Privacy exposed

Wottrich, V.M.


6

GENERAL CONCLUSION AND DISCUSSION

With the technological advancements during the past years, more and more devices that are monitoring our online behavior have entered our lives. Of those devices, mobile devices such as smartphones and tablet PCs probably know most about us. Almost always on and with us, mobile devices can facilitate the data collection and data sharing to a degree unprecedented in the desktop environment (Federal Trade Commission, 2013). Most of the data collection and sharing takes places in the context of mobile apps. Before being able to download an app, users usually have to grant app permissions, that is, an app's request to collect and process personal data about its user. While the data collection and usage practices of mobile apps bring about benefits for both consumers (e.g., instant and often free access to information) and businesses alike (e.g., increased marketing efficiency), they also raise concerns about privacy. So far, literature on how consumers respond to the data collection and usage practices of mobile apps is scarce and mixed. To get more insights into this matter, this dissertation investigated (1) the status quo of privacy protection behavior, (2) the drivers of information disclosure, and (3) the consequences of information disclosure in the privacy-sensitive context of mobile apps. In sum, this dissertation provides five main conclusions about consumers' responses toward the data collection and usage practices of mobile apps.

1. **Mobile app users are currently not empowered and motivated enough to tackle the data collection and usage practices of mobile apps.**

First, this dissertation showed that mobile app users are not armed and motivated enough to protect their privacy in mobile apps. As chapter 2 illustrated, app users' current knowledge about the data collection and usage practices of mobile apps is very limited. In addition, app users are only moderately concerned about their privacy and they do not feel very vulnerable to potential privacy invasions caused by mobile apps. Furthermore, app users only have moderate confidence in their own ability to control the disclosure and subsequent use of personal information in the mobile app context. Also, while their motivation to protect their privacy in the mobile app context is moderate, app users only report low levels of actual privacy protection behavior (e.g., reading the privacy policy of apps). These findings extend previous research on consumers' understanding of data-driven marketing (e.g., Park, 2011; Smit et al., 2014).

2. **Mobile app users are more likely to engage in privacy protection, when they feel vulnerable, concerned, and think that they are able to protect themselves from the data collection and usage practices of apps.**

Second, chapter 2 of this dissertation showed that mobile app users are more inclined to protect their privacy when they think that privacy invasions caused by mobile apps can, in fact, also affect them. Moreover, they are more likely to protect themselves if they are concerned about their privacy and have confidence in their own ability to control the disclosure and subsequent use of their personal information. Self-efficacy plays the most important role in this regard, because it had the strongest relationship with protection behavior. This is in line with earlier findings showing that self-efficacy has the most consistent impact on the enactment of safe behaviors and that it is the strongest predictor of online safe behaviors (Boehmer et al., 2015; D. Lee et al., 2008). Surprisingly, higher levels of knowledge about the data collection and usage practices of apps were not associated with more, but with less protection motivation and behavior. This might indicate that users with higher knowledge simply have given up protecting their privacy, because they know that it is difficult to tackle the threat. Alternatively, this finding could imply that users with more knowledge feel sufficiently armed against or invulnerable to the data collection practices, which results in a lower protection motivation.

3. **Mobile app users engage in a privacy trade-off when downloading mobile apps in which app value trumps app intrusiveness and privacy concerns.**

Third, this dissertation demonstrated that mobile app users engage in a privacy trade-off when downloading mobile apps (chapter 3). In this trade-off, the value of an app increases app users' intention to accept app permission requests, providing, to our knowledge, the first empirical evidence for earlier assumptions made in the mobile app context (Eling et al., 2013; Keith et al., 2013). Moreover, in line with earlier research on general Internet users (e.g., Cecere & Rochelandet, 2013; van Doorn & Hoekstra, 2013; Wirtz et al., 2007), perceived app intrusiveness has a negative effect on mobile app users' intention to accept permission requests and privacy concerns were negatively related to permission acceptance intention. When considering the joint effect of app value, intrusiveness, and privacy concerns, this dissertation showed that the benefits (i.e., app value) trump the costs (i.e., intrusiveness, privacy concerns) in the privacy trade-off. This means that mobile app users tend to trade their privacy for apps that are of value to them.

