Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones

Lydia Kraus, Ina Wechsung, Sebastian Möller
Quality and Usability Lab, Telekom Innovation Laboratories, Technische Universität Berlin
Email: {lydia.kraus, ina.wechsung, sebastian.moeller}@tu-berlin.de

***Abstract*—Much work has been conducted to investigate the obstacles that keep users from using mitigations against security and privacy threats on smartphones. By contrast, we conducted in-depth interviews (n = 19) to explore users' motivations for voluntarily applying security and privacy actions on smartphones. Our work focuses on analyzing intrinsic motivation in terms of psychological need fulfillment. Our findings provide first insights on the salience of basic psychological needs in the context of smartphone security and privacy. They illustrate how security and privacy actions on smartphones are motivated by a variety of psychological needs, only one of them being the need for *Security*. Moreover, the results illustrate how psychological needs can help to explain the adoption of security and privacy technologies and the interaction with those technologies. We further discuss how the design of security and privacy technologies could be guided by the gained knowledge.**

Keywords: Security and privacy; smartphones; psychological needs; user experience; user behavior

I. Introduction

Smartphones are an extensive source for positive user experiences: using a smartphone allows people to stay connected, to consume new games and media, or to "quantify themselves" with fitness and health monitoring apps.

While smartphones offer vast opportunities for positive experiences, threats to users' security and privacy emerge at the same time. Those include malicious apps, data loss, surveillance, and profiling, just to name a few.

Related work indicates that users are concerned about many of these threats and about their privacy on smartphones [1], [2], [3]. To mitigate these threats there is a variety of actions users can take [4]. Former works suggest to gain further insights into security and privacy aspects from an end-user perspective by using experiential approaches [5], [6]. In this context experience is seen as a holistic and broad view on the matter in order to gain a rich understanding of people's practices and lives [6]. Accordingly, while much work has been conducted to understand users' perceptions of smartphone security and privacy in terms of understanding [7], concerns [2], awareness [3], [8], attitudes [1], and feelings [9], we suggest using an experiential approach based on psychological needs to gain a deeper understanding of the matter.

User eXperience (UX) is a field of study which emerged between the mid-nineties and the turn of the millenium. In contrast to usability, which is mainly concerned with the functional aspects of technology usage, UX includes non-functional factors such as beauty and affective aspects of HCI [10]. Accordingly, UX is a multi-dimensional construct with a holistic view on the perceived product qualities (beyond usability), users' emotions, motivations, usage situations, and other dimensions (for a literature review of UX dimensions and study methods refer to [10]).

In our paper, we focus on the motivational dimension of user experiences in terms of psychological need fulfillment. Psychological needs have been suggested in several theories as an explanation for human behavior: for instance, self-determination theory suggests basic psychological needs as the fundamental mechanism for self-motivation [11]. Furthermore, it has been shown that need fulfillment is related to satisfying events and positive affect [12]. In the context of user experience research, Hassenzahl et al. [13] show that the main motivation to use an interactive technology is the fulfillment of psychological needs; a positive user experience is thus the result of need fulfillment [13].

A user for instance makes a phone call to experience the feeling of being close to others (thus, the motivation would be the fulfillment of the need *Relatedness*), rather than for the call's sake (example taken from [14]). Or, a user activates the privacy setting in a messaging app so that the sender of the messages cannot see when a message was read. This avoids the pressure to reply immediately to a message. In this case, the privacy setting is used to fulfill the basic psychological need of *Autonomy*. Psychological need fulfillment is a primary goal which all users have in common, the instantiation of the primary goal - the experience - is however highly context-dependent and subjective [14].

The goal of this paper is to learn about the psychological needs which users intend to fulfill with security and privacy actions on smartphones. We conducted semi-structured in-depth interviews with 19 users to explore the security and privacy actions which users employ on their smartphones and the reasons for them. Our findings illustrate how a variety of psychological needs drive those actions, only one of them being the need for *Security*. This knowledge can help to establish a new design space for positive user experiences

EuroUSEC '16, 18 July 2016, Darmstadt, Germany
Copyright 2016 Internet Society, ISBN 1-891562-45-2
http://dx.doi.org/10.14722/eurousec.2016.23009

induced by security and privacy actions on smartphones (cf. also Section V).

Contributions:

- We explore the motivational factors for security and privacy actions on smartphones in terms of psychological need fulfillment.
- We discuss how psychological needs can support the explanation of user behavior related to the adoption of and interaction with security and privacy actions.
- We provide examples on how to include psychological needs in the design of security and privacy technologies on smartphones.

Structure: After detailing related work on security and privacy actions on smartphones, user experience, and psychological needs in Section II, the interview methodology is presented in Section III. The interview results are reported in Section IV and discussed in Section V. We further discuss possibilities to use psychological needs as a design inspiration for security and privacy mechanisms in Section V.

II. Related Work

Much work has been conducted to describe user practices, concerns, and usability issues related to smartphone security and privacy. Despite the known usability issues of security mechanisms, users report being interested in applying further such mechanisms [15]. In the following, an overview of the main security and privacy actions users could deploy on their smartphone is presented. Those actions were also covered in the interviews which were conducted for this paper.

A. Usability and adoption of smartphone security and privacy mechanisms

Scrutinizing app permissions is an indispensable action to avoid privacy intrusions and security issues on smartphones [4]. In the past, the implementation of the permission model differed between smartphone operating systems (OSes): Whereas iOS users were shown a permission-request as soon as an app requested it for the first time, android users had to accept all permissions or groups thereof before an app could be installed. In this implementation, Android permissions showed to be difficult to understand for users; also, the permission requests were shown at an unfavorable point in the decision making process, that was when the decision to install an app has already been made [7]. Several solutions have been suggested to increase the understanding of and the attention towards permissions including improved information presentation and risk communication (cf. e.g. [16], [17], [18], [19]). In 2014, the Android permissions were grouped and their presentation was modified to include icons for each group. While this improved information presentation, security concerns remained [20]. The newest Android version (6.0), released in 2015, enables users to grant or not to grant single permissions for each app [21]. However, as of March 2016, Android 6.0 still has a negligible market share (2.3%) in the studied population [22]. Thus, the above described issues are still relevant.

A method to protect a smartphone from unauthorized access and subsequent privacy intrusions or security issues is the deployment of a screen lock together with an authentication method, such as a password or a PIN [4]. However, unlocking a smartphone with an authentication mechanism is time-consuming [23]. In a study of 2011, the PIN was perceived as a reliable method for protecting a mobile phone by only a quarter of users (26%) [15]. Nevertheless, as of 2014, many users are using a PIN or password to protect their device: 66% of users in Germany use a screen lock with a password [24]. A viable alternative to knowledge-based authentication methods are biometric methods such as Touch ID on iPhones and face unlock on Android devices [25]. Biometric methods, however, also rely on PINs or passwords for fallback authentication.

