Decoding Privacy – An Anthropological Study Of The Privacy Concept In Mobile Software Development

Tanja Kornberger

Abstract

Despite it's ubiquitous social importance, the concept of privacy is challenged in unprecedented ways by the emergence of mobile technologies. Previous research has shed some light onto user concerns regarding privacy in a mobile context, however, only little attention has been paid to the attitudes and practices of mobile developers. To close this gap, this study presents an empirical account for the role of privacy within mobile software development from the perspective of developers. The study is comprised of two samples of unstructured interviews with developers from the United States of America and Germany; it applies an anthropological method in an engineering context and uses ATLAS.ti to implement a grounded theory approach. ATLAS.ti is used to analyze developer's conceptualization of privacy as well as country specific aspects of user privacy. The code system generated with ATLAS.ti further represents developer's awareness of privacy relevant conflicts, their assessment of the different stakeholders involved in the user privacy debate and their knowledge of and experience with privacy measures. Based upon this code system a framework is derived that structures crucial factors for the understanding and implementation of privacy strategies in mobile software development.

Keywords

privacy, information, technology, mobile software development, qualitative research, interview, grounded theory

Privacy In The Context Of Mobile Technologies

In recent days, news headlines have been dominated by reports about privacy scandals ranging from insecure communication protocols by popular mobile applications such WhatsApp (Kanjilal, 2013) to Google Glass' potential to become a silent big brother (Miller, 2013; Simons & Chabris, 2013) and the exposed governmental surveillance program PRISM (Simonite, 2013; Sottek

& Kopstein, 2013) – information privacy is in the focus of widespread media attention. Privacy is without doubt a hot-button topic at the moment. Even though public debates concerning privacy are not new, the magnitude of potential privacy threats appears to be unheard of. Two millennia ago Plato defined privacy as the counterpart to the public sphere; the topic has been anchored in philosophical, sociological, political and anthropological discourse ever since (DeCew, Zalta, Nodelman, Allen, & Perry, 2009). Nowadays, privacy has been widely recognized as a human right and is included in the Universal Declaration of Human Rights of the United Nations (Assembly, 1948). While there can be no doubt about the centrality of privacy to many societies, the whole concept is being challenged by the advent of digital technology. As technologies evolve, many new conflicts arise. Digital technologies outpace any legal, political and societal discourses about privacy measures. Information becomes the new currency in the digital world and with that come many more question about where this trend is leading (Boyd & Crawford, 2011). Smartphones in particular have become our daily companions and are filled with all kinds of personal data, which can be accessed by the applications stored on the device and used in potentially malicious ways (La Polla, Martinelli, & Sgandurra, 2012). Meanwhile numbers of mobile devices and respective applications are growing, new concepts and devices keep on popping up (Dover, 2012; ICD, 2013; Whitfield, 2013). With 3G cellphone antennas installed at the Mount Everest's base camp, it is even possible to surf the Internet from the world's highest peak (Bilton, 2013). It seems that smartphones have penetrated every layer of human life.

With the profound popularity of smartphones, come unprecedented amounts of data about literally everything and various embedded sensors and cameras can track our every move and more (Ferber, Jansa, & Dilli, 2012). Research shows that users express concerns about the safety of their data and privacy in the context of mobile technology usage. In a recent study by the Pew Research Center more than half of the users uninstalled or avoided the usage of a mobile application due to a potential threat to their privacy (Boyles, Smith, & Madden, 2012). Chin, Felt, Sekar and Wagner (2012) found that users are more concerned about their privacy with regards to their smartphone than other devices such as their laptop. Further, they identify the distrust of applications among the top factors that smartphone users are worried about. Other research further confirms increasing concerns about information privacy in the context of mobile technology use (Ben-Asher et al., 2011; Muslukhov, Boshmaf, Kuo, Lester, & Beznosov, 2012; Roesner et al., 2012). Despite numerous attempts to capture the concerns of users, research has hardly paid any attention to the perspectives and opinions of those, who create and implement mobile applications – software developers. To close this gap the present research aims to shed light into this particular aspect of the technology-privacy debate by dissecting the privacy concept in mobile software development from the perspective of software developers.