4. **In branded gaming apps (i.e., advergames), customization features and brand trust may increase information disclosure and brand attitude, but this influence is strongly conditioned by consumers' privacy concerns.**

Fourth, this dissertation offered a better understanding of how games motivate consumers to share personal information as well as to adapt their brand attitude and which role consumer privacy concerns play in this regard. As indicated in chapter 4, consumers' privacy concerns may provide a boundary condition to the effects of customization features and brand trust in advergames. In line with prior research (Przybylski et al., 2010; Ryan et al., 2006), players have a more positive brand attitude when the game contains customization features, but only if their privacy concerns are low. When privacy concerns are high, a game containing customization features leads to a more negative brand attitude. Moreover, different levels of privacy concerns do not affect players' responses (i.e., information disclosure, brand attitude) toward high trust brands, suggesting that trusted brands could withstand privacy issues in advergames. For low trust brands, however, effects on information disclosure and brand attitude are conditioned by consumers' privacy concerns: more-concerned players share less information and have a more negative brand attitude than less-concerned players.

5. **Branded app intrusiveness has a damaging effect on app and brand perceptions for fictitious apps, but not for real apps.**

Last, this dissertation showed that collecting data about consumers via branded mobile apps could have negative consequences for marketers. As illustrated in chapter 5, the more information a fictitious, unknown branded app collects, the more negatively consumers respond to this app in terms of app attitude and app trust. This is in line with earlier research on mobile marketing showing that the intrusive nature of mobile apps negatively affects consumers' attitudes toward mobile advertising (Tsang et al., 2004). The negative effect of intrusiveness on app perceptions is conditioned by consumers' privacy concerns: more-concerned users respond more negatively than less-concerned users. However, chapter 5 also showed that app intrusiveness does not seem to have an effect on consumers' app and brand perceptions when the app is originating from a real brand to which consumers have a neutral stance in terms of brand attitude. This could mean that consumers have become so used to the data collection and usage practices of established brands that they do not act upon their intrusiveness perceptions anymore. Also, these findings could mean that consumers do not connect the feeling of intrusiveness to a specific brand or app, but that it is rather a general feeling of distrust not affecting app and brand perceptions.

Theoretical Implications

Nissenbaum's (2009) contextual integrity framework was used as a conceptual backbone for this dissertation. Her framework assumes that we are living in various contexts and each of these contexts is governed by context-relative informational norms. Whether a context-specific information flow is appropriate depends on the type of information, the actors involved in the transmission (e.g., sender, receiver), and the conditions under which the information transmission takes place (Nissenbaum, 2015). When informational norms are violated the information flow is inappropriate and our sense of privacy is disturbed. Thus, context-specific informational norms structure people's privacy expectations and their responses toward information requests (Nissenbaum, 2009). This dissertation investigated consumers' responses to the data collection and usage practices by focusing on three different app contexts, that is general mobile apps (chapters 2 & 3), gaming apps (chapter 4), and branded mobile apps (chapter 5). Although it did not explicitly test all constructs of the contextual integrity framework, this dissertation provides first empirical evidence for Nissenbaum's theoretical framework, so far. Hence, the framework is a valuable starting point for assessing consumer responses to data collection and usage practices of apps.

In addition, chapter 2 provides a theoretical refinement of Protection Motivation Theory (PMT) (Rogers, 1975; 1983) by showing the need for including the concept of *knowledge* as an additional construct pertaining to the theory. In doing so, chapter 2 extends PMT and makes it more applicable to the mobile app context. Moreover, it provides a more nuanced understanding of the factors that motivate app users to protect their privacy.

Chapter 3 contributes to theory on the privacy calculus (Acquisti et al., 2013; Culnan & Armstrong, 1999; Dinev & Hart, 2006) in two important ways. First, it confirms the generalizability of the privacy calculus theory in the mobile app context. Second, it extends literature on the privacy trade-off by manipulating the costs and benefits of it without forcing participants to trade the costs against the benefits. To our knowledge, our study is the first to draw causal inferences on the interplay of costs and benefits in privacy decision-making in the mobile app context, which is an important test of the theory.