Regarding communication, eavesdropping and interception pose a threat. They can be mitigated by deploying end-to-end encryption of communication (calls and/or messages) [26]. Only recently, Whatsapp, one of the most popular instant messaging services for Smartphones, has announced the implementation of end-to-end encryption which is activated by default [27]. However, the usage of instant messaging services is not only accompanied by the risk of being eavesdropped, but also by the risk of privacy intrusions by other users. The latter can be counteracted by appropriate privacy settings. For instance, Rashidi and Vaniea report that many users actively use the privacy settings of Whatsapp - in a survey among Saudi Arab users almost a third of the respondents hid their last seen notice [28].

Another security threat, malware, might be mitigated by antivirus apps which can be easily installed for Android; however, their usefulness is questionable [29]. Likewise, the usage of security software is considered by many users as nonessential [3]. Keeping the device up-to-date is another mitigation strategy against malware. However, in a case study on update installation behavior, many users of an Android app did not immediately install updates - a behavior which may result in security vulnerabilities [30].

Threats may also arise from the device being unavailable due to denial of service attacks or exhausted battery power [26]. For counteracting the former, a resource management solution may be installed; these kind of applications are, however, difficult to implement [26]. A study by Chin et al. also showed that users worry about limited battery lifetime [1] when asked about concerns related to smartphone usage.

Data loss due to device loss or theft can be easily mitigated by backups. While users are concerned about the latter threats [1], other tools to mitigate negative consequences in case of theft or loss such as remote data wipe, device locators and device encryption are poorly adopted [3]. This might be due to unawareness towards the existence of such features [1].

Chin et al. conducted a detailed study of users' practices on smartphones and their perception of security and privacy [1]: they found that users worry about the threats of physical theft or damage, data loss and insufficient back up, malicious apps and wireless network attackers, limited battery lifetime, and signal strength. Users' practices to protect from those threats may however have limited effectiveness. In some cases users deduce trust indications from indicators not meant as such. For instance, much value is put on other users' reviews in the app repository [1]. Kraus et al. investigated in a qualitative study which threats and mitigations on smartphones are known to users and how they perceive them: users reported different feelings including social pressure, helplessness, dependency, and fatalism [9]. They suggest that the reasons for those negative feelings may be grounded in a lack of psychological need fulfillment. Nevertheless, in their study, the use of self-reported mitigations was related to positive feelings such as trust and feelings of being able to exercise control[1] [9].

Related work suggests that users worry about threats to their security and privacy on smartphones and that many users are willing to adopt mitigations. However, usability shortcomings of mitigation technologies on smartphones and users' mixed feelings regarding threats and mitigations call for an approach that focuses on new methods to enable positive user experiences when applying security and privacy actions.

B. Experiential approach to security and privacy

The necessity to include principles from user experience research into the design of security and privacy technologies has been recognized before. For example, Bødker et al. suggest that experiential approaches should be used to understand user behavior in the IT-security domain [5]: "In daily life, people rarely do activities solely for the purpose of security. Instead, most IT-security decisions are part of other activities with other purposes. When analyzing these use situations it is impossible to isolate IT-security tasks or decisions." Hence, security is dependent on context and usage motives, and not only on a secure device and the implemented security procedures [5]. By gaining an understanding of users' motivation in terms of psychological needs, our paper sheds lights on this issue.

Dunphy et al. [6] note that experience design faces a special challenge when it comes to security and privacy applications as within those applications two kind of users need to be taken into account: the target user and the adversary; moreover, a user might switch between being a targeted person and being an adversary depending on the context. For example, users can become adversaries when they start intruding the privacy of people with whom they interact in social networks. Gaining an understanding of target users' motivation in terms of psychological needs could also help to explain these kinds of situations.

C. Psychological needs

Sheldon et al. [12] investigated the relationship between psychological needs and satisfying life events. They selected 10 psychological needs according to well-known theories of psychological need fulfillment (such as Deci and Ryan's self-determination theory [31], Epstein's cognitive-experiential self-theory [32]) and found that *Self-esteem*, *Autonomy*, *Relatedness* and *Competence* are the most salient needs in the context of satisfying life events. Their results were shown to be stable over time and across cultures.

Hassenzahl [14] took up the needs suggested by Sheldon et al. [12] and related them to a model of user experience. Psychological needs are used to describe classes of experiences [14]. This is done by considering different types of goals that underlie an action; do-goals and be-goals are differentiated[14]. Do-goals are derived from higher-level be-goals that are the fulfillment of an underlying need. A user, for instance, makes a phone call to experience the feeling of being close to others. Thus, the be-goal is feeling close to others (i.e. the fulfillment of the need *Relatedness*). The do-goal is the action of making the call (example taken from [14]). The fulfillment of psychological needs (the be-goal) leads to a positive user experience [13].

While psychological needs serve to describe motivational aspects and thus allow for making interpretations of users' behavior, they can also serve as an inspiration for product design [14], [33]. Studies show that need fulfillment can be manipulated through product features leading to a positive change in user experience evaluations [33], [34]. Also, users' judgement of a system's hedonic quality, i.e. quality aspects beyond the functional, is influenced by need fulfillment [14]. However, this depends on the attribution, i.e. the degree to which users deem the product responsible for the experience [14].

The study presented in this paper is based on the needs as defined in Sheldon et al. [12]. The usefulness of this set of needs in the context of HCI has previously been shown by Hassenzahl et al. [13]. Fronemann and Peissner [33] also build upon a set of psychological needs defined by Sheldon et al. [12] and Reiss [35]. An additional need they define which is not covered by the definitions of Sheldon et al. [12] is *Keeping the meaningful* [33]. We too included this need into our study. In the following, definitions of the psychological needs which we used in our research are provided.

Autonomy: *"Feeling like you are the cause of your own actions rather than feeling that external forces or pressures are the cause of your actions."* [12]
Competence: *"Feeling that you are very capable and effective in your actions rather than feeling incompetent or ineffective."* [12]
Relatedness: *"Feeling that you have regular intimate contact with people who care about you rather than feeling lonely and uncared for."* [12]
Self-actualization: *"Feeling that you are developing your best potentials and making life meaningful rather than feeling stagnant and that life does not have much meaning."* [12]
Security: *"Feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances."* [12]
Popularity: *"Feeling that you are liked, respected, and have influence over others rather than feeling like a person whose advice or opinions nobody is interested in."* [12]
Money/Luxury: *"Feeling that you have plenty of money to buy most of what you want rather than feeling like a poor person who has no nice possessions."* [12]
Physical/Bodily: *"Feeling that your body is healthy and well-taken care of rather than feeling out of shape or unhealthy."* [12]
Self-esteem: *"Feeling that you are a worthy person who is as good as anyone else rather than feeling like a 'loser'."* [12]
Stimulation: *"Feeling that you get plenty of enjoyment and pleasure rather than feeling bored and understimulated by life."* [12]

[1] Note, that the actual and perceived security of what users consider to be a mitigation can vary greatly and will not be discussed at this point.

