Privacy Management in Mobile Apps - The Way to Put Concerns Aside

Denis Weinecker
Justus-Liebig-University Gießen
Monika Schuhmacher
Justus-Liebig-University Gießen

Privacy Management in Mobile Apps – The Way to Put Concerns Aside

Abstract

Privacy concerns are a powerful factor in the decision to use a mobile app. Hence, companies have to find effective measures to manage consumers´ privacy in apps. However, surrounding company- or app-related factors like app type, information type or branding can make the difference within privacy evaluations. Based on communication privacy management theory, we develop three experiments to explore how different privacy levels as well as different app-specific designs effectively reduce the formation of privacy concerns with mobile apps. First insights reveal that the level of information privacy influences the formation of consumers´ privacy concerns. The findings demonstrate that enhanced information ownership and control attenuate consumers´ potential concerns. Additionally, we show that the effect is more important when introducing a new app compared to an improved version of an existing app. The empirical insights highlight that companies need to consider the aspect of privacy for the successful adoption of apps.

Keywords: Privacy Concerns, Mobile Apps, Communication Privacy Management

Track: Product and Brand Management

1. Introduction

The topic of information privacy in mobile apps is gaining relevance through the public debate on data misuse as well as upcoming regulations for data protection (e.g. Shilton & Greene, 2019). While companies reason their extensive information collection to enable free applications and customized offerings, customers often evaluate these practices as an invasion of their information privacy (Gerlach, Eling, Wessels, & Buxmann, 2019). Therefore, the perception of privacy concerns in mobile apps and consequences for their development receive soaring interest among researchers (i.e. Feng & Xie, 2019; Pavlou, 2011).

So far, scholars mostly agree upon the negative effect of privacy concerns on behavioral outcomes in the mobile app environment such as low trust in app (Konya-Baumbach, Schuhmacher, Kuester, & Kuharev, 2019), reduced information disclosure (Wang, Duong, & Chen, 2016) or non-installation (Chin, Harris, & Brookshire, 2018). However, research on possibilities to reduce the perception of privacy concerns or risks provides inconclusive results. For example, several studies find no significant effects of privacy intrusive policies on information disclosure (Berendt, Günther, & Spiekermann, 2005) or privacy-related statements on risk perceptions (McKnight, Kacmar, & Choudhury, 2004). At the same time, other scholars demonstrate beneficial effects of privacy notices (Milne & Culnan, 2004) or privacy settings control (Feng & Xie, 2019) to mitigate consumers´ privacy concerns.

While extant studies focus on information privacy related policies, only little is known about how specific company- or app-related aspects as well as different data types can mitigate consumers´ privacy concerns in mobile apps. In this regard, the record of accomplishment or trust in a company might be of relevance. For example, start-ups compared to established companies or existing apps versus new apps cannot build upon aspects of trustworthiness or brand reputation (Chin et al., 2018; Kuester, Konya-Baumbach, & Schuhmacher, 2018). Addressing this research gap, we build upon communication privacy management (CPM) theory to investigate the effects of different privacy versions on consumers´ privacy concerns. Further, we specifically compare differences for an existing app and new app. Furthermore, we aim to reveal if different types of data, i.e. person data or online data influence privacy concerns´ and subsequent behavioral outcomes.

2. Theoretical Background: Communication Privacy Management Theory

CPM theory has its roots in explaining privacy-related communication between marital couples and thus, explaining the management of private information disclosure within interpersonal relationships (Petronio, 1991). CPM theory reveals that individuals develop different communication boundaries based on rules that are constituted by cultural, gendered, situational, motivational or risk-benefit-ratio criteria (Xu, Gupta, Rosson, & Carroll, 2012). These individual boundaries ensure personal beliefs about private information ownership and control of potential private information flow. Thus, private information ownership and control are decisive operating principles for persons´ decision about sharing information with external parties and letting others become the co-owner of private information (Petronio, 2002). Once the owner shares private information, both parties have to negotiate mutually accepted privacy rules about third party sharing. If co-owners try to cross individual privacy boundaries without permission or fail in coordinating privacy rules with the owner, they violate the boundary coordination rules. Consequently, owners would experience a boundary turbulence. This boundary turbulence aims to restrict or cut back a person's ability to control ownership and flow of private information and thus, leads to the development of privacy concerns and related protection behaviors (Gu, Xu, Xu, Zhang, & Ling, 2017; Petronio, 2002).