The most important theoretical contribution of chapter 4 is that it shows that advergame players' perceived privacy concerns moderate the effects of advergame features (i.e., customization and brand trust). Against the backdrop that online games often collect consumer information (Thurm & Kane, 2010), these findings imply that theoretical and empirical models of advergame effects should not only take into account advergame characteristics, but also the moderating influence of privacy

concerns. Regarding the online context, motivational theories, such as Social Cognitive Theory, should acknowledge the important conditioning role privacy concerns might play.

By linking the data collection and usage practices of branded mobile apps with consumers' app and brand perceptions, chapter 5 extends research on Social Contract Theory (Donaldson & Dunfee, 1994; Dunfee et al., 1999) by showing that breaching a social contract does not necessarily lead to negative consumer responses. Apparently, for some contracts, contract breaches have become acceptable or consumers have simply accepted that they cannot do much about the constant breaches.

Practical Implications

The collection of personal data is no new phenomenon. Information about us has always been collected, be it by video cameras in public places or by record systems of governmental institutions. What is new is the scope of the data collection and the sensitivity of the often unwittingly collected information. With the proliferation of mobile devices, the smallest details of our lives are monitored more closely than ever before. According to Bauman and Lyon (2013), surveillance has become liquefied: "once seemingly solid and fixed, [it] has become much more flexible and mobile, seeping and spreading into many life areas where once it had only marginal sway" (p. 3). Currently, it seems unlikely that this trend will stop or slow down soon. Instead, digital devices (e.g., Internet of Things, wearables, robots) will increasingly enter our lives, bringing about new opportunities, but also challenges for privacy. The question is how do we as consumers respond to these privacy challenges? This dissertation tried to shed light on this question focusing on the context of apps. The insights gained from the four empirical studies of this dissertation provide three important take-aways for policy makers, consumers, and marketers.

First, **the current self-regulation principle in general, and the informed consent regulations more specifically, seem to be ineffective in protecting consumer privacy.** An important and perseverative question in the consumer privacy context is whether consumer privacy can be protected through industry self-regulation, meaning that firms and consumers are responsible for taking the necessary means to protect privacy, or whether policy makers need to intervene. In the European Union (EU), policy makers do intervene by generally regulating how businesses collect and protect consumer information. However, the data protection authorities also partly place the responsibility for privacy protection on consumers. This also reflected in the recently introduced reform of data protection rules (EU General Data Protection Regulation, 2016), which entered into force in May 2016 and which shall apply from May 2018. This

dissertation shows that mobile app users already seem to be overwhelmed by the current privacy regulations (e.g., informed consent) and it, therefore, raises doubt as to whether consumers should be given even more responsibility for the protection of their privacy. Mobile app users' knowledge on the data collection and usage practices is limited and privacy concerns and protection motivation are rather low. This suggests that the current informed consent regulations do not seem to reach their aims, which makes it very difficult for users to respond the data collection and usage practices of apps in an informed manner.

In addition, this dissertation shows that although consumers do engage in a privacy trade-off, they still seem to be insufficiently equipped to make well-considered privacy decisions when downloading apps. This is because the value of an app seems to overrule the influence of app intrusiveness and privacy concerns in the decision-making process. Raising awareness of the intrusiveness of apps, for instance, via the app permissions screen, and evoking privacy concerns might decrease app users' permission acceptance intention, but this strategy might not work for highly valued apps. Considering that app users probably mainly download apps that are of value to them, informing people about the costs of the information trade might not be the best way to protect consumer privacy. Thus, the current informed consent measures seem to be deficient to empower mobile app users to make well-informed privacy decisions.