Keeping the meaningful: *"Collecting meaningful things"* [33]/*"saving"* [35]

III. Methodology

Following the description of be-goals and do-goals, psychological needs are related to the question why something is done whereas actions are related to the question what is done and how it is done [14]. Therefore the script for the semi-structured in-depth interviews concerned the following research questions:

- Which security and privacy actions are employed by smartphone users? *(What?)*
- How are they employed? *(How?)*
- Why are they employed? *(Why?)*

The interview script can be found in the appendix of this paper. With this approach participants were not explicitly asked for the needs they aim to fulfill with their actions. Therefore, we considered the why-questions to provide answers regarding the reasons for doing an action and we coded those reasons with the psychological needs.

The interview script covered a variety of possible actions, extracted from the literature on smartphone security risks [4], [26] and users' threat perception [1]. Action-questions were intentionally designed in an open manner as we did not want to assume that users only stick to the actions which are defined in the literature. The salience of the topics security and privacy increased during the course of the interview.

The interview was divided into three parts. In the first part, participants were asked about their general smartphone usage habits, e.g. reasons why they bought a smartphone, which operating system they use, and if they have used another operating system before. Then they were asked about smartphone sharing and usage at work. Afterwards, several questions on app usage, app installing, and uninstalling were asked. Some of the questions were taken from [1].

In the second part of the interviews, the central themes were security and privacy actions, including questions about the first time that participants set up their smartphone, usage of data connections, installing of updates, usage of pre- and postpaid options, battery consumption, theft protection, backups, internet usage, financial functions, protection from app access to sensitive information and communication.

In the third part, questions covered security and privacy software usage, password lock usage, and thoughts on general threats of smartphone usage. For each question of the interview, the interviewers were instructed to ask follow-up questions on reasons and triggers for behavior.

A. Procedure

The interviews were conducted in German in the beginning of 2015 at our lab. Each interview was conducted by one interviewer. To reduce interviewer effects, there were two interviewers. Approximately half of the interviews were conducted by Interviewer 1, the other half by Interviewer 2. Audio recordings were taken to enable verbatim transcription after the interviews. The audio recordings were deleted after the transcription process. The sessions took between 20 and 40 minutes depending on how talkative the participants were. Participants received 12 EUR reimbursement. At the beginning of the interview, participants received an information sheet and were asked for consent. Then, questions on demographics, smartphone usage (frequency of use, etc.), privacy concern and ICT attitudes were presented to the participants. During the recruitment we did not mention that the interview is about security and privacy, but we told the participants that we are interested in their smartphone usage habits.

At the end of the interviews the participants were thanked and debriefed. Due to the nature of the interview it might have been that the participants became aware of shortcomings in their security behavior. Therefore, after the interview, they were provided with a flyer on which they could find further information on how to protect their security and privacy on smartphones.

B. Analysis

The codebook consisted of the descriptions of the 11 psychological needs (cf. Section II), the items of the need fulfillment questionnaire [12], and a few items of the UNEEQ questionnaire (only for *Keeping the meaningful*) [36]. Thus, the codes could be used for either need fulfillment or frustration.

Two coders independently coded the interviews by applying the codebook described above. Interrater-agreement between the two coders was found to be moderate (Cohen's κ = 0.46) according to Landis and Koch [37]. The disagreements between the coders stemmed from a few issues. During the coding, the coders came across many passages in which participants told that they would do an action in order to save money. However, saving money is not explicitly part of the definition of the need *Money/Luxury* as described in Section II. Nevertheless, in most passages related to saving money, participants were willing to corrupt their privacy or security in order to get access to nice possessions. For instance, they said that they would choose the free version of an app rather than the paid version, although the free version required more permissions. Thus after discussion, the coders decided to label these passages as *Money/Luxury*. The coders also discussed about the *Security* code. This code was rather found in the context of *being safe from threats* than *having a need for structure or control*. The coders agreed that the first definition is valid as it can be found in the questionnaire on need fulfillment [12]. There was also disagreement on whether situations in which the participants reported the desire that others cannot track or observe them should be coded as *Security* or *Autonomy*. This is a typical situation related to privacy; however, a need for privacy is not part of the needs suggested in the related literature (cf. Section II). In the end, the coders agreed on coding these passages as *Autonomy* - in line with Westin's definition of the functions of privacy, one of them being personal autonomy [38]. In the following we use the coded transcripts upon which the coders finally agreed.

Additionally to the analysis of the psychological needs, a list of security and privacy actions was extracted from the data by the coders. Actions in the list include actions as defined in the literature [4], [26] and actions which were additionally mentioned by the participants. Based on this list, the coders analyzed independently whether an action was applied by a participant or not. For the coding of the actions, the coders reached almost perfect interrater-agreement (Cohen's $\kappa = 0.84$) according to Landis and Koch [37]. The coders met to discuss disagreements and to reach consent. Table I reports the results upon which the coders agreed.

C. Participants

19 smartphone users (10 female) were recruited from a panel of our institution. The age ranged from 18 to 58 years with an average of 31 years. Participants had diverse educational levels (approximately equally distributed among secondary school degree, qualification for university entrance, and university degree). Among the sample were 9 employees, 7 students and 3 job seekers.

D. Smartphone usage

There were 13 Android users, 5 iPhone users and 1 Windows Phone user. The sample roughly reflects the distribution of smartphone operating systems among the smartphone user population in Germany at the time of the study (Android 70%, iOS 20%, Windows Phone 5%) [39]. Smartphone usage experience among the participants was diverse: 4 participants had owned their smartphone for less than a year, 7 for 1-3 years and 8 for more than 3 years. Most of the participants use their smartphone at least once per hour (N=15). Only one participant had a professional IT background.

IV. Results

Participants reported the application of many security and privacy actions. Those actions largely rely on either mindfulness or pre-installed mechanisms. The psychological needs motivating the application of the reported actions are diverse: besides *Security* which was likely to be a motivator due to the nature of the interview, *Autonomy* and *Money/Luxury* play a major role. *Competence*, *Relatedness*, and *Stimulation* were found to be of moderate importance. *Keeping the meaningful* and *Popularity* were only relevant for a few actions. *Self-actualization*, *Physical/Bodily*, and *Self-esteem* were found to play a minor role as motivators.