Method

This qualitative empirical work aims towards capturing subjective perceptions and experiences of software developers with regards to privacy concepts and conflicts related to the development of mobile applications. In particular, this study wants to create insights into the development process and the role of privacy measures within this process. To this end an interview guide made up of open questions was created, which includes the following topical segments:

- Conceptualizations of privacy in a mobile software context
- Awareness regarding recent issues and trends
- Assessment of different stakeholders
- Analysis of privacy conflicts and strategies

Ultimately, this research aims to help understand privacy in all its aspects from the perspective of a software developer and use those insights to generate solutions for user privacy.

Sample

The empirical data is comprised of 2 samples of qualitative, unstructured interviews conducted in the United States of America and Germany. All interviewees were asked the same questions in their respective native language. The interviews had an average duration of 40 Minutes. In total, 21 mobile developers from the US and Germany were interviewed.

In order to be considered as a participant for the study interviewees had to be involved in the development of mobile applications for the US market or the German market respectively.

The first set of interviews was conducted with developers in the San Francisco Bay Area and consists of 1 female and 9 male participants. The second set of interviews was conducted in the Munich area with 2 female and 9 male participants. Application types that interviewees have worked on, range from health, over finance, education, event management, location-based services, social services and entertainment.

All interviewees were recruited on a voluntary basis and were not compensated monetarily for their participation. Access to the interviewees was established through personal contacts, participation calls via mailing lists and on-the-spot recruitment at specific events. Following the snowball sampling technique further participants were recruited through the networks of previously interviewed participants.

Nearly all interviews were conducted face to face with a few exceptions that were conducted via Skype. Prior to the interview, participants were informed about the topic and the procedure of the interview and asked for their consent to be recorded. They were assured that anonymity would be provided at all times. To enhance the transparency of the research process all participants received a copy of their interview transcript prior to analysis.

Analysis

All interviews were digitally recorded using the software RecForge and fully transcribed using the software f5. Nonverbal expressions, such as laughter or longer periods of silence, were included in the transcripts to ensure the accuracy of the transcript and allow for a comprehensive analysis. All names and personal references such as places, employment details or relations have been censored and replaced by placeholders in order to fully guarantee anonymity.

The data analysis process was informed by the grounded theory methodology according to Strauss and Corbin (2007). Grounded theory is an approach to data analysis within which a theory is derived inductively from empirical phenomena. It involves an iterative, circular process consisting of data gathering, data analysis and theory construction. The aim of this study however was not theory construction. Nevertheless the first steps of developing categories and their properties as described by Strauss and Corbing served to be very fruitful for the analysis of this study. All conclusions are directly linked to empirical evidence present in the transcripts. The analysis was carried out using the software ATLAS.ti as a tool.

As the interview guide already provided a rough segmentation of the data, those segments were used to structure the analysis. At first codes were created in ATLAS.ti according to the respective topical segments of the interview guide and each transcript was coded using this segmentation. The second step involved a more detailed analysis. The data was coded line-by-line, sub-codes were created and themes and contents were clustered more granularly. Besides the frequency with which a specific content was mentioned, one of the main criteria for the creation of a new code or a sub-code remained the intra-individual relevance of a statement as assessed by the researcher. Those codes were then clustered into code families, subsuming different aspects of the segments provided by the interview guide into one code family.

While the data was dissected transcript by transcript in the first two steps, in the third and final step the data was analyzed by means of the codes in each category rather than each transcript, which included reassigning data to other codes, subsuming semantically similar codes as well as further refining them.

The analysis yielded five categories grouped into five code families respectively and a total of 44 codes, which are listed in Table 1.

Concept	concept_control concept_culture concept_data concept_identity concept_on_off_diff concept_on_off_same concept_ownership concept_protect concept_safety concept_seclusion concept_security concept_sharing concept_technology concept_transparency concept_trust concept_wellbeing evolution_tech
Awareness	aw_anonimity aw_concerns_user aw_legal aw_legal_0 aw_legal_1 aw_media aw_p_issues aw_relevance
Responsibility	resp_knowledge_user resp_own_p resp_p_issue resp_practice_comm resp_role-user resp_stakeholder
Solution	solution_complex solution_general solution_problem
Future	future_edu future_general future_tech

Table 1: Categories and their codes

Results

The description of the five resulting categories is grounded in the statements of the interviewees. As such it represents their views and perceptions only and cannot and should not be generalized beyond that.

