to understand for users (Acquisti et al., 2016). Especially unexpected data flows resulting from conscious transactions of personal data with other parties are not visible for users, although strongly affecting users' privacy (e.g., the collection of *meta*-data for profiling; Bräunlich et al., 2021).

Two other research findings further complicate users' privacy-related behaviors with mobile apps. First, research showed that privacy and security risks are perceived to be more likely on desktop computers than on mobile phones (Volkamer et al., 2015). Second, Choi et al. (2018) showed that privacy fatigue increases disengagement in protective measures and ostensible indifference towards privacy violation, eventually outweighing privacy concerns.

2.2. Understanding of privacy: The role of expertise

Privacy can be seen as a fuzzy concept, especially in online contexts. Its intangible and non-urgent nature can at least partially be attributed to a lack of knowledge among users about the risks of online behaviors and the consequences of data disclosure (Bandara et al., 2017). This might imply that technical expertise leads to different valuations of personal data and better precautions online. In a study on phone embedded tracking, Ketelaar and Van Balen (2018) found some paradoxical evidence for this assumption: Smartphone users with considerable knowledge about the technical mechanisms behind data collection and types of data targeted had lower privacy concerns and more positive attitudes toward location tracking, likely attributable to their ability to take better precautions against data gathering.

In a similar vein, knowledge of and attitudes toward security measures might explain that personal data are protected differently and eventually more effectively by experts than by non-experts (Ion et al., 2015). However, in their study on attitudes towards instant messaging services, De Luca et al. (2016) found that, despite their technical knowledge, experts showed similar risky behaviors online as lay users. Interestingly, Reidenberg et al. (2015) showed that privacy policies of Web services are especially ambiguous when making statements about data sharing and sensitive information. This ambiguity prompts misinterpretations about data sharing practices and might cause unintentional disclosure of personal data, an effect that is not only observable among lay users but also among privacy policy experts. Still, lay users seem to be more prone to decisions based on false assumptions about security and privacy than experts are. Similarly, mental models lay users have of Tor architecture are found to be superficial, incomplete, and rather abstract compared to those of experts, who showed a deeper understanding of threats models. Lay users' false assumptions about security may have serious impact on their privacy-related behaviors online. Interestingly, experts have knowledge gaps as well, but less serious than novice users (Gallagher et al., 2017). Still, their knowledge gaps appear to have similar effects on their privacy-related behaviors.

2.3. Estimation of privacy: proxies that guide decision making

The aforementioned research findings underline that, within the complex and highly technical mobile environment and the boundaries of human cognition, it is hard for users to make informed decisions about the appropriateness of an app and that this may even be the case for users with considerable technical knowledge about online privacy and security. Users must rely on several signals to decide whether to download an app or not. Permission requests could function as a proxy for privacy-related information. Still, less literate users often encounter difficulties understanding them and click through such prompts without paying much attention. As a result, factors such as app design, ratings, download rates, reviews, costs, functionality and peer recommendations may easily outweigh privacy-related considerations, or, even worse, privacy is not even considered in the evaluation and adoption process of apps (Benton et al., 2013; Chin et al., 2012; Felt et al., 2012; Kehr et al., 2015; Kelley et al., 2012). The app selection process seems to be guided by a 'take the first' heuristics (predominantly based on star ratings), a recognition heuristic (e.g., hearsay or prior experiences), or a vote heuristic (based on ratings and reviews). Furthermore, apps for free seems to be a guiding principle (Dogruel et al., 2015; Joeckel et al., 2017). Technical knowledge and considerations of permissions as proxies for privacy risks seemed to be outweighed by ratings, app design, and costs (Barth et al., 2019).

A more sophisticated understanding of the Internet and its underlying (technical) mechanisms does not automatically result in stronger privacy protection. Experts' ability to take protective measures may still be ruled out by internal considerations (e.g., a nothing-to-hide-feeling) or contextual cues such as familiarity with the service or company or symbols indicating privacy protection (Kang et al., 2015). Experts and lay users might estimate privacy differently and use different proxies to guide decisions on adopting an app. For instance, experts report to predominantly take permission information and reviews into account, whereas lay user put more emphasis on app descriptions and ratings (Jorgensen et al., 2015). However, the question whether technical knowledge leads to a more sophisticated evaluation of apps and different privacy-related behaviors is still unanswered.

3. Method

To answer the research questions, we conducted a qualitative study based on semi-structured interviews with privacy and cybersecurity experts. The interviews served multiple purposes. In this article, we focused on the experts' personal views on online privacy and online behavior. In another article, we will report on their professional knowledge about online privacy. The study was

approved by the Ethical Committee of the Electrical Engineering, Mathematics and Computer Science faculty of the University of Twente. Below, we will outline the details of the research.

3.1. Participants

From our academic and professional network, 40 privacy and cybersecurity experts were invited by e-mail to participate in this study. The participants received no compensation for taking part in this study.Potential candidates were contacted based on recommendations from their superiors. Inclusion criteria were a job description focusing on privacy and cybersecurity and experience with mobile apps and online privacy. In the invitation e-mail, the potential participants were provided with a summary of the research objectives and a preview of the interview questions, so that they could decide for themselves whether they would be suitable as participants. Participants who accepted the invitation were asked if they perceive themselves as suitable privacy experts for this study.