The results of the psychological need analysis are structured according to the macro-structure of the interview script. For each subsection, the 2-3 most mentioned needs are discussed.

A. Security and privacy actions

An overview of the reported actions is provided in Table I. Saving battery lifetime was reported most frequently, followed by switching off all data connections, deploying updates and protecting the device from theft.

Neither the installation of nor the subscription to additional apps or services is required for the 10 top strategies as those strategies are either based on mindfulness or on pre-installed security/privacy mechanisms. Examples for the latter include screen lock with authentication or backups to the cloud (if the backup app was pre-installed).

Note, that actions encompass what the participants have reported, not what they may actually use. For example, iPhone users may not have been aware that encryption on iOS is enabled by default when using a screen lock with authentication. Further note, that end-to-end encryption was not implemented in many messaging apps by the time of the study. Thus, the use of messaging apps with end-to-end encryption was interpreted as a separate action. Table I does not take into account intensity and frequency of the deployed actions. For example, for "checking permissions" there may be participants who check app permissions everytime, while other participants may only check them when they are suspicious for some reason.

Security and privacy actions	freq.	%
Save battery lifetime	18	95%
Switch off all data connections (e.g. by flight-mode)	17	89%
Deploy updates	16	84%
Protect from theft (e.g. by securely storing the device)	14	74%
Check permissions	14	74%
Make backups	14	74%
Use screen lock with authentication	12	63%
Avoid financial apps/ functions (e.g. online banking)	10	53%
Check monthly bill/ prepaid balance	9	47%
Disable WiFi connection	6	32%
Disable Bluetooth	5	26%
Disable GPS	4	21%
Hide one's identify (e.g. by fake user profiles)	4	21%
Reduce online "data traces"	3	16%
Adjust privacy settings of messaging apps	3	16%
Use antivirus apps	3	16%
Log out from services	3	16%
Take out insurance	3	16%
Use remote management apps	3	16%
Do not use messaging apps	2	11%
Use apps for privacy protection/ permission management	2	11%
Use messaging apps with end-to-end encryption	2	11%
Modify privacy settings of the device	1	5%
Uninstall pre-installed apps	1	5%
Root the device	1	5%
Do not download apps at all	1	5%
Use data/ device encryption	0	0%

TABLE I. Self-reported security and privacy actions. Percentages do not sum up to 100 as participants could report several actions.

In the following we report the psychological needs related to the different actions.

B. Saving battery lifetime

From an IT-security perspective the (automatic) monitoring of battery consumption may be used to detect malicious activities on a device [26]. While users could also regularly check their battery status to detect apps that unnecessarily drain energy, the participants in our study mentioned checking their battery status as a safety measure: they reported to save battery lifetime to be, for example, available for friends. Thus, *Relatedness* is one reason for saving battery lifetime. P12 mentioned that he started to check his battery status regularly as there have been situations where "I was somehow absentminded and my battery only had 30%, but I was somewhere outside for let's say five or six hours; well, I need to be available for friends or so."

Another reason for saving battery lifetime is *Security*, as evident in the statement by P9: "Mhm well, in fact [...] it happens quite often, that I need to find my way home via Google Maps or public transport and therefore I always want to have at least 10% battery left and that's why... that's why I save battery".

C. Connectivity

When we asked the participants about situations in which their data connections such as Bluetooth, NFC or GPS are disabled, we expected that they report on turning off WiFi for example in order to avoid network attacks. Instead, most of the participants mentioned situations in which they switch off all data connections (e.g. by activating the flight mode). This behavior is driven by the need for *Autonomy*: "I don't need to be available all the time, well, I can be without my mobile phone" (P11). "Because I want to be let alone" (P9). "I always disabled it [all data connections] at work, so that I don't get distracted" (P15). *Money/Luxury* is another reason why data connections are switched off. P17 noted: "[...] when I am at home then I use WiFi and switch off my mobile internet, because I think I can save some of my data contingent doing so at least that is how I understood it." However, for few participants, a need for *Security* was found related to the usage of public WiFi spots: "Well, for me that is... open WiFi is too risky for me." (P15)

D. Updates

Updates were seen as a source for *Stimulation* rather than a necessity in terms of *Security*, for instance by P8: "Yes, if there are new updates I install them so that I have the latest version [of an app]." Doing updates manually provides *Autonomy* for some of the participants: "In certain intervals, maybe once per month, I enter Google Play and then I check which apps I have [on my phone] and for which of those apps updates are needed. Then I decide what I update or what I don't update" (P2).

E. Protection from theft

Interestingly, instead of using remote management apps or the like, many of the participants mentioned that they store their device securely or that they pay attention to where they leave the device. This provides them with a feeling of *Security*, as can be seen in the quote by P15: "It's always strange, when it [the phone] is somewhere else, for example in my backpack; I'd rather carry it on me, then I know it's there and I notice relatively quickly if it would be gone." P12 stated: "I just do it [storing it securely] as a preventive measure, just not to be placed in such a situation [that the phone is stolen]."

F. Screen lock with authentication

Not surprisingly, most quotes related to screen locks with authentication were coded with *Security*, an example is the following quote by P8: "Uumh, if it [the phone] is stolen or so, [for the thief] it wouldn't be so easy to use it immediately." P6 noted as a reason to use password lock: "I believe that it's maybe... In case that one loses the phone, it is a bit more difficult [to access it]." *Security* and *Popularity* as reasons to adopt a password lock were mentioned by P5: "In the beginning it was, because I thought it is pretty cool how my friends typed in their security codes on their mobile phone. Now it is just for security reasons." Thus, for P5 locking mechanisms have the potential to convey the impression of being "cool" to others.

G. App selection, uninstalling apps and mitigating access to sensitive information

When it comes to app selection *Stimulation* plays a major role as noted by P11: "sometimes I check the category 'newest apps' and those that sound interesting will be downloaded." Also, the influence of the price, i.e. *Money/Luxury*, was mentioned by several participants, for instance in this quote: "Well, there are enough [apps] for free" (P17).

Security may be a decision factor in the app selection process, as noted by P3: "It depends on what kind of app it is, how urgent do I need that app? Well, if I want to download some game just for fun and [then I] see 'Okay, the App wants to have access to everything', [...] than I just dont install it." P4 mentions *Security* concerns during app selection: "[...] but then sometimes I do worry, a self-employed developer, what kind of mischief they could do."