Trust Is Good, Control Is Better – Privacy As A Concentric Model Of Informational Control

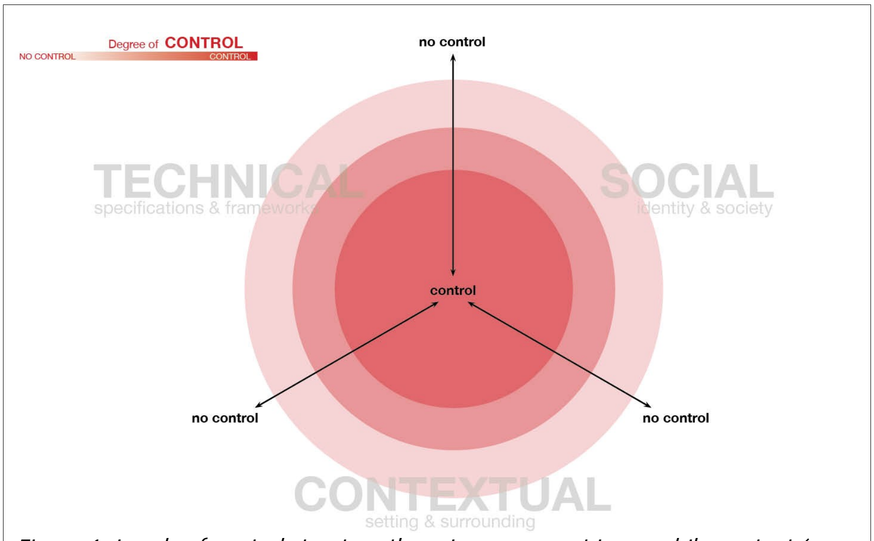

Figure 1: Levels of control structure the privacy concept in a mobile context (own illustration)

The first category encompasses the concept of privacy. Privacy was characterized as an elusive, relative term. It is not an action or a particular state of being *per se* that creates privacy, but the affective, intra-individual evaluation of a person about what is appropriate and what is not. There were four major themes that were repeatedly used to describe and characterize privacy. The most prominent theme emerging from the analysis was control over personal information. That is, to have control over one's own data means to have privacy. Control was described as the right to authorize access to information. This does not require the information *per se* to be deemed confidential, but stresses a person's ability to decide what happens to a piece of information. While some interviewees pointed out that privacy is relevant for information that is worthy of protection, this classification remains a subjective appraisal, as different individuals will strive to protect different kinds of information. Even when not directly asked about definitions and conceptualizations interviewees repeatedly pointed out the loss of control when describing privacy conflicts and concerns. This particular focus on control was attributed to the fact that in a mobile technology context it becomes increasingly challenging to obtain control as well as to gauge the consequences of granting access to personal information. The subjective feeling of control over information defines privacy in the context of mobile application usage; the perception of control, however, is structured by three additional themes: social, contextual and technological aspects. Those themes can be seen as three spheres of informational control. They all can contribute to a person's feeling of being in control in various ways. Figure 1 is a graphic representation of the category "privacy concepts".

The distinguishing character of this social sphere is that it encompasses aspects that are internalized by the individual. This can allude to specific norms and values including cultural norms and practices. For example, it was mentioned by many German developers that they perceive the German users to be less willing to share information about them and be rather conservative about their privacy compared to other nations. Others pointed out that the contents, which are deemed appropriate for public sharing, may vary according to cultural norms. The social sphere does also include aspects such as identity or reputation through which a person is known to the outside world. A breach of privacy in this context could be the possibility to tie a person's activity to their real identity without the consent of that person or to track, collect, store and / or share information about them and use it to compromise their social identity and reputation respectively. The third theme, contextual aspects, refers to all external factors such as settings and surrounding, which influence the perception of control. Interviewees referred to a range of factors such as the identity of other stakeholders or the type of information that influence whether someone perceives their privacy as being maintained or breached. At their workplace for example people might think differently about their informational privacy as opposed to their home. They might also share different information with their colleagues than with their partner, family or occasional acquaintances. The lines between the social and contextual spheres can get blurry, as they are not independent but can influence each other.

Finally, privacy also depends on technical aspects, i.e. the way the application deals with user information. It can allude to the level of stability of the architecture and the code of an application, but does also include the permissions that an application requires such as access to messages, phone calls, contact data and so forth. Privacy in the technical sphere means that an application is able to protect a user from malicious hacker attacks and does not obtain sensitive data without the consent of the user. Technical aspects can take away control from the user in any context and without their knowledge.

The framework highlights that software developers have an elaborate understanding of what privacy is, but it also makes evident how difficult it can be to grasp the concept of privacy and that no one single definition suffices to encompass its vast complexities and nuances.