Following the recommendations of Marshall et al. (2013), who recommend a sample size between 15 and 30 participants for qualitative IS research, 20 participants were interviewed in face-to-face settings (one of whom withdrew afterwards) and one participant was interviewed remotely, resulting in a final sample of 20 privacy and cybersecurity experts. The qualitative nature of the research and the specificity of the sample justify this sample size (Sim et al., 2018). More importantly, the adequacy of the sample was underlined by the theoretical saturation that was reached when analyzing the data: Our data contained many similar views and behaviors reported by the participants. It is normal that in interview studies, the added value of newly added participants diminishes. This was also the case in our study; although they formulated their views and experiences differently than the earlier participants, the last participants interviewed did not add substantially new insights to our findings.

The participants were between 24 and 54 years old (mean = 38.1 years). All participants were male and had an engineering background. Their most frequent job descriptions were researcher, scientist, or analyst (N = 9), followed by security, technical, or program manager/coordinator (N = 5), consultant (N = 3), developer (N = 2), and software engineer (N = 1). All participants worked for public or private organizations operating in the domain of cybersecurity.

3.2. Research instrument

The semi-structured interviews were based on an interview guide with open-ended questions. First, participants were asked about their background, specifically their age, education, and current job. Participants were then asked to give an impression of their job activities and responsibilities and discuss the role of privacy and security issues in their job. For the first research question—how experts value their personal online privacy—we asked the participants about the importance they attach to online privacy in general and regarding mobile apps in particular. For the second research question—how experts evaluate and use mobile apps—we asked them about their personal smartphone usage and their practices regarding downloading apps (e.g., the cues they use to guide decisions about downloading an app).

3.3. Procedure

Each interview lasted between 45 and 90 minutes. Before starting with the semi-structured interviews, information about the research aim was shared. All participants signed an informed consent form and agreed on audio recording the interview. After that, questions from the interview guide were discussed with participants, giving them sufficient possibility to present their ideas on the topic in question. At the end of the session, the participants were debriefed and thanked for their participation.

3.4. Analysis

Interviews were transcribed verbatim and personal information that could identify participants was removed. After that, the data were imported into ATLAS.ti for code creation and analysis. Starting with an open coding procedure, a list of codes was derived based on research questions and literature and reading through all transcripts. Meaningful text passages were highlighted and codes were attached to them until a point of saturation was reached. Data saturation was reached at the point that no addititional new information was obtained from the data and further coding was no longer necessary (Fusch & Ness, 2015).

The units of analysis varied from single buzzwords to statements made in multiple sentences. The list of codes was discussed among the co-authors and considerably shortened, which eventually resulted in the following main code categories: (a) age and working position, (b) views on privacy, (c) review of signals, and (d) mobile phone usage. To assess the reliability of the codebook, 10% of the sample was coded by two independent coders (the first author and an independent researcher). The procedure was repeated twice, with the codebook being refined after each round and intensive discussions between both coders. Eventually, Cohen's kappa was 0.75, indicating substantial agreement. The remaining 90% was then coded with the revised codebook by the first author.

4. Results

4.1. Value of online privacy

The results show that the participants differed in their opinions about the value of privacy, eventually resulting in three groups: (1) experts who are concerned about their privacy (N = 7), (2) experts who are conscious about their privacy but not overly concerned (N

= 7), and (3) experts who do not pay much attention to their privacy (N = 6). These groups correspond to the three user categories distinguished by Westin's (1967) privacy orientation index: (1) *privacy fundamentalists*, who are 'at the maximum extreme of privacy concern' who 'are the most protective of their privacy,' (2) *privacy pragmatists*, who 'weigh the potential pros and cons of sharing information… …. after this, they decide whether it makes sense for them to share their personal information,' and (3) *privacy unconcerned*, who are 'the least protective of their privacy – they feel that the benefits they may receive . . . far outweigh the potential abuses of this information' (cf. Kumaraguru and Cranor, 2005; p. 15). Table 1 summarizes the three categories, along with typical quotes regarding online privacy value and mobile phone behavior. We will use these categories to provide in-depth descriptions of participants' views and behaviors.

4.1.1. Privacy fundamentalists

Seven of the twenty participants found their online privacy important or very important. Five of them claimed that their personal views on privacy matched their professional views. As a matter of fact, their strong views on the importance of privacy were a reason for several of them to find a job in the privacy and security domain. One participant stated that privacy for him was a moral decision. Using an online service is a '*transaction that takes place at a given moment in time, but beyond that transaction, the service is not allowed to obtain information.*' Other participants, however, mentioned a reverse relationship, with their professional knowledge about privacy and security increasing the attention they pay to privacy issues in private settings. One participant argued that deciding about privacy in his job is easier than doing so in real-life situations: At work he can follow clear definitions of privacy, but in his private life he is confronted with continuous decision making within changing contexts.

Although these participants seemed to be very conscious about their personal privacy and aware of privacy risks, they tended to use online services nevertheless, including the more risky ones. They justified this behavior referring to external factors such as time constraints or group pressure, but also to internal factors such as laziness, convenience, or an irresistible desire to use a certain app: '*I don't want apps to disclose my personal data to others, although I know that this happens… …. and yes, I use them nevertheless. For the mere reason that others, with whom I communicate, use that app.'* Although privacy was high on their agenda, they sometimes made decisions of which they knew '*that they are not optimal,*' because the urgent need to own and use an app outweighed their concerns. Such justifications indicate that a given discrepancy between stated valuing privacy and actual behavior was sometimes present. In addition, it mattered to these participants if a service could be held legally accountable for data misuse and privacy violations.