A feeling of not being *competent* when it comes to judging permissions was expressed by P7: "Therefore I don't see myself in the position, to switch those things [the permissions] off; I think that I am allowing it [having access] to some apps."

Autonomy is experienced by not allowing apps to access location data "[I switch off GPS] because I do not want, that someone who should not know it, knows where I am." (P11). When it comes to uninstalling apps, *Autonomy* is a reason, as evident from this statement by P12: "Simply because I don't want Apple to know where I am or something like that". However, also *Money/Luxury* may be a reason for uninstalling an app: "Well, sometimes there are apps which are advertised to be free of charge and then you only got a couple of functions and you have to pay for many other functions. And well then I rather uninstall those apps because it annoys me." (P13).

H. Backups

Security and *Keeping the meaningful* were the only reasons that were salient in the context of backups: "Yes, because the data on my mobile phone is important to me... and well it is better... safety comes first." (P8). Unsurprisingly, the desire to keep (meaningful) things is related to the subjective value that the participants attach to them, as implied by this statement by P3: "Well, I am a person who loses his mobile phone quite often, and, well I was in Brazil and took some pictures there. And after two weeks of traveling I dropped my mobile phone in a river. Well, then I thought 'mhh damn it'. I got my phone to work again, but then I uploaded everything to the cloud well, so that I do not lose all my pictures [...]."

I. Communication

Being in contact with people one cares about, i.e. *Relatedness*, was mentioned by many of the participants as a reason for using messaging apps: "The reason for using it [WhatsApp] is actually that all my friends are using it, otherwise I would like to use another one [app]." (P9). "Because everyone used to use it and if you did write an SMS, then you were kind of out and well then you just used it too. Last year I tried to get rid of WhatsApp, but there are still too many people who still got it and won't write SMS and well then you just have to get back to WhatsApp." (P15).

When we asked the participants if they do something in order to protect their communication, we expected that they would mention end-to-end encryption or the like. However, only one participant reported to use it. Instead many said that they use privacy settings in messaging apps. We labeled these statements with *Autonomy*: “I wouldnt describe it as a protection measure, but for WhatsApp I turned off, that you can see when I was online the last time or stuff like that... well.” (P3). Group chats in messaging apps were seen as a possible source of unpleasant consequences by P6: “Yes, so, I am careful when it comes to these group... group-chats or things like that. I do not use them, because I think they are quite precarious [...].” Therefore, this quote was coded with *Security*.

Summarizing, we found a variety of examples how psychological needs, i.e. be-goals, drive security and privacy actions on smartphones: for instance, the participants reported *Relatedness* and *Security* as motivators for saving battery lifetime; they further reported that *Autonomy*, *Money/Luxury*, and *Security* are playing a role in managing connectivity; they also mentioned that *Stimulation* and *Autonomy* motivate actions related to updates and that the need for *Security* motivates the protection from theft; *Security* was mainly mentioned as motivator for using a screen lock with authentication, however, there is also a potential for *Popularity* being addressed with this action. App selection was noted to be driven by *Stimulation* and *Money/Luxury*, whereas *Security*, *Competence* (or a lack thereof) and *Autonomy* were reported to be related to uninstalling apps and mitigating access to sensitive information. The interviews further indicated that backups are motivated by *Keeping the meaningful* and the need for *Security*; communication is related to *Relatedness*, whereas its protection is related to *Autonomy*, and *Security*, both rather in the context of threats arising from other users.

V. Discussion

Our findings indicate that users apply diverse security and privacy actions to protect themselves from threats on their smartphones. Quantifying the effectiveness of these actions is out of the scope of this paper. However, the mere finding suggests a huge design space for future security and privacy technologies. Our results further illustrate how a variety of psychological needs drive security and privacy actions on smartphones. How psychological need fulfillment can be included into the design of security and privacy technologies, is discussed in the following.

A. Limitations

Our study is of qualitative nature, thus, we do not aim to infer any statements on the importance of each need for each action. Need fulfillment is on the one hand context-dependent. On the other hand, there may be some needs which are especially important for specific actions. Quantifying them is subject to quantitative studies, for which our paper provides a profound basis.

The interviews were annotated with predefined concepts from theories of psychological needs. This is a subjective process and it might be that some quotes could be interpreted in a different way. The moderate inter-rater agreement indicates that the application of psychological needs in the context of security and privacy on smartphones may profit from further conceptualization and specification. We leave additional conceptualizations to future work for which our paper provides a good starting point.

Our study sample consisted partly of students and job seekers which might have led to the result that saving money was a rather salient motive in the decision making process. Despite this limitation, our sample reflects well the smartphone operating system distribution in the studied population. Studies aiming at quantifying and generalizing the results, should however, administer a sample which is representative w.r.t. to further population characteristics.

B. Psychological needs as an explanation for user behavior

The results of the interviews indicate that a variety of psychological needs is salient in the context of security and privacy actions on smartphones. As psychological needs can be considered as high-level primary goals (“be-goals” [14]), our results provide insights into these primary goals and how they are aligned (or not) with security and privacy actions. For instance, backups may be motivated by the need for *Keeping the meaningful* rather than for the sake of *Security* only. A password lock for the smartphone screen may be used to achieve a feeling of *Security*, but it may be also motivated by the need for *Popularity*. This is the case when its usage is perceived as “trendy”. Data connections may be switched off for privacy reasons (i.e. *Autonomy*), but also for *Security* reasons or to save money (i.e. *Money/Luxury*). Using certain messaging apps may be motivated by the need for *Relatedness* rather than the need for *Security*, but the communication itself might be regulated through privacy settings whenever there is a need for *Autonomy*. App selection can in some cases be driven by the need for experiencing new things (i.e. *Stimulation*); in other situations users check the permissions thoroughly to avoid being surveilled by privately owned companies (i.e. the emphasis is on the need for *Autonomy*). Concerning communication, *Relatedness* is a motivator for the adoption of messaging apps and communication protection is driven by *Autonomy* and the need for *Security*.

Security or privacy are often considered as secondary goals [40]. However, one could have expected that for users of security and privacy actions on smartphones, security and privacy would be primary goals. Nevertheless, the interview results indicate that even for security and privacy actions the need for *Security* is only one primary goal among others. Which psychological need users intend to fulfill depends on the one hand on contextual factors. On the other hand, there may be groups of users with similar characteristics that intend to fulfill a specific need with a specific security and privacy action. We plan to conduct further studies to examine the relationships between context, user characteristics and psychological need fulfillment for security and privacy actions on smartphones.

C. Using psychological needs in the security and privacy context

During the analysis of the psychological needs, we have made a number of assumptions regarding their interpretation.