A Penny For Your Thoughts – Awareness Of User Concerns And Legal Regulations

The second code category depicts developer's awareness of privacy relevant aspects including user concerns and legal regulations. The analysis shows that a substantial part of developers is not aware of the concrete concerns users might have. While a part of the participants believes that users are generally not very concerned about their privacy, some did state that they are very keen to learn more about user concerns and worries, but have not done so yet.

Most of the concerns named by interviewees were based on guesses and were not real concerns that have been communicated to them as part of their role as mobile developers. Developers depicted the origin of existing privacy issues as third party access, meaning that some type of stakeholder firstly gets access to the sensitive data of a person and secondly uses it in a way that is undesirable for that person. Two types of third parties were mentioned. The first refers to companies, such as advertising companies, gaining access to user data, which can then result in data leakage or data selling. One subject mentioned that the selling of data would pose less of problem, if that data is anonymized and used for the purpose of offering customized ads. However, data leakage is perceived as malicious and is associated with the misuse of credit card details or email account details. While data selling and leakage were mentioned as two separate things, it should be noted that they do not exclude each other

and can occur in succession such as data being leaked and then sold to yet another party. The damage involved in this kind of abuse can be characterized as mainly material. The second kind of third party access refers to other users, which pose a different kind of threat. Sensitive data is shared with other members of various social groups or the general public and results in embarrassment and a potential damage of reputation. One interviewee mentioned that some users might engage in punitive behavior, which might violate someone's privacy. This refers to the fact that other users can misuse functions of a mobile application, such as a rating or review function, to punish other users by giving them extremely bad ratings or by disclosing personal information via this function. The consequence of this can again be either public embarrassment and /or damage of reputation. The interviewees used two major keywords repeatedly when they talked about existing privacy issues, which are: anonymity and transparency. It was mentioned that aspects such as collecting and storing sensitive data is less of a problem, if that data is anonymous. In fact, one subject mentioned that there has to be a certain amount of data collection if the Internet is to remain a free space. That is, as long as anonymity is provided, users have to accept the analysis of their data in exchange for using a service at no charge.

Moreover, lack of transparency concerning the usage of data is a barrier to good privacy standards. Transparency in this context refers to the clear communication of the functionality and settings of an application as well as the announcement of changes within those . Most interviewees expressed that they had no specific knowledge about legal regulations with regards to privacy and the use of mobile applications. Though, those who are involved in several activist groups around privacy were very well familiar with regulations and trends concerning user data in online as well as in the offline contexts. In cases where an application was developed with a core functionality requiring sensitive user data, lawyers were consulted. The analysis also indicates that interviewees from the German sample were more able to name specific regulations. However, overall legal trends were perceived as a grey area with no clear standards or significant relevance.

One reason for this is that the technological development outpaces legal trends by far and hence there is no adaption possible to the ever-changing nature of digital technologies.

To Use Or Not To Use – Dissecting The Responsibility Of Stakeholders Within Mobile Application Usage

Active user participation was identified as the basis for healthy privacy standards. However, when it comes to questions of responsibility the subject of user privacy is entangled in a mix of different stakeholders influencing privacy measures.

On the one hand users need to show genuine interest in the protection of their informational privacy, act responsibly, recognize possible threats and be aware of the consequences of their behavior. They ought to avoid the usage of applications and systems that are known for ill practices and report such. Though this is portrayed as the ideal behavior, developers do not see current users display that behavior. It is assumed that many of users act negligent and ignorant.

The ultimate control over one's own data was described as the refusal to use an application altogether. It is important to note that the usage of an application might not only compromise the privacy of the person using it but also of those in contact with that person. It was also recognized that it becomes increasingly difficult for users to protect their privacy and that other stakeholders are responsible as well. It is for example the responsibility of companies to enable the user to protect their data. Companies should also educate and if possible train their users in matters related to privacy to ensure good user conduct on their own platform. Developers reported to be mostly unable to control the design of specific functions since they are either bound by customer requirements or instructions given by their product managers. They may play a consulting role within which they can raise awareness for privacy measures, but will ultimately follow their assignments as long as those are within legal bounds. It is noteworthy that while developers are implementing the functionality of applications they have only limited influence on the concept of the application unless they are developing for themselves.