To minimize risks and resolve cognitive dissonance when using apps, the participants said they evaluated whether the required app permissions corresponded to their personal privacy boundaries and to the core functionalities of the apps. If this was not the case, permissions were seen as '*dangerous*' and were sometimes denied. Some permissions, though, were considered hard to interpret and the challenge of understanding them with all their implications was pointed out by some participants. However, one participant made a contradictory statement about the importance of understanding permissions, relativizing the impact of understanding troublesome permissions: *'In most cases I look at the permissions, try to understand and explain them… …. However, I have never denied an app because of the permissions so far.'*

Some participants argued that the selection and use of apps occurred very consciously and that all measures to protect personal data were taken, but could not describe clearly how they assessed the risks. App usage was kept to the minimum necessary, but *'standard apps like YouTube, Twitter, Facebook'* are used, *'even though preferably not, but this is a necessary evil.'* However, if an app is perceived as absolutely not trustworthy, it will not be downloaded. In most cases, the participants had a certain degree of mistrust of permissions.

4.1.2. Privacy pragmatists

Seven other participants could be characterized as privacy-conscious but not overly concerned. They generally tried to make rough risk-to-benefit calculations before downloading and using mobile apps. They were quite conscious about certain threats to their privacy, but still privacy was not as high on their personal agenda as it was in their professional life. Professionally, the right to privacy was very important to them, but this did not manifest itself as clearly on the personal level. They emphasized that users should always have the choice which data to disclose when using online services, but appeared to pay less attention to the data they disclosed themselves. They were fully aware that some companies know a lot about mobile phone users. But as long as they were not directly confronted with it, data gathering practices of companies were considered to be acceptable.

Similar to the group of privacy fundamentalists, these participants found it difficult to assess the risks of apps. Some participants tried to remedy such difficulties by limiting the online services or apps they actually used without restricting data gathering. One participant stated:

> *Yes, on the one hand, I consciously decided to use Google products, but Google products exclusively, so that one big company knows much about me, I don't think that's something really bad. I don't worry about the information they have about me, but I do not want them to tell me point blank that they have that information about me.*

Furthermore, some participants questioned the control someone actually can have about personal data in online environments. With high effort and considerable knowledge about technical issues, one might gain control of personal data. Still, in many situations, users do not have the time and willingness to engage in protective measures. The interviews suggest that these participants use online services despite knowing that personal data are not always treated confidentially. Because of their background in privacy and cybersecurity, they were aware that they should pay more attention to online privacy and disclosure of personal data than they actually did. One participant pointed out that his offline life corresponds with his online life and that more or less the same information about him is available in both contexts. At the same time, however, this participant was aware that business models of online services are not comparable with those of offline services, arguing that this is *'not a big deal.'*

Table 1
Expert groups based on Westin's privacy orientation index (POI).

Privacy Orientation	N	Illustrative Quotes	
		Value of Online Privacy	Mobile Phone Behavior
Privacy fundamentalists	7	'… on an Android phone, Google tracks your data by default. This can be what shops I visit, what hotels I book. The only thing I did is to switch on my mobile phone and immediately data gathering starts. I perceive this as an invasion of my privacy, because Google should not do that kind of things…. Yes, privacy is really important to me.'	'I think that this is dangerous. I avoid such things … if an app does not need to send SMS, why should I give permission to that. I don't trust it then. Sorry.'
Privacy pragmatists	7	'I always try to figure out how they apply security measures and how they handle data. These kinds of things. And what is the risk that you might take. And then I try to weigh risks against benefits. But do I really worry about it, no, I cannot say that. Yes, of course, there are certain risks when you do things online. I know that … but …'	'I know quite well who knows what about me. And I don't worry about it because I only tell people, Facebook or Google for instance, about things I want them to know. Yes, of course, some organizations have access to my personal pictures, for instance. Therefore, I have only pictures on my mobile phone they are allowed to see … but privacy is not very important to me. And this reflected in the fact that I install everything on my mobile phone.'
Privacy unconcerned	6	'You know the risks … but I have nothing to hide, so I don't worry about it.'	'There are no apps I worry about.'

Especially in this group of participants several contradictory statements are made. They appeared to know well that their data are not always treated properly and that their personal privacy might be infringed. Still they tended to use online services without really protecting themselves from privacy threats. Interestingly, some participants called themselves naive, as they could not imagine that '*big brother is watching you*' all of the time. Plausible strategies to act in line with their privacy concerns would be to be very selective in which data to disclose and which data to keep private or to count on paid apps instead of overprivileged free ones. However, it appeared that both strategies were not put into practice often by the participants.

4.1.3. Unconcerned users

The last group of six participants can be described as not valuing their personal privacy very much. Most of these participants claimed that they know the risks but do not mind disclosing personal data online. In this group, the *'I have nothing to hide'*-argument and the defeatist argument that online privacy does not exist anymore were mentioned often. Furthermore, the participants found it acceptable if their data are analyzed generically, as long as the individual is not identifiable. To them, privacy seemed to be manageable at first sight, but became complicated and nuanced after obtaining deeper insights about data gathering practices. However, this realization did not lead to a change in online behavior but to *'I should have known it better'*- explanations.

Unconcerned participants were aware that they have to give something in return for using certain online services, but still perceived the benefits as more important than their personal need for privacy. Furthermore, they questioned the availability of real alternatives. One participant stated:

> *Of course that might trigger an inner alarm, but what is the alternative to the permissions they ask for? Yes, you could decide to not install that app eventually. But the question remains, do you choose to play safe or to not install the app? I don't think that I won't install the app because of the permissions they ask for… …. Of course, it's a dilemma because it costs me something.*

Mistrust of certain services remained, but risks were accepted because of a lack of alternatives and a strong wish to own and use an app. This strategy of neglecting privacy risks was followed as long as nothing serious happened with their data. Furthermore, peers were taken as a reference point (*'If they do, it should be ok'*). The organization behind the app was also used as an important consideration (*'All my apps are from more or less big companies. That's helping me to trust them. Maybe, that's a bit naive but …'*). Moreover, privacy cynicism seemed to manifest itself in participants' reasoning regarding online privacy, starting with feelings of helplessness (*'I am unable to change the situation anyway'*) and eventually leading to an acceptance of data handling practices, even if they are not in line with one's personal views.