Therefore, this dissertation encourages policy makers to better empower consumers and to reassess whether app permission pages in their current form are the right means for educating consumers about the data collection and usage practices of apps. In addition, this dissertation suggests potential ways to empower consumers. Policy makers could, for instance, concentrate their empowerment efforts on increasing (1) mobile app users' awareness of potential privacy threats and (2) their belief that they can, in fact, protect their mobile privacy. In that sense, it would do well if awareness creation would go beyond just informing consumers about the data collection practices of apps, for instance, by using privacy policies. Policy makers could, for example, create awareness for the *concrete negative consequences* of the data collection and usage practices of apps (e.g., discrimination in buying situations, identity theft, fraud) and increase protection motivation by stimulating a public debate about the topic using mainstream media. Apart from recommending improving current consumer empowerment efforts, this dissertation also cautions policy makers to place too much responsibility for the protection of privacy on consumers. If it is the aim to protect consumer privacy, then policy makers could better take the burden off consumers' shoulders and implement new laws restricting mobile apps in their data collection and processing activities.

Second, **mobile app users can do better to protect their privacy in apps.** Although mobile app users might feel helpless or overwhelmed when it comes to protecting their privacy, there are still some steps they can take. First and foremost, they can actively inform themselves about the data collection and usage practices of mobile apps and their consequences on educational websites. As part of the EU's *Safer Internet Program* and the *CEF Telecom Program*, 31 countries in the EU currently have a so-called *Safer Internet Center* (European Commission, 2012). These centers, among others, promote media literacy and safe Internet behavior. The Dutch Safer Internet Center www.veiliginternetten.nl (translated: safely surfing on the Internet), for instance, informs users about the different types of information mobile apps usually want to access, briefly addresses the pro's and con's of each information access, and stimulates users to read privacy policies and to assess whether they find the information access acceptable or not. Also, users could download apps that visualize what kind of information other installed apps collect and to what extent they threaten user privacy. One example for these kinds of apps is "My Permissions Privacy Cleaner" (MyPermissions, 2017). By downloading apps like this, users can become more aware of the data they are sharing and use this knowledge to make better-informed privacy decisions. In the MyPermissions app, users can, for instance, directly remove apps that collect too much information or mark apps they trust. Furthermore, users could consider using alternative apps offering the same service while accessing less personal information. For example, the messaging service "Threema", offers a similar service as the popular messaging app "WhatsApp", while actively preventing the collection of meta data, thereby guaranteeing privacy (Threema, 2018). Finally, depending on which device they possess, app users can partly control which permissions apps can access after installing them. Mobile devices running Android 6.0 and up as well as iPhones allow users to manually enable or disable certain permissions via the device's settings once they started using the app (Apple, 2017; Google, 2018). Turning off permissions, however, may cause apps to lose functionality. Therefore, users have to turn on permissions again once they want to use a specific app.

Third, **marketers should be aware that collecting too much data and raising privacy concerns might have negative consequences**. This dissertation showed that the more information unknown branded apps collect, the more negatively consumers respond in terms of app attitude and app trust. Based on these findings, marketers willing to launch a new branded app may consider limiting the collection of consumer data. Given that developing branded apps is cost intensive, marketers might, thus, consider restricting their data collection behavior to avoid triggering undesirable responses toward the new app. The negative effects of app intrusiveness on app and brand

perceptions are conditioned by consumers' privacy concerns: more-concerned users responded even more negatively than less-concerned users. In a gaming environment, more-concerned players responded more negatively to customization features than less-concerned players. Marketers should be aware of the role privacy concerns play in consumers' responses to the data collection and usage practices of apps. Before employing apps that collect consumer information, marketers should investigate how sensitive their target group is when it comes to privacy. Based on this investigation, they should decide how much consumer information they can collect without running the risk to "scare off" consumers.

Limitations and Future Research

As with most research, it is important to consider some limitations when interpreting the findings of this dissertation. First of all, the experimental nature of the research presented here might have had consequences for the ecological validity of our findings. In chapters 3 and 5, our participants were asked to carefully inspect an app permissions page, which might not happen often in practice, because many mobile app users do not seem to read app permissions when installing apps (Liu, 2014; Shklovski et al., 2014). Consequently, the privacy trade-off might look somewhat different in real life. For the same reason, it is possible that consumers generally experience lower levels of intrusiveness and that they respond differently in terms of app and brand perceptions. To verify that our findings also hold in practice, future research could test the privacy trade-off and the effects of banded app intrusiveness in another context where consumers are less habituated to simply click on "accept". Also, asking people to play an advergame in a laboratory setting in exchange for extra course credit or money, as done in chapter 4, also might have had consequences for participants' motivation to play and therefore for some of our findings. Future research might focus more on a naturalistic setting to validate our results.