Yet another stakeholder comes into play when considering the responsibility of the operating system provider, which usually offers the platform through which applications are purchased. App stores can support the implementation of privacy measures by communicating clearly what rights an application claims on the one hand and by giving guidelines to developers as to what is appropriate access to user data. Nevertheless, it was highlighted that technical systems are always subject to hacker attacks or technical failure and hence secure system are necessary to pave the way to stable user privacy.

It's A Fine Line – Privacy Strategies Need To Consider Both User And Technology

Most solutions proposed by the developers revolved either around user involvement or particular technical solutions. On the user side solutions can be clustered according the degree of user initiative they require, which can range from completely passive to fully active. On the technology side strategies vary according to their position within the smartphone architecture.

Altogether, more than 130 solutions were coded during the analysis. Figure 2 portrays the diversity of possible privacy solutions.. Each dot represents a concrete solution or a use case reported by the interviewees. The different layers of the smartphone architecture as depicted on the x-axis are adopted from Chow and Jones functional layers of a generic smartphone (2008). As the depth with which each solution varies greatly for every interviewee and every solution, the classification depicted in Figure 2 is to be understood as a rough scheme.

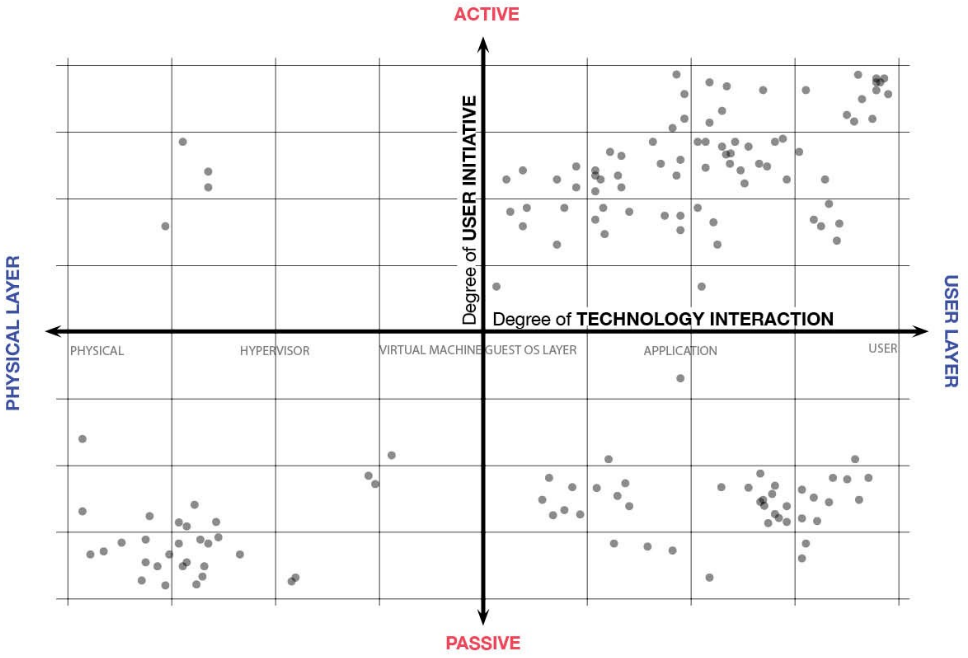

Figure 2: Proposed privacy measures by degree of user initiative and technology interaction

It is evident that most solutions require active user participation and are located in the application or the user layer. Most examples alluded to the conceptual design of the application and the construction of clear and concise language with regards to the permissions that an application claims. Solutions located on the user layer were concerned with proactive educational trainings with regards to privacy settings and the functioning of mobile applications in general. In contrast, solutions related to the physical layer mostly require very little user interaction and include examples such as encrypted storage or haptic feedback from the device.

It is noteworthy that although political and legal changes have been mentioned when discussing the possible future development of the privacy concept, they were not once directly proposed as solutions. In general, it emerged that designing privacy measures is very complex as solutions need to raise user awareness without being perceived as overly obtrusive.

When discussing potential privacy measures the introduction of standard solutions was evaluated negatively. Reasons for this are on the one hand the massive variety and diversity of systems and issues that make it impossible to create standard solutions. Interviewees doubted the practicability of the introduction of industry wide standards. On the other hand many expressed the concern that standards would hurt or hamper innovation.