Although unconcerned users seemed to pay little attention to their privacy, it seemed that privacy boundaries, as far as possible, still played a role in their considerations (*'I have nothing to hide… …. But anyway, I try to consider the purpose . . . And yes, I try to choose a serious app that aligns with it'*).

4.2. Reviewing of privacy-related cues

Despite the differences described above, 90% of all participants indicated to review privacy-related cues before downloading an app. The cues functioned as proxies to evaluate whether an app is trustworthy enough to download. Most participants generally made a superficial scan of the app instead of conducting a real risk analysis. When looking at the group segmentation of fundamentalists, pragmatists and unconcerned users, one might expect that fundamentalists would review most privacy-related cues when evaluating an app. This was not the case: The average number of signals used was comparable in the three groups. Fundamentalist reviewed on average 2.4 different cues to judge the privacy friendliness of an app, whereas pragmatists and unconcerned users on average reviewed 2.3 and 2.5 different cues, respectively.

Table 2 gives an overview of the cues considered by the participants. Of all cues experts mentioned, requested permissions were most often mentioned. However, it is unclear whether the requested permissions really influenced participants' decision of whether to download an app or not. Only few participants stated that they sometimes did not download an app because of its disproportionate permission requests. The majority reviewed permissions, but as long as they—at least to some degree—related to the app's functionality, they downloaded the app even if not all permissions were entirely explainable. The second most considered cue were reviews, in which other users share their experience with the app. Often only the reviews on top or the most positive and negative ones were read, or only apps with positive reviews were taken into account. However, the participants did not pay attention in the interviews to the reliability of the reviews.

Interestingly, 35% of the participants considered the developer or owner of the app as an important cue for trustworthiness. They wanted to know where the app comes from, whether the developer of the app is officially registered, and/or whether the developer or company behind the app had already published other apps. One participant mentioned that the 'certified developer flag,' a recommendation of Google, helped him to estimate the trustworthiness of the app. Likewise, they inferred the degree of trustworthiness of an app from the number of downloads: The more downloads, the better the app is and, therefore, the more trustworthy it is. Besides, 25% of the participants looked at the description of the app or the ratings displayed in the Appstore. In the descriptions, professional language seemed to be important, as unprofessional or plain language use was equated with untrustworthiness. Apps with bad or no

ratings were not further considered. Other cues mentioned by individual participants were screenshots of the app in the app store, word-of-mouth, the number of versions and updates of an app, and familiarity.

In conclusion, only two participants did not look at cues at all, downloaded everything they were interested in, and saw later on what would happen. Sometimes, they uninstalled an app afterwards, because they did not like or trust the app anymore. The other participants took at least one cue into account before they actually made a decision which app to download on their phone. However, the exhaustiveness of their considerations appeared to differ between participants.

5. Discussion

5.1. Main findings and theoretical contribution

Our interviews with experts from the privacy and cybersecurity field can be summarized into three main findings that contribute to our understanding of online privacy: (1) technical knowledge does not automatically contribute to more privacy-conscious behaviors, (2) experts and lay users do not differ in the way they justify risky online behaviors, (3) although experts and lay users use different cues to evaluate the appropriateness of apps, the resulting online behaviors are largely similar.

5.1.1. The role of expertise in valuing privacy and protecting personal data

The segmentation of experts into groups corresponding with Westin's (1967) privacy orientation index showed that technical knowledge about privacy and cybersecurity does not automatically lead to a higher privacy valuation or more precautions to protect personal data online. On the contrary, experts may engage in different data handling practices that have similar outcomes: (1) a fundamentalistic view on privacy *but* still vulnerable to biases, (2) a pragmatic view on privacy *and* vulnerable to biases and, (3) an unconcerned view on privacy and little or no consideration of risks. Whatever importance experts attached to their online privacy, the strategies they used often led to unsafe, sometimes careless, online behaviors. Irrespective of their privacy orientation, the experts, just like lay users, struggled with the strong immediate temptations of free apps and had mechanisms in place to temporarily relativize the importance of privacy.

As such, the privacy paradox applies to the experts' attitudes and self-reported behaviors regarding mobile apps as much as it applies to those of lay users. Primarily based on studies with lay users, research on the privacy paradox (Acquisti, 2004; Barth and De Jong, 2017) shows that, irrespective of the value users attach to their online privacy, data disclosure happens rather easily, especially in the fast changing environment of mobile computing (Kehr et al., 2014). Lay users are often unable to resist downloading apps and giving up personal data because of biases in human decision making—for instance, too many and too complex factors to be considered, time constraints, or optimism bias (Acquisti, 2004; Shklovski et al., 2014). However, it is also argued that technical expertise might, at least to some extent, compensate for such biases. Technologically savvy users are assumed to be able to protect their personal data more effectively than lay users (Ion et al., 2015; Ketelaar and Van Balen, 2018) or at the very least, technical understanding brings more clarity to the complex online environments (Bandara et al., 2017). The assumption that experts who are specialized in privacy and cybersecurity are better able to evaluate and act upon the potential risks of data disclosure was not confirmed by our interviews: Similar to earlier findings of Kang et al. (2015), De Luca et al. (2016), and Barth et al. (2019), the self-reported online behaviors of privacy and cybersecurtity experts resembled those of lay users. Our data show that even considerable technical knowledge can be overruled in practice by situational or external factors (e.g., time constraints, money considerations, group pressure) and that being

Table 2
Cues reviewed by experts before downloading a mobile app.

