Privacy Exposed: Consumer Responses to Data Collection and Usage Practices of Mobile Apps

V.M. Wottrich

English Summary

Today, mobile devices, such as smartphones and tablet PCs, play an important role in our lives. Almost always on and with us, they offer unprecedented, instant, and often free access to information, entertainment, and social interaction at any time and from any place. However, these benefits do not come without risks. By downloading and using mobile applications ("apps"), smartphone and tablet users constantly —and often unwittingly— create quantifiable information online. This information is often collected, stored, used, and auctioned off by third parties, such as app developers, data brokers, analytics companies, and marketers. These data collection and usage practices might impose a threat to app users' privacy, because the gathered information is often used for discriminating between users in buying situations, social sorting, (hidden) manipulation, or fraudulent behaviors, such as identity theft. Currently, app users' influence on the gathering of personal information via mobile apps is limited. As they often cannot selectively grant or decline certain permission requests or simply "opt out" of the tracking, the guiding principle is often "all-or-nothing": accept the information request or do not install the app.

So far, literature on how consumers respond to this situation is scarce and mixed. While some studies show that app users engage in privacy protecting behavior (e.g., uninstalling apps) due to privacy concerns, others demonstrate that users willingly trade their privacy for convenience, functionality, or financial gains. To get more insights into how consumers respond to data collection and usage practices of mobile 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.

Conclusions

This dissertation reports the results of four empirical studies, which are based on seven different datasets gathered among more than 4,000 participants. Together, these studies provide five main conclusions about consumers' responses toward 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.**

App users' current knowledge about the data collection and usage practices of mobile apps is very limited. Moreover, app users are only moderately concerned about their privacy, they do not feel very vulnerable to potential privacy invasions caused by mobile apps, and they only have moderate confidence in their own ability to control the disclosure and subsequent use of personal information in the mobile app context. Currently, app users' are moderately motivated to protect their privacy, however, they barely engage in actual privacy protection behavior in the mobile app context.

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.**

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. 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, which is raising doubts concerning the assumption of informed privacy decision-making in the context of mobile apps.

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

Mobile app users tend to trade their privacy for apps that are of value to them. The benefits of an app (i.e., app value) seem to trump the costs (i.e., intrusiveness, privacy concerns) in the privacy trade-off.

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.**

Privacy concerns may provide a boundary condition to the effects of customization features and brand trust in branded gaming apps. Privacy concerned players respond more negatively to gaming features 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.**

Collecting data about consumers via branded mobile apps could have negative consequences for marketers. 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. However, intrusiveness does not seem to have an effect on consumers' app and brand perceptions when the app is originating from a real brand.

Conclusion and Practical Implications

This dissertation provides new insights into how consumers respond to data collection and usage practices of apps. It does not only contribute to the scientific literature on privacy decision-making in various ways, but it also provides three important take-aways for policy makers, consumers, and marketers. First of all, this dissertation raises doubts as to whether the current self-regulation principle in general, and the informed consent regulations more specifically, are effective in protecting consumer privacy. Instead of placing too much responsibility for the protection of their privacy on consumers, 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. Second, this dissertation shows that mobile app users can do better to protect their privacy in apps. Although it might seem difficult, there are still some steps consumers can take to protect their privacy and this dissertation encourages them to make use of the means that are already available. Mobile app users can, for example, actively look for more information about data collection and usage practices of apps on educational websites, such as www.veiliginternetten.nl or they could consider downloading alternative apps offering the same service as privacy-invading apps. Third, marketers should be aware that collecting too much data and raising privacy concerns might have negative consequences for their brand. 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. All in all, this dissertation provides a more nuanced understanding of consumers’ responses to data collection and usage practices of mobile apps, which will hopefully shape future inquiries in the area of information privacy and consumer protection.