We have interpreted the desire for privacy as being related to *Autonomy*. Pedersen [41] and Westin [38] suggest that there is a variety of privacy behaviors which are driven by further functions (besides *Autonomy*) such as emotional release, self-evaluation, and limited and protected communication [38]. We suspect that including the privacy functions will lead to a better conceptualization of psychological needs in the context of security and privacy research. We plan to conduct further studies to investigate how the functions defined by Westin and Pedersen can be integrated into the concept of psychological needs. We further interpreted *Money/Luxury* to include the desire to save money. However, this desire could be rather an extrinsic motivational factor than an intrinsic motivational factor (psychological needs are considered as intrinsic motivators). Thus, saving money may not lead per se to a positive user experience and may be rather a necessity than a reason. This issue should be considered in future studies.

D. Psychological needs as design inspiration for security and privacy technologies on smartphones

Addressing psychological needs in security and privacy technologies for smartphones creates a new design space for such technologies. In the following, we provide examples on how security and privacy technologies that support psychological need fulfillment could look like.

1) Authentication: We suggest improving the user experience of password locks by addressing additional needs besides *Security* such as *Stimulation* (e.g. by making unlocking fun) or *Popularity* (by having a "cool" screen lock). There are a few examples for addressing *Stimulation* in terms of joy during authentication: related work shows that for instance gesture-based authentication is able to evoke different positive emotional outcomes. Aumi et al. [42] present an authentication system which is based on in-air gestures performed in the vicinity of a portable device. In a user study they show that the gestures' security is positively correlated with ratings of pleasantness and excitement. Moreover, Karlesky et al. [43] find full-body gestures for access control to provide a potential for interactions which are perceived pleasurable by users. *Popularity* in authentication mechanisms could be addressed by providing users with a "cool" authentication method. For example, Bhagavatula et al. find that fingerprint authentication on smartphones is perceived as "cool" [25]. Also, many solutions to improve usability of knowledge-based authentication methods have been suggested in the domain of graphical authentication [44]. It is subject to future research to investigate whether those solutions could provide for better need fulfillment and a positive user experience. Furthermore, we plan to investigate in future studies how psychological needs such as *Stimulation* and *Popularity* can be systematically addressed in the design of mobile authentication methods.

2) Updates: Participants in our study mentioned installing updates to get the newest version of an app. By definition, experiencing new things is associated with the need for *Stimulation*. However, this applies only if the new experience is positive. Vaniea et al. [45] show that users become frustrated when installing updates that feature new user interfaces that interrupt the users' normal workflow. Thus, updates are a two-edged sword: on the one hand they are able to positively surprise users when new functionalities or features are added to an app, thus addressing the need of *Stimulation*. On the other hand, users who have had bad experiences with installing updates may refrain from installing them in the future which may lead to security vulnerabilities [45]. One option to avoid negative effects on users' security behavior is to separate security updates from other updates [46]. Thereby, in the best case, users will not experience any changes after installing a security update. Nevertheless, it may also be the case, that updates just for security purposes are not deployed. Thus, an approach based on psychological need fulfillment could be to motivate users to install security updates by connecting these updates with stimulating experiences. For instance, appraisal messages could be shown or gamification approaches could be used to achieve such experiences. How approaches that address psychological needs in update messages could look like in detail, is an interesting research question for future studies.

3) App Permissions: Not only in our study, app permissions proved to be hard to understand by some of the participants (cf. also [7]). As a consequence, the psychological need of *Competence* may be deprived. On the other hand, our results suggest that users appreciate having the possibility to autonomously select which permissions they grant (for instance with respect to location data). Providing users with a clear context to make a decision is in any case recommendable [40]. Related work also indicates that a clear context supports security-friendly decisions when granting permissions [17], [18]. Whether this approach is also capable to address users' need for *Competence* and inducing a positive user experience is a subject for future studies. Another worthwhile topic for future studies is to investigate to which degree run-time permissions (as currently featured in iOS and Android 6.0) are perceived as fulfilling the need for *Autonomy* without being annoying.

In summary, our results illustrate how psychological needs can be used as high-level primary goals for the explanation of user behavior related to security and privacy actions on smartphones; moreover, they provide new inspirations for the design of security and privacy technologies on smartphones. How the psychological needs can be systematically addressed in the design of security and privacy technologies on smartphones is an interesting research topic for future studies.

VI. Conclusion

We conducted semi-structured in-depth interviews with 19 participants to investigate the psychological needs that drive security and privacy actions on smartphones. Our results show a variety of self-reported actions and illustrate how those actions are motivated by a variety of psychological needs, beyond the need for *Security*. Our results provide examples on how psychological needs can be used as high-level primary goals to explain user behavior related to the adoption of security and privacy actions on smartphones; furthermore, they provide design inspirations for new versions and future prototypes of security and privacy technologies. Our paper offers a basis for further conceptualizations and for elaborating on the potential that the application of psychological needs offer in the security and privacy context.

VII. Acknowledgments

This work was funded by the EU FP-7 support action ATTPS under grant agreement no. 317665. We would like to express our gratitude to Tobias Fiebig for his assistance in preparing the interview study and to Maija Poikela for proofreading the paper.

References

[1] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, “Measuring user confidence in smartphone security and privacy,” in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 1.

[2] 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*. ACM, 2012, pp. 33–44.

[3] A. Mylonas, A. Kastania, and D. Gritzalis, “Delegate the smartphone user? security awareness in smartphone platforms,” *Computers & Security*, vol. 34, pp. 47–66, 2013.

[4] G. Hogben and M. Dekker, “Smartphones: Information security risks, opportunities and recommendations for users,” *European Network and Information Security Agency*, vol. 710, no. 01, 2010.

[5] S. Bødker, N. Mathiasen, and M. G. Petersen, “Modeling is not the answer!: Designing for usable security,” *interactions*, vol. 19, no. 5, pp. 54–57, Sep. 2012. [Online]. Available: http://doi.acm.org/10.1145/2334184.2334197

[6] P. Dunphy, J. Vines, L. Coles-Kemp, R. Clarke, V. Vlachokyriakos, P. Wright, J. McCarthy, and P. Olivier, “Understanding the Experience-Centeredness of Privacy and Security Technologies,” in *Proceedings of the 2014 workshop on New Security Paradigms Workshop*, 2014, pp. 83–94.

[7] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, “Android permissions: User attention, comprehension, and behavior,” in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 3.