Expert	Privacy Orientation	Permissions	Reviews	App Developer/Owner	Downloads	App Description	Ratings	Total
1	Fundamentalist	x	x	x		x		4
2	Fundamentalist		x	x	x			3
3	Fundamentalist	x						1
4	Fundamentalist	x		x				2
5	Fundamentalist	x		x	x			3
6	Fundamentalist		x	x				3
7	Fundamentalist	x						1
8	Pragmatist		x		x	x		3
9	Pragmatist	x						1
10	Pragmatist							–
11	Pragmatist	x	x		x	x	x	5
12	Pragmatist	x						1
13	Pragmatist	x	x		x			4
14	Pragmatist	x		x				2
15	Unconcerned	x					x	1
16	Unconcerned	x			x			2
17	Unconcerned		x	x		x	x	4
18	Unconcerned							–
19	Unconcerned	x	x				x	3
20	Unconcerned	x	x		x	x	x	5
Total		14 (70%)	9 (45%)	7 (35%)	7 (35%)	5 (25%)	5 (25%)	

technically literate does not automatically lead to different valuations of privacy or better online precautions. On the contrary, our results indicate that technical knowledge does not limit the effect of biases in decision making and heuristic thinking and that the influence of technical knowledge must be relativized. Futhermore, digital literacy might go beyond familarity with technical aspects of online services. Possibly, awareness of institutional practices of online services, a detailed understanding of business models, and the legal jargon included in most privacy policies are as problematic for expert users as they are for lay users. Therefore, enhancing such awareness should be a top priority when promoting digital literacy among all kinds of users (Park, 2011).

5.1.2. Justifications of risky online behavior

Our results not only show that experts appear to behave online as unsafely as lay users; the arguments they provide to justify their risky online behaviors are comparable to those of lay users. First, experts experience a lack of alternatives. For instance, if there is only one suitable app available, they may be inclined to accept everything, even if it might affect their privacy negatively. Experienced helplessness in an online environment leads to disclosure of data, despite privacy concerns and an inherent wish to protect private data (Hoffmann et al., 2016). Several experts claimed that the individual user is unable to change data handling practices anyway. Furthermore, and similar to the perceptions of lay users, statements associated with time constraints (Flender and Müller, 2012) and a disregard of long-term effects (Acquisti, 2004), both negatively related to personal privacy protection, were mentioned. Experts indicated not having the time or willingness to carefully consider every single aspect that might infringe their privacy, despite having the capability to do so. Especially the experts with lower levels of privacy concerns mentioned that they did not care about future consequences and therefore refused to engage in protective behavior. Group pressure and trust in others (e.g., the 'if everyone does it should be fine'-heuristic; Flender and Müller, 2012; De Luca et al., 2016) eventually result in situations in which benefits outweigh risks. The experts stated explicitly that in many situations the benefits are so attractive that the app is downloaded although they professionally know that this might cause risks. Although a lack of information and information deficit (e.g., due to the complex online environment and technical processes running in the background) are an important factor assumed to influence the behaviors of lay users (Acquisti et al., 2016; Bräunlich et al., 2021), it is not surprising that these limitations are not considered by experts. Nevertheless, the results of our study confirm that even considerable technical knowledge is easily outweighed by internal and external factors. Similar to the behavior of lay users, a lack of time, unwillingness to consider an app in great detail, and trust in peers are important factors influencing experts' decision-making process.

5.1.3. Determining the appropriateness of apps

The cues experts take into account for judging the suitability of apps differ from lay users' strategies. Similar to the findings of Jorgensen et al. (2015), requested permissions are by far the most frequently reviewed cues experts use, whereas lay users may at best only superficially consider them (Felt et al., 2012). Experts see permission requests as the most informative cue about potential privacy threats. However, the effects of their reviews of permissions are questionable, as most experts reported to still use overprivileged apps. Furthermore, permission requests are even for privacy and cybersecurity experts sometimes hard to understand and assessing the link to app functionality requires considerable reflection. If even experts have trouble using permission requests as useful cues, how can lay users be expected to understand and use them?

One might expect that experts are inclined to make decisions based on their expertise and professional judgment, but the influence of others—in the form of reviews, downloads, and ratings—should not be underestimated. Other cues involve the company behind the app or the app developer, which experts can probably judge more easily than lay users can, and app descriptions. Although their evaluation strategies may be different, experts are, just like lay users, also in favor of 'hit-or-miss-analyses' instead of making in-depth risk analyses. The knowledge they have of potential privacy risks and ways to avoid them does not make a big difference here. To avoid ill-considered decision-making, with exposure to overlooked risks and unintended data disclosure, users need specific privacy-related facts about apps in a smart, appealing, and alerting way.

5.2. Practical implications

Our results suggest that the privacy knowledge experts have does not have consequences for their privacy-related attitudes and behaviors. Some experts indicated that the broad and specialized knowledge they have is rather far removed from the specific decisions they must make about downloading and using a specific app. Based on the results of our study, providing mobile phone users with more information about privacy and even making then more aware of the potential threats associated with downloading and using apps do not seem to be useful strategies to solve the privacy paradox. General privacy knowledge and privacy awareness are relevant factors, but our expert study shows that even when both are present there will still be other mechanisms that make users not behave in line with their privacy concerns. The privacy paradox must be seen as an unruly phenomenon, requiring more than information provision and persuasion for a solution.