Quo Vadis Privacy – Education, Business Models And Technology Development As Drivers For User Privacy

The final code category represents the assessment of the future of user privacy. Three major themes were identified, which include user behavior, technological developments and the evolution of new business models, all of which can influence user privacy in both positive and negative ways and are intertwined with each other. While there were discrepancies within the exact individual predictions, it was evident that the education of users with regards to the topic of data privacy will be of core importance. Growing interest, education and awareness could lead to careful handling of personal information. However, this trend could be counteracted by indifference and a narcissistic urge to display personal information publicly. Nonetheless, most interviewees reckoned that users would be more educated about potential threats and harms and act more responsibly. In this context it was highlighted that initially people also had many troubles with emails, which they were able to overcome once they learned how to properly use and manage them.

Moreover, it was mentioned that users would have more trust and confidence in companies and in web services in general. By the same token, users will tend to choose those companies and applications that they will feel most comfortable with. Therefore, it will be more profitable for companies to be transparent and cater to user needs. This already touches upon the second theme, which encompasses business models. Current application business models were perceived as detrimental to user privacy. Since most applications are free of charge, application providers are forced to generate revenue by other means, which often compromise user privacy. Popular platforms that follow those practices, such as Facebook or Instagram, can only be replaced by alternative services that offer the same features but rely on different revenue streams.

The third pillar, which is believed to shape the future of user privacy, is the technology underlying the applications. This does on the one hand refer to the security of the application architecture. On the other hand it entails the concern that technology will advance in such a way that will make it easier to get access to sensitive data without the user's knowledge. As long as obtaining user data remains profitable, people will always be willing to breach privacy standards. However, it was also assumed that a range of tools will be available that will actually facilitate information privacy. One way or another, the way in which technological aspects will advance will clearly influence the state of user privacy in the future.

Conclusion

The analysis showed that developers have a deep understanding of user privacy but lack knowledge concerning concrete user concerns. Likewise, they are not particularly familiar with legal aspects, which they perceive to be unclear and irritating.

With regards to the responsibility for privacy measure, developers portray a complex environment with numerous stakeholders. They expect responsibility and active protection of data on the user side and do not tolerate negligence. At the same time they understand the user's limited accountability for the abuse of private data, as interfaces and systems often come equipped with shortcomings and can be embedded in business models built on the premise to sell user data. Developers were able to provide a vast array of possible strategies to protect user data, which can be categorized according their degree of user initiative and their position within the smartphone architecture. Nonetheless, not many solutions outside of those categorizations were proposed, leaving political and legal approaches unmentioned.

Finally developers predicted that the future of information privacy in the mobile context would depend on user education, technological advances and the emergence of new business models.

Practical Implications

Their deep and detailed understanding of user privacy and the associated implications, qualifies software developers to function as experts in the discussion around privacy measures.

As developers expressed their wish to learn more about user concerns, this highlights the need for an easy and effective communication between developers and their users, so that developers can learn about privacy conflicts and users are able to directly convey their concerns to developers.

It was pointed out that guidelines for the implementation of privacy measures should be made available to developers in the same way that style guidelines are provided. Again, more communication between relevant stakeholders working on the topic of user privacy should be encouraged.

Further, policy makers need to be aware that the introduction of any strict standards might be hard to realize and will not be met with acceptance by developers. Standards are perceived as barriers to innovation and development, so developers might not incorporate restrictive measures voluntarily.

Lastly, it is assumed that the future of user privacy will not only depend on technological advances, but also on new business models and user education. Hence, it is essential to promote alternative business models that are not based on compromising user privacy by selling their data. Beyond that, users need to be exposed to educational campaigns and be offered opportunities to learn how to protect their privacy.

Limitations

Despite practical implications, a few limitations have to be considered with regard to the interpretation of the research results. All participants were recruited on a voluntary basis and hence the sample might be slightly biased towards people that already express interest in the subject of

privacy. Some of the interviewees were even active in various groups revolving around cyber law and the protection of user rights. Future research objectives might want to consider recruiting developers that have little prior knowledge of the subject and might therefore offer a different perspective.

Ultimately, the aspect of social desirability has to be mentioned. It is a possibility that some interviewees expressed high interest and concern because they regarded it as a socially expected and accepted attitude. On the other hand, all subjects were aware of their anonymity and did hence not face the threat of being exposed publicly for any statement made as part of this research.

References

Assembly, UN General. (1948). Universal declaration of human rights. *Resolution adopted by the General Assembly*, 10(12).