[8] L. Reinfelder, Z. Benenson, and F. Gassmann, *Trust, Privacy, and Security in Digital Business: 11th International Conference, TrustBus 2014, Munich, Germany, September 2-3, 2014. Proceedings*. Cham: Springer International Publishing, 2014, ch. Differences between Android and iPhone Users in Their Security and Privacy Awareness, pp. 156–167. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-09770-1_14

[9] L. Kraus, T. Fiebig, V. Miruchna, S. Möller, and A. Shabtai, “Analyzing end-users knowledge and feelings surrounding smartphone security and privacy,” *S&P. IEEE*, 2015.

[10] J. A. Bargas-Avila and K. Hornbæk, “Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2689–2698.

[11] R. M. Ryan and E. L. Deci, “Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being.” *American psychologist*, vol. 55, no. 1, p. 68, 2000.

[12] K. M. Sheldon, A. J. Elliot, Y. Kim, and T. Kasser, “What is satisfying about satisfying events? testing 10 candidate psychological needs.” *Journal of personality and social psychology*, vol. 80, no. 2, p. 325, 2001.

[13] M. Hassenzahl, S. Diefenbach, and A. Göritz, “Needs, affect, and interactive products–facets of user experience,” *Interacting with computers*, vol. 22, no. 5, pp. 353–362, 2010.

[14] M. Hassenzahl, “Experience design: Technology for all the right reasons,” *Synthesis Lectures on Human-Centered Informatics*, vol. 3, no. 1, pp. 1–95, 2010.

[15] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller, “On the need for different security methods on mobile phones,” in *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*. ACM, 2011, pp. 465–473.

[16] P. G. Kelley, L. F. Cranor, and N. Sadeh, “Privacy as part of the app decision-making process,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013, pp. 3393–3402.

[17] M. Harbach, M. Hettig, S. Weber, and M. Smith, “Using personal examples to improve risk communication for security & privacy decisions,” in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2647–2656.

[18] L. Kraus, I. Wechsung, and S. Moller, “Using statistical information to communicate android permission risks to users,” in *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on*. IEEE, 2014, pp. 48–55.

[19] K. Benton, L. J. Camp, and V. Garg, “Studying the effectiveness of android application permissions requests,” in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on*. IEEE, 2013, pp. 291–296.

[20] C. Toombs, “Simplified Permissions UI in The Play Store Could Allow Malicious Developers To Silently Add Permissions,” http://www.androidpolice.com/2014/06/10/simplified-permissions-ui-in-the-play-store-could-allow-malicious-developers-to-silently-add-permissions/, (accessed: 2016-02-06).

[21] Android Developers, “Requesting Permissions at Run Time,” http://developer.android.com/training/permissions/requesting.html, (accessed: 2016-05-04).

[22] Statista - Das Statistikportal, “Anteil der verschiedenen Android-Versionen an allen Geräten mit Android OS weltweit im Zeitraum 01. März 2016 bis 07. März 2016,” http://de.statista.com/statistik/daten/studie/180113/umfrage/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os/, (accessed: 2016-04-25).

[23] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, “Itsa hard lock life: A field study of smartphone (un) locking behavior and risk perception,” in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[24] Initiative D21 and Huawei Technologies, “Mobile Internetnutzung Gradmesser für die digitale Gesellschaft,” http://www.initiatived21.de/wp-content/uploads/2014/12/Mobile-Internetnutzung-2014_WEB.pdf, (accessed: 2016-04-25).

[25] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, “Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption,” *Proc. USEC*, 2015.

[26] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, and S. Dolev, “Google android: A state-of-the-art review of security mechanisms,” *arXiv preprint arXiv:0912.5101*, 2009.

[27] WhatsApp Blog, “end-to-end encryption,” http://blog.whatsapp.com/10000618/end-to-end-encryption, 2016, (accessed: 2016-04-25).

[28] Y. Rashidi and K. Vaniea, “Poster: A user study of whatsapp privacy settings among arab users,” in *IEEE Symposium on Security and Privacy*, 2015.

[29] R. Fedler, J. Schütte, and M. Kulicke, “On the effectiveness of malware protection on android,” *Fraunhofer AISEC, Berlin, Tech. Rep*, 2013.

[30] A. Möller, F. Michahelles, S. Diewald, L. Roalter, and M. Kranz, “Update behavior in app markets and security implications: A case study in google play,” in *Proc. of the 3rd Intl. Workshop on Research in the Large. Held in Conjunction with Mobile HCI*, 2012, pp. 3–6.

[31] E. L. Deci and R. M. Ryan, “The” what” and” why” of goal pursuits: Human needs and the self-determination of behavior,” *Psychological inquiry*, vol. 11, no. 4, pp. 227–268, 2000.

[32] S. Epstein, “Cognitive-experiential self-theory. handbook of personality: theory and research/ed. pervin l. a,” 1990.

[33] N. Fronemann and M. Peissner, “User experience concept exploration: user needs as a source for innovation,” in *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*. ACM, 2014, pp. 727–736.

[34] A. Sonnleitner, M. Pawlowski, T. Kässer, and M. Peissner, “Experimentally manipulating positive user experience based on the fulfilment of user needs,” in *Human-Computer Interaction–INTERACT 2013*. Springer, 2013, pp. 555–562.

[35] S. Reiss, “Multifaceted nature of intrinsic motivation: The theory of 16 basic desires.” *Review of General Psychology*, vol. 8, no. 3, p. 179, 2004.

[36] “Uneeq - user needs questionnaire,” http://www.hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence_UserNeedsQuestionnaire_EN.pdf, (accessed: 2016-04-25).

[37] J. R. Landis and G. G. Koch, “The measurement of observer agreement for categorical data,” *biometrics*, pp. 159–174, 1977.

[38] A. F. Westin, "Privacy and freedom, atheneum," *New York*, p. 7, 1967.

[39] Statista - Das Statistikportal, "Marktanteile der Betriebssysteme an der Smartphone-Nutzung in Deutschland von Dezember 2011 bis Februar 2015," http://de.statista.com/statistik/daten/studie/170408/umfrage/marktanteile-der-betriebssysteme-fuer-smartphones-in-deutschland/, (accessed: 2016-04-25).

[40] S. Garfinkel and H. R. Lipford, "Usable security: History, themes, and challenges," *Synthesis Lectures on Information Security, Privacy, and Trust*, vol. 5, no. 2, pp. 1–124, 2014.

[41] D. M. Pedersen, "Psychological functions of privacy," *Journal of Environmental Psychology*, vol. 17, no. 2, pp. 147–156, 1997.

[42] M. T. I. Aumi and S. Kratz, "Airauth: evaluating in-air hand gestures for authentication," in *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*. ACM, 2014, pp. 309–318.

[43] M. Karlesky, E. Melcer, and K. Isbister, "Open sesame: re-envisioning the design of a gesture-based access control system," in *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2013, pp. 1167–1172.