On the short term, knowledge-based strategies such as privacy education and exhaustive privacy statements also do not seem to be helpful. A type of support that might help users—both lay users and experts—in their privacy-related decisions would be a privacy visualization available with all other app information in the app store (Barth et al., 2021). Ideally, such a visualization would raise users' privacy awareness at the very moment of their decision about buying downloading an app, and provide users with the specific information they need to make sense of the severity of its privacy threats. It should inform users about the types of data gathered (e.g., personal or anonymous data) and the way the data are handled (e.g., analyzed, sold, protected, or stored) in a concise and transparent manner. The goal would be to highlight all relevant information without overwhelming users with too much information.

5.3. Limitations and future work

This study gained insights into the privacy considerations and online behaviors of users with expertise in privacy and cybersecurity. In interpreting the results, it is important to keep the following three limitations in mind.

First, we included experts based on their expertise related to their professional role. Although we were very careful in selecting participants, paying attention to their education, their job, and their experience, we cannot be sure of each individual expert's specific level and types of expertise regarding privacy. We can imagine that participants' knowledge and views may be based on different professional and personal experiences, which we could not include in the interviews. Future research confronting different experts' specific knowledge of and views on privacy, for instance in a Delphi study, could be an interesting follow-up to our study.

Second, all participants included in our sample were male. This is to some extent explainable by the male–female ratio in ICT in the Netherlands, with less than 18% females in the technical workforce in 2018 (UWV, 2018), but much to our regret we did not manage to include any female participant in our sample. As the literature on the effects of gender on privacy perceptions and online behavior is inclonclusive (Park, 2015; Schumacher & Morahan-Martin, 2001; van Deursen & van Dijk, 2011), it is hard to speculate about the effect of gender on experts' privacy views and behaviors. Future research using stratified sampling to compare male and female experts and/or male and female lay users would be interesting to shed more light on this.

Third, retrospective face-to-face interviews are in principle vulnerable to social responsibility and memory bias. As a result, their self-reported behaviors might deviate from their actual behaviors. We tried to reduce social desirability bias by creating a confidential atmosphere in the interviews and, given the results of the interviews, we succeeded in this: Two-third of the participants confessed to pay moderate to very limited attention to their personal online privacy, not over-emphasizing their valuation of privacy. We tried to reduce memory bias by encouraging the participants to come up with specific examples. Future research might try to overcome these potential sources of bias by observing the actual behaviors of users, in real life or with scenarios.

Fourth, we compared the experts' knowledge and self-reported behaviors only to the aggregated insights from earlier research; we did not conduct the same study among experts and lay users. It would be interesting if future research would make a direct comparison of the behaviors of privacy and cybersecurity experts and lay users. This can be done in a qualitative study based on, for instance, scenario-based interviews or observations or in a quantitative pseudo-experimental design.

6. Conclusion

The purpose of this study was to examine the privacy perceptions and online behaviors of privacy and cybersecurity experts. Results show that experts' privacy valuation and reported online behavior is comparable to those of lay users. Despite their technical background and thorough understanding of privacy risks, the majority of experts often does not engage in better precautions online. Instead, experts often engage in 'hit-or-miss-analyses' of apps, which makes them vulnerable to heuristic thinking, immediate gratifications, or optimistic bias, too. Our results suggest that general privacy knowledge and privacy awareness do not play a decisive role in the occurrence of the privacy paradox among users.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by Dutch Research Council (NWO; grant number 628.001.011) in collaboration with TNO, the Research and Documentation Centre (WODC), and Centric.

References

Acquisti, A., 2004. Privacy in electronic commerce and the economics of immediate gratification. Proc. 5th ACM Conf. Elec. Commerce, 21-29. https://doi.org/10.1145/988772.988777.

Acquisti, A., Taylor, C., Wagman, L., 2016. The economics of privacy. J. Econ. Lit. 54 (2), 442–492. https://doi.org/10.1257/jel.54.2.442.

Bandara, R., Fernando, M., Akter, S., 2017. The privacy paradox in the data-driven marketplace. The role of knowledge deficiency and psychological distance. Proc. Comp. Sci. 121, 562–567. https://doi.org/10.1016/j.procs.2017.11.074.

Barnes, S.B., 2006. A privacy paradox: Social networking in the United States. Retrieved from First Monday 11 (9). http://firstmonday.org/article/view/1394/1312.

Barth, S., de Jong, M.D.T., 2017. The privacy paradox. Investigating discrepancies between expressed privacy concerns and actual online behavior. A systematic literature review. Telemat. Inform. 34 (7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013.

Barth, S., De Jong, M.D.T., Junger, M., Hartel, P.H., Roppelt, J.C., 2019. Putting the privacy paradox to the test. Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telemat. Inform. 41, 55–69. https://doi.org/10.1016/j.tele.2019.03.003.

Barth, S., Ionita, D., de Jong, M., Hartel, P., Junger, M., 2021. Privacy rating: a user-centered approach for visualizing data handling practices of online services. IEEE Trans. Prof. Commun. 64 (4), 354–373. https://doi.org/10.1109/TPC.2021.3110617.

Benenson, Z., Kroll-Peters, O., Krupp, M., 2012. Attitudes to IT security when using a smartphone. Proc. Feder. Conf. Comput. Sci. Inform. Syst. (FedCSIS), 1179-1183.