Extending the context of interpersonal relationships, the management of private information is of particular interest in the case of mobile apps where the exchange of private information is often indispensable for their usage (Arora, ter Hofstede, & Mahajan, 2017). Within this person-computer interaction, mobile apps become co-owner of data by requesting various permissions and rights to collect, analyze and share private user information, which we refer to as the level of information privacy (LIP). Accordingly, LIP addresses the dimensions of CPM as the app needs to access owners´ private information and interferes the owners' control of information flow. If the LIP exceeds the owners´ accepted boundary coordination rules, i.e. by demanding the right to share private information with third parties, the app causes boundary turbulences. Then, these turbulences result in the formation of privacy concerns (Petronio, 2002). In line with boundary coordination, we investigate app-related characteristics, i.e. app type, requested information type or branding as potential means to handle boundary turbulences and thus, their effect on the formation of consumers´ privacy concerns.

3. Conceptual Framework and Hypotheses Development

For the conceptual framework of our present study, we draw on CPM theory (Petronio, 1991) to investigate the effect of different information privacy versions on consumers´ privacy concerns and how this effect is influenced by varying mobile app types (existing vs.

new), data types (person vs. online) and brand types (established vs. new). For now, we develop the first two hypotheses in the context of study 1. For the conference, we will have conducted all three experiments to illuminate the overall research framework (see Figure 1).

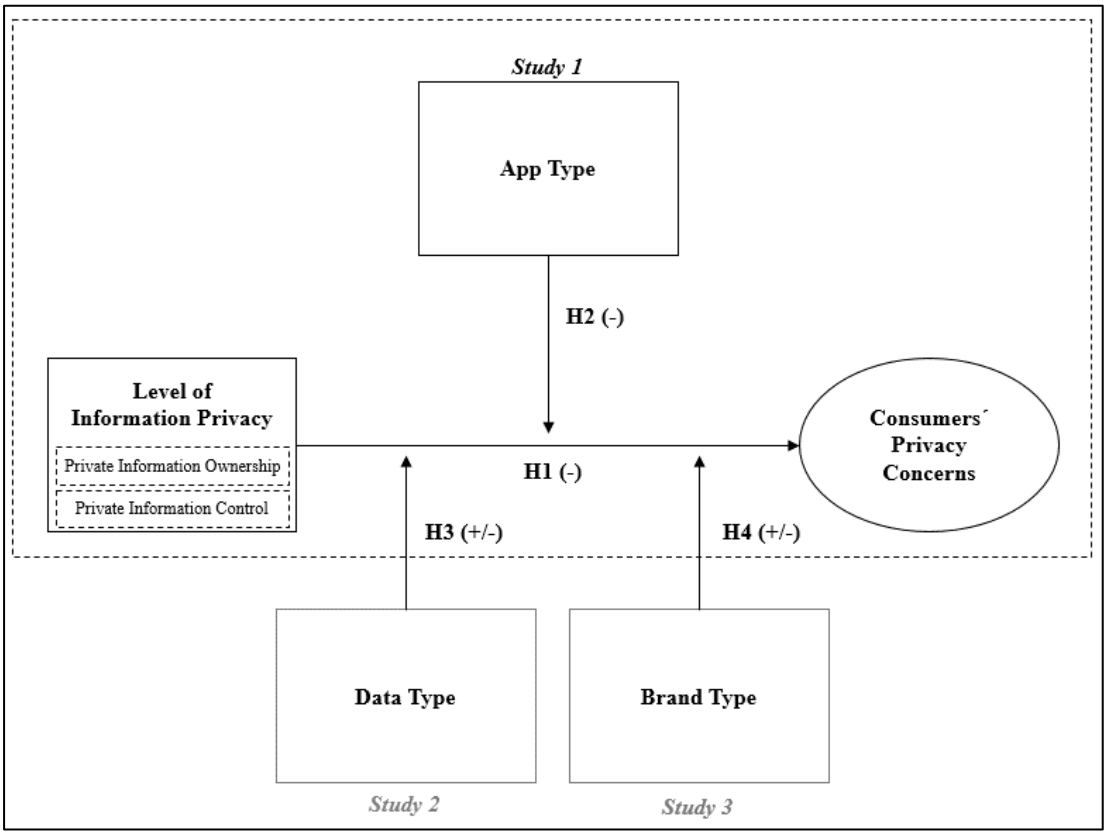
Study 1
App Type
H2 (-)
Level of Information Privacy
Private Information Ownership
Private Information Control
H1 (-)
Consumers´ Privacy Concerns
H3 (+/-)
H4 (+/-)
Data Type
Brand Type
Study 2
Study 3

Figure 1. Research Framework on the Formation of Consumers´ Privacy Concerns

3.1 The impact of information privacy levels

Consistent with prior research and in line with CPM theory, privacy management can be constituted through dimensions of (1) private information ownership, (2) private information control over flow of information and (3) boundary turbulences (Petronio, 1991; Xu et al., 2012). All dimensions are responsible for the management of users´ privacy boundaries, the decision to disclose information to potential co-owners and the formation of privacy concerns (Petronio, 2002). If a user of an app decides to share personal information with a co-owner, i.e. a mobile app, both parties agree on a collective privacy management. If the co-owner violates the boundary coordination rules, the owner (consumer) develops privacy concerns.