[44] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, p. 19, 2012.

[45] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: how negative experiences affect future security," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2671–2674.

[46] I. Ion, R. Reeder, and S. Consolvo, "... no one can hack my mind: Comparing expert and non-expert security practices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 327–346.

Appendix

A. *Interview script*

Smartphone usage

- Why did you decide to buy a smartphone?
- You are currently using a smartphone with [Android/ iOS/ windows] operating system (OS). Was this a conscious decision? What were the reasons [for this decision]?
- Have you used another operating system before?
- If so, which? What were the reasons for changing the OS?

Smartphone sharing (Adapted from Chin et al. [1])

- Is this your only smartphone?
- If not,
  - How many smartphones do you own?
  - Why do you own several smartphones?
  - Which of them do you use mainly?
- Are there any other people who use your personal smartphone on a regular basis?
  - If so, how many? Who else is using your personal smartphone?
- Is there someone else who sometimes uses your smartphone?
  - If so, under which circumstances?

Work related use

- Do you also use your smartphone for work?
- If so,
  - For which purpose [e.g. calling, e-mailing etc.]?
  - What are the main differences between private and occupational use of your smartphone?
  - Did your employer set any requirements for work related smartphone usage?

App usage

- Do you use apps?
- If not, why?
- Which are your favourite apps on your smartphone?
- Which apps do you consider the most useful on your smartphone?

Paid apps

- Do you use apps you have to pay for?
- If not, are there any reasons why not?
- If so,
  - How do you pay for the apps?
  - Do you use in-app purchases?
    - If so, is the in-app purchase function password protected?

App selection and download

- Which criteria do you use to decide for an app you want to download or install?
- Which platform (i.e. app market) do you use to download apps?

App avoidance

- Are there any apps which you intentionally don't install? If so, what kind of apps?

App uninstalling

- Have you ever cancelled the installation of an app? If so, why?
- Have you ever uninstalled an app? If so, why?

Smartphone set up

- When you used your smartphone for the first time
  - How did you take action?
  - Did you set up the device according to your preferences?
  - If so, what did you do?

Data connections

- Which type of data connections do you use (e.g. Bluetooth, NFC, WiFi)? What are you using them for?

- If WiFi was mentioned: Which access points do you use [which networks do you use, respectively]?
- Are there situations in which you switch off your data connections?
- If so,
    - Why?
    - Do you remember any causes that made you start doing so?

Updates

- Do you install app updates?
- If so,
    - Why?
    - Do you install updates automatically or manually?
    - Is there any reason why you install them automatically/ manually?
    - Do you remember any causes that made you start doing so?

Post-paid vs. pre-paid

- Do you pay for your smartphone usage on a monthly basis or do you use pre-paid?
- What are the reasons why you decided for [payment method]?
- If Post-paid:
    - Do you check your monthly phone bills?
    - If so,
        - Why?
        - Do you remember any causes that made you start doing so?
- If Prepaid:
    - Do you check your prepaid balance from time to time?
    - If so,
        - How often?
        - Do you remember any causes that made you start doing so?

Battery lifetime

- Do you check your battery status from time to time?
- If so, do you do anything to save battery lifetime?
    - If so,
        - Could you please describe what exactly you're doing?
        - Do you remember any causes that made you start doing so?

Protection from theft

- Do you do anything to protect your smartphone from theft?
- If so,
    - What are you doing?
    - Do you remember any causes that made you start doing so?
- Do you use locating or remote access apps?
- If so,
    - Why?
    - Do you remember any causes that made you start doing so?

Backups

- Do you make backups of your smartphone data?
- If so,
    - What are the reasons for making backups?
    - How often do you make backups?
    - Where do you store your backups?
    - Do you remember any causes that made you start doing so?

Internet und Surfing

- Do you surf the Internet on your smartphone?
- If not, why not?
- If so
    - Which browser do you use? Why?
    - Which search engine do you use on your smartphone? Why?
    - Have you ever changed your browser settings?
        - If so, what did you want to change?
        - Was the action successful?
    - Do you take any measures to reduce your data traces on the web while surfing with your smartphone?
        - If so, what do you do?

Financial Transactions

- Do you use apps which include handling money such as mobile payment, mobile TAN procedures, online banking or shopping apps?
- If not, why not?
- If so,
    - Which kind of apps do you use?
    - Do you have any concerns while using these apps? If so, what kind of concerns?
- Do you use online banking via the browser?
    - If so, how does such a typical banking session look like?

App access to sensitive data

- Many apps request access to sensitive data (such as calendar or address book) and functions (such as camera and location).
- Do you allow those apps to access this data and functions?

  - If not, why not?
    - How do you avoid it?
    - Do you remember any causes that made you start doing so?
  - If so,
    - Do you allow all apps to access everything or only certain apps?
    - Do allow always access or only in certain situations?
  - Do you consider any data or functionalities more sensitive than others?

Communication

- Do you use your phone to communicate with other people?
- If so,
  - How do you communicate? (e.g. calling, SMS, Chat, email, social networks)
  - Which messaging apps do you use? Why do you use exactly these?
- Do you do something to protect your communication?
- If so, what do you do?
- Whom do you protect your communication from?
- Can you remember any causes that made you start doing so?

Data stored on the device

- Do you protect the data which is stored on your device?
- If so,
  - How do you protect your data?
  - What do you protect your data from?
  - Do you remember any causes that made you start doing so?

SPAM

- Do you sometimes receive SPAM (i.e. unwanted adds or messages) on your smartphone?
- If so,
  - Could you give us some examples?
  - How often do you receive SPAM?
  - Do you do anything to reduce the amount of SPAM you receive?

“Backup” questions: *Those questions were only asked if the related topics were not already mentioned during the interview.*

- Do you do anything to protect yourself from apps that collect too much data?
- If so,
  - What do you do?
  - How do you define these kinds of apps?
- Do you use additional security software on your smartphone?
- If so,
  - Which kind of apps do you use?
  - Against what do you want to protect yourself?
- Do you use pre-installed security mechanisms such as screen lock with a password?
- If so,
  - What are the reasons therefor?
  - Do you remember any causes that made you start doing so?
- Do you perceive any threats related to smartphone usage?
- If so,
  - Which threats do you perceive?
  - Do you have an individual strategy to protect yourself against these threats?
  - If so, could you please describe your individual strategy?
- Do you perceive any security and privacy threats related to smartphone usage?
- If so,
  - Which threats do you perceive?
  - Do you have an individual strategy to protect yourself against these threats?
    - If so, could you please describe your individual strategy?
- Do you have any comments or questions regarding the topics which we discussed today in this interview?