Benton, K., Camp, L.J., Garg, V., 2013. Studying the effectiveness of Android application permissions requests. Proc. IEEE Int. Conf. Perv. Comput. Comm. Workshops, 291-296. https://doi.org/10.1109/PerComW.2013.6529497.

Bräunlich, K., Dienlin, T., Eichenhofer, J., Helm, P., Trepte, S., Grimm, R., Seubert, S., Gusy, C., 2020. Linking loose ends. An interdisciplinary privacy and communication model. New Media Soc. https://doi.org/10.1177/1461444820905045.

Chin, E., Felt, A.P., Sekar, V., Wagner, D., 2012. Measuring user confidence in smartphone security and privacy. Proc. 8th Sympos. Usab. Priv. Sec., article 1. https://doi.org/10.1145/2335356.2335358.
Choi, H., Park, J., Jung, Y., 2018. The role of privacy fatigue in online privacy behavior. Comput. Hum. Behav. 81, 42–51. https://doi.org/10.1016/j.chb.2017.12.001.
Debatin, B., Lovejoy, J.P., Kathrin Horn, A.-K., Hughes, B.N., 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Comput.-Med. Comm. 15, 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x.
Deloitte., 2019. Global mobile consumer survey: US edition. A new era in mobile continues. https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-us-edition.html.
De Luca, A., Das, S., Ortlieb, M., Ion, I., Laurie, B., 2016. Expert and non-expert attitudes towards (secure) instant messaging. 12th Symp. Usab. Priv. Sec. SOUPS 147–157.
Deuker, A., 2010. Addressing the privacy paradox by expanded privacy awareness: The example of context-aware services. In: Bezzi, M., Duquenoy, P., Fischer-Hüber, S., Hansen, M., Zhang, G. (Eds.), Privacy and identity management for life, Vol. 320. Springer, pp. 275–283.
Dogruel, L., Joeckel, S., Bowman, N.D., 2015. Choosing the right app. An exploratory perspective on heuristic decision processes for smartphone app selection. Mob. Media Comm. 3 (1), 125–144. https://doi.org/10.1177/2050157914557509.
Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D., 2012. Android permissions: user attention, comprehension, and behavior. Proc. 8th Symp. Usab. Priv. Sec. 3 https://doi.org/10.1145/2335356.2335360.
Flender C., Müller G., 2012. Type indeterminacy in privacy decisions: The privacy paradox revisited, in: Busemeyer, J.R., Dubois, F., Lambert-Mogiliansky, A., Melucci, M. (Eds.), Quantum Interaction. QI 2012. Lecture Notes in Computer Science, 7620. Springer, Berlin. https://doi.org/10.1007/978-3-642-35659-9_14.
Fusch, P.I., Ness, L.R., 2015. Are we there yet? Data saturation in qualitative research. Qual. Rep. 20, 1408–1416. http://www.nova.edu/ssss/QR/QR20/9/fusch1.pdf.
Gallagher, K., Patil, S., Memon, N., 2017. New me. Understanding expert and non-expert perceptions and usage of the Tor anonymity network. Proc. 13th Symp. Usab. Priv. Sec., 385–398.
Hoffmann, C.P., Lutz, C., Ranzini, G., 2016. Privacy cynicism. A new approach to the privacy paradox. Cyberpsychol. J. Psychosoc. Res. Cyberspace 10 (4), article 7. https://doi.org/10.5817/CP2016-4-7.
Ion, I., Reeder, R., Consolvo, S., 2015. '... No one can hack my mind.' Comparing expert and non-expert security practices. Proc. 11th Symp. Usab. Priv. Sec., 327-346.
Joeckel, S., Dogruel, L., Bowman, N.D., 2017. The reliance on recognition and majority vote heuristics over privacy concerns when selecting smartphone apps among German and US consumers. Inform. Comm. Soc. 20 (4), 621–636. https://doi.org/10.1080/1369118X.2016.1202299.
Jorgensen, Z., Chen, J., Gates, C.S., Li, N., Proctor, R.W., Yu, T., 2015. Dimensions of risk in mobile applications. A user study. Proc. 5th ACM Conf. Data Applicat. Sec. Priv, 49–60. https://doi.org/10.1145/2699026.2699108.
Kang, R., Dabbish, L., Fruchter, N., Kiesler, S., 2015. 'My data just goes everywhere.' User mental models of the Internet and implications for privacy and security. Proc. 11th Symp. Usab. Priv. Sec., 39-52.
Kehr, F., Wentzel, D., Kowatsch, T., 2014. Privacy paradox revised. Pre-existing attitudes, psychological ownership, and actual disclosure. 35th Int. Conf. Inform. Syst., 1-12.
Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Inform. Syst. J. 25, 607–635. https://doi.org/10.1111/isj.12062.
Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C., 2013. Information disclosure on mobile devices: R-examining privacy calculus with actual user behavior. Inter. J. Hum.-Comp. Stud. 71, 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016.
Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., Wetherall, D., 2012. A conundrum of permissions. Installing applications on an Android smartphone. In: Blythe, J. (Ed.), Financial cryptography and data security. Springer, Berlin, pp. 68–79.
Ketelaar, P.E., Van Balen, M., 2018. The smartphone as your follower. The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. Comp. Hum. Behav. 78, 174–182. https://doi.org/10.1016/j.chb.2017.09.034.
Kumaraguru, P., Cranor, L.F., 2005. Privacy indexes: A survey of Westin's studies. Carnegie Mellon University, Pittsburgh, Pennsylvania.
Marshall, B., Cardon, P., Poddar, A., Fontenot, R., 2013. Does sample size matter in qualitative research?: A review of qualitative interviews in is research. J. Comp. Inform. Syst. 54, 11–22. https://doi.org/10.1080/08874417.2013.1164566.