Ben-Asher, Noam, Kirschnick, Niklas, Sieger, Hanul, Meyer, Joachim, Ben-Oved, Asaf, & Möller, Sebastian. (2011). *On the need for different security methods on mobile phones.* Paper presented at the Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services.

Bilton, Nick. (2013). Bits Pics: Video Calls From the Top of the World, from http://bits.blogs.nytimes.com

Boyd, D., & Crawford, K. (2011). Six provocations for big data.

Boyles, Jan Lauren, Smith, Aaron, & Madden, Mary. (2012). Privacy and Data Management on Mobile Devices. Washington, D.C.: Pew Research Center.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. Paper presented at the Proceedings of the Eighth Symposium on Usable Privacy and Security.

Chow, G. W., & Jones, A. (2008). Framework for Anomaly Detection in OKL4-Linux Based Smartphones. Paper presented at the Australian Information Security Management Conference.

DeCew, J., Zalta, E., Nodelman, U., Allen, C. and Perry, J. (2009), Privacy, Menlo Park, Stanford University, Center for the Study of Language and Information.

Dover, Sarah. (2012). Study: Number of smartphone users tops 1 billion Retrieved 06.08.2013, from http://www.cbsnews.com/

Ferber, Thomas, Jansa, Paul, & Dilli, Johannes. (2012). Security & Privacy-Wie machen das Apple, Google und Co.?: eine Sicherheitsbetrachtung mobiler Endgeräte. University of Stuttgart, Stuttgart.

ICD. (2013). Strong Demand for Smartphones and Heated Vendor Competition Characterize the Worldwide Mobile Phone Market at the End of 2012, IDC Says Retrieved 06.08.2013, 2013, from http://www.idc.com

Kanjilal, Chinmoy. (2013). WhatsApp Uses a Potentially Insecure Authentication Mechanism. Retrieved 03.08.2013, 2013, from http://techie-buzz.com

La Polla, Mariantonietta, Martinelli, Fabio, & Sgandurra, Daniele. (2012). A survey on security for mobile devices.

Miller, Claire Cain. (2013). Privacy Officials Worldwide Press Google About Glass Retrieved 03.08.2013, from http://bits.blogs.nytimes.com

Muslukhov, Ildar, Boshmaf, Yazan, Kuo, Cynthia, Lester, Jonathan, & Beznosov, Konstantin. (2012). *Understanding Users' Requirements for Data Protection in Smartphones.* Paper presented at the Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on.

Roesner, Franziska, Kohno, Tadayoshi, Moshchuk, Alexander, Parno, Bryan, Wang, Helen J, & Cowan, Crispin. (2012). *User-driven access control: Rethinking permission granting in modern operating systems.* Paper presented at the Security and Privacy (SP), 2012 IEEE Symposium on.

Simonite, Tom. (2013). Companies Complying with NSA's PRISM May Face E.U. Lawsuits. Retrieved 03.08.2013, from http://www.technologyreview.com/

Simons, Daniel J, & Chabris, Christopher F. (2013). Is Google Glass Dangerous? Retrieved 03.08.2013, 2013, from http://www.nytimes.com

Sottek, T.C., & Kopstein, Josh. (2013). Everything you need to know about PRISM. Retrieved 03.08.2013, from http://www.theverge.com/

Strauss, A., & Corbin, J. (2007). Basics of qualitative research: Techniques and procedures for developing grounded theory: Sage Publications, Incorporated.

Whitfield, Karl. (2013). Fast growth of apps user base in booming Asia Pacific market. Retrieved 06.08.2013, 2013, from http://www.portioresearch.com

Tanja Kornberger

University of Munich, University of California, Berkeley. Correspondence concerning this article should be addressed to Tanja Kornberger, Untere Grasstraße19, 81541 Munich. Email: Kornberger@ischool.berkeley.edu

Article Information

This article is published at the Digital Repository of Technische Universität Berlin, URN urn:nbn:de:kobv:83-opus4-44174, http://nbn-resolving.de/urn:nbn:de:kobv:83-opus4-44174. It is part of ATLAS.ti User Conference 2013 : Fostering Dialog on Qualitative Methods, edited by Susanne Friese and Thomas Ringmayr. Berlin: Universitätsverlag der TU Berlin, 2014, ISBN 978-3-7983-2692-7 (composite publication), URN urn:nbn:de:kobv:83-opus4-51577, http://nbn-resolving.de/urn:nbn:de:kobv:83-opus4-51577