Second, the apps employed in all of our studies were all free, meaning that our findings are only applicable to apps that are at no charge. The reason for only including free apps is that these often request more information than paid apps, as they are subsidized by sales of user data to advertising networks (Egelman et al., 2013). Users might view paid apps differently in terms of privacy issues compared to free apps. As they often collect and share less information, users might perceive paid apps as less privacy invading, which could, for instance, positively influence app usage and encourage them to share more personal information with the app. A fruitful next line of research may focus on consumer responses to paid mobile apps. Questions worth investigating would be, for instance: To what extent are consumers aware of the fact

that free apps collect more information than paid apps? How do paid apps affect consumers' privacy protection behavior? Which (different) effects do paid apps have on consumers' responses to apps? To what extent are consumers' responses to paid apps the same as to free apps, because they are unaware of the differences in data collection and usage?

Third, this dissertation mainly focused on apps that can be installed on smartphones and tablet PCs. However, there are also other devices, such as smart watches, fitness trackers, the Internet of Things, or intelligent personal assistants (e.g., Amazon Echo), which collect even more sensitive data (e.g., sleep intervals, heart rate, presence at home, voice recordings). The variety of devices is growing and it is not clear yet how consumers respond to the data collection and sharing practices of these devices. Consumers might, for instance, experience privacy concerns due to the sensitivity of the collected data and, therefore, refrain from adopting the new technology. Future research should focus on consumer responses toward the data collection and usage practices of apps that are connected to wearables and devices connected to the Internet of Things.

Finally, it should be noted here that chapter 4 tested a browser game and not a mobile gaming app. Compared to the other studies of this dissertation, in chapter 4 the data collection was more visible and information disclosure required more action from participants, because they were asked to actively provide personal information. Also, the type of information that was collected in chapter 4 differed slightly from that collected in the other studies. Due to these differences, the insights gained from chapter 4 are not completely transferrable to the mobile gaming context. Future research might want to investigate how consumers respond to the "more hidden and passive" data collection and usage practices of mobile gaming apps. It could be that advergame effectiveness is less impaired by privacy concerns in mobile gaming apps, as the data collection is less obvious than in the game tested in chapter 4.

Conclusion

Mobile apps are increasingly jeopardizing consumer privacy by collecting, storing, and sharing personal information. However, little is known about users' responses to data collection and usage practices of apps. This dissertation investigated (1) the status quo of privacy protection behavior, (2) the drivers of information disclosure, and (3) the consequences of information disclosure in the privacy-sensitive context of mobile apps. Results show that app users are currently not empowered and motivated to protect their privacy in apps, because they only have limited knowledge on the data collection and usage practices of apps, and they are only moderately concerned

about their privacy. Potential ways of empowering and motivating app users to protect their privacy include making them feel vulnerable and concerned, and showing them that they are able to protect themselves from the data collection and usage practices of apps. With respect to the drivers of information disclosure in the mobile app context, this dissertation showed that app users engage in a privacy trade-off when downloading mobile apps. In this trade-off, the benefits (i.e., app value) trump the costs (i.e., intrusiveness, privacy concerns), meaning that mobile app users tend to trade their privacy for apps that are of value to them. Furthermore, in an online gaming context, customization features and brand trust increase information disclosure and brand attitude, but this influence is strongly conditioned by how concerned players are about their privacy. Finally, this dissertation shows that the data collection and usage practices of apps might have negative consequences for marketers, because the more information apps collect, the more negative users are. This holds for fictitious branded apps, but not for real branded apps. All in all, this dissertation provides important insights into consumers' responses to data collection and usage practices of mobile apps, which shape future inquiries in the area of information privacy and consumer protection in the mobile app context.