Martin, K., 2013. Transaction costs, privacy, and trust: the laudable goals and ultimate failure of notice and choice to respect privacy online. First Monday 18 (12). https://doi.org/10.5210/fm10.5210/fm.v18i1210.5210/fm.v18i12.4838.
Odum, A.L., 2011. Delay discounting: trait variable? Behav. Process. 87 (1), 1–9. https://doi.org/10.1016/j.beproc.2011.02.007.
Park, Y.J., 2011. Provision of Internet privacy and market conditions: an empirical analysis. Telecomm. Pol. 35 (7), 650–662. https://doi.org/10.1016/j.telpol.2011.06.003.
Park, Y.J., 2015. Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. Comp. Hum. Behav. 50, 252–258. https://doi.org/10.1016/j.chb.2015.04.011.
Pentina, I., Zhang, L., Bata, H., Chen, Y., 2016. Exploring the privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. Comp. Hum. Behav. 65, 409–419. https://doi.org/10.1016/j.chb.2016.09.005.
Reidenberg, J.R., Breaux, T., Cranor, L.F., French, B., Grannis, A., Graves, J.T., Liu, F., McDonald, A., Norton, T., Ramanath, R., Russell, N.C., Sadeh, N., Schaub, F., 2015. Disagreeable privacy policies. Mismatches between meaning and users' understanding. Berkeley Tech. LJ 39. http://ir.lawnet.fordham.edu/faculty_scholarship/619.
Renaud, K., Volkamer, M., Renkema-Padmos, A., 2014. Why doesn't Jane protect her privacy?, in: De Cristofaro, E., Murdoch, S.J. (Eds.), Privacy enhancing technologies, PETS 2014. Springer, Cham, pp. 244–262. https://doi.org/10.1007/978-3-319-08506-7_13.
Schumacher, P., Morahan-Martin, J., 2001. Gender, internet and computer attitudes and experiences. Comp. Hum. Behav. 17 (1), 95–110. https://doi.org/10.1016/S0747-5632(00)00032-7.
Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., Borgthorsson, H., 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. Proc. SIGCHI Conf. Hum. Fact. Comput. Syst, 2347–2356. https://doi.org/10.1145/2556288.2557421.
Sim, J., Saunders, B., Waterfield, J., Kingstone, T., 2018. Can sample size in qualitative research be determined a priori? Int. J. Soc. Res. Methodol. 21 (5), 619–634. https://doi.org/10.1080/13645579.2018.1454643.
Simon, H.A., 1982. Models of bounded rationality. MIT Press, Cambridge, Massachusetts.
Statista, 2019. Number of mobile app downloads worldwide in 2017, 2018 and 2022 (in billions). https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/.
Sundar, S.S., Kang, H., Wu, M., Go, E., Zhang, B., 2013. Unlocking the privacy paradox: Do cognitive heuristics hold the key?. Proc. CHI '13 Extend.Abstr. Hum. Fact. Comp. Syst., 811-816. https://doi.org/10.1145/2468356.2468501.
Taddicken, Monika, 2014. 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. J. Comp.-Med. Comm. 19 (2), 248–273. https://doi.org/10.1111/jcc4.12052.
UWV (2018). Moeilijk vervulbare vacatures. Oorzaken en gevolgen voor werkgevers [Difficult to fill vacancies. Causes and consequences for employers]. https://www.uwv.nl/overuwv/Images/moeilijk-vervulbare-vacatures-oorzaken-en-gevolgen.pdf.
van Deursen, Alexander, van Dijk, Jan, 2011. Internet skills and the digital divide. New Med & Soc. 13 (6), 893–911. https://doi.org/10.1177/1461444810386774.
Veltri, G.A., Ivchenko, A., 2017. The impact of different forms of cognitive scarcity on online privacy disclosure. Comp. Hum. Behav. 73, 238–246. https://doi.org/10.1016/j.chb.2017.03.018.
Volkamer, M., Renaud, K., Kulyk, O., Emeröz, S., 2015. A socio-technical investigation into smartphone security. In: Foresti, S. (Ed.), Security and trust management. Springer, Cham, pp. 65–273. https://doi.org/10.1007/978-3-319-24858-5_17.
Westin, A.F., 1967. Privacy and freedom. Atheneum Books, New York.

Susanne Barth received the Ph.D. degree in Communication Science from the University of Twente, Enschede, the Netherlands, in 2021. Her Ph.D. project centered on privacy and security requirements for mobile applications. She currently works for a greentech company that develops innovative solutions for clean water, climate change, and circular waste disposal. Her research expertise is rooted within communication science and psychology, focusing on the human factor in technology and societal challenges intertwined with new media and technologies these days.

Menno D. T. de Jong received the Ph.D. degree in Communication Science from the University of Twente, Enschede, the Netherlands, in 1998. He is currently a Full Professor of Communication Science with the University of Twente. Between 2009 and 2015, he was the Editor-in-Chief of *Technical Communication*, the flagship journal of the Society for Technical Communication. He has authored or coauthored in a broad range of academic journals. His research interests involve the role of communication in societal challenges.

Marianne Junger received the Ph.D. degree in law from the Free University of Amsterdam, Amsterdam, the Netherlands, in 1990. She is the Emeritus Professor of Cyber Security and Business Continuity with the University of Twente, Enschede, the Netherlands. Her research investigates the human factors of fraud and cybercrime. More specifically, she investigates victimization, disclosure, and privacy issues. She co-founded the *Crime Science* journal and was an Associate Editor for six years.