Following CPM theory, we look at the dimensions of private information ownership and control by capturing the LIP of a mobile app. Here, we expect that a low LIP, i.e. many permission rights and request of data transfer to third parties, will exceed consumers´ accepted privacy coordination rules. In particular, a privacy turbulence that limits consumers´ control of information flow and ownership beliefs is likely to happen. Consequently, consumers develop more severe privacy concerns towards the mobile app. In contrast, we assume that a version with less extensive permission requests resembles a higher LIP, i.e. more control and ownership for the consumer (Dinev, Xu, Smith, & Hart, 2013). Therefore, we assume that higher levels of information privacy will enhance consumers´ feelings of private information ownership and control and thus, reduce potential privacy concerns´ of sharing private information with the app. Based on that, we hypothesize:

H1: A high LIP compared to a low LIP leads to lower privacy concerns.

3.2 The moderating effect of app type

The landscape of mobile apps encompasses high uncertainties and intransparency towards quality, trustworthiness and value (Keith, Babb, Lowry, Furner, & Abdullat, 2015). From a CPM perspective, these uncertainties drive potential turbulences for consumers´ privacy boundaries. In contrast to previous research focusing on information privacy related policies (e.g. Bansal, Zahedi, & Gefen, 2015) to manage potential boundary turbulences, we argue – based on insights from digital innovation marketing (Konya-Baumbach et al., 2019; Kuester et al., 2018) - that existing company- or app-related factors shape the effect of information privacy handling on privacy concerns. Especially companies that introduce new mobile apps are confronted with liabilities of newness, higher uncertainty and a lack of trustworthiness (Kuester et al., 2018). Furthermore, we argue that due to a missing record of accomplishment or brand reputation (Featherman & Pavlou, 2003; Kuester et al., 2018), users perceive the provision of access rights to collect and transmit private information as more threatening in the context of a new app scenario.

In contrast, existing apps can account for a certain popularity, network sizes and prior experiences that reduce feelings of uncertainty and provide more knowledge about the real value of an app (Gu et al., 2017). While higher levels of information privacy indicate aspects of safety and control and thus, reduce potential privacy concerns, we assume that this effect is even stronger for an unknown, new app compared to the safer environment of an existing app. We hypothesize:

H2: The negative effect of a high LIP compared to a low LIP on consumers´ privacy concerns will be stronger for a new app compared to an existing app.

4. Methodology

4.1 Pilot and pre-test

For the scenario of an existing app, we chose an app that is widely used among smartphone users i.e. *Instagram*. For our second scenario of a new app, we ran a pilot test to evaluate the degree of newness among a set of apps that were not available in the German app market. Here, we selected the app of a new delivery service called “QickPack”.

4.2 Participants, design and procedure

We conducted a web-based survey among mobile app users of different ages, gender and educational backgrounds and assigned them randomly to the 2 (information privacy: low vs. high) x 2 (app type: existing vs. new) between subjects factorial design. After eliminating participants due to speeding behavior (Buchanan & Scofield, 2018) and missing data, our sample consists of 419 participants covering all age groups starting with 18 years or older. Overall, 31.5 % women and 68.5 % men participated.

We asked participants first whether they used or knew the existing app (*Instagram)* or the new app *(QuickPack).* After that, participants received information that the corresponding app will be re-launched due to an update of its information privacy with a display of new access rights (as table) and information regarding data storage, analysis and transmission to third parties (text). While there is no common operationalization of privacy levels, the two different LIPs (low vs. high) were shown with regard to requested permission rights for data collection and indications regarding the use/transmission of collected data. Then, participants were asked about their privacy concerns regarding the corresponding app (adapted from Dinev & Hart, 2006), and other aspects, such as privacy victim experience (adapted from Heng Xu and Hock-Hai Teo, 2004) or consumers´ privacy concerns (adapted from Liao, Liu, & Chen, 2011). Finally, we asked for other personal behaviour variables as well as demographic data.

5. Results

The manipulation check confirmed that participants in the high LIP scenario perceived a significantly higher extent of information privacy (M = 4.29) compared to the low information privacy scenario (M = 2.06; F = .100, $p < .001$). For testing our hypotheses, we used hierarchical moderated regression analyses (see Table 1). Model 1 presents the control variables only. Model 2 shows the direct effects of LIP and the app type on consumers´ privacy concerns. Here, a high LIP compared to a low LIP shows a significantly higher, negative effect on consumers´ formation of privacy concerns (β = -1.679, p < .001). Thus, we find support for H_1.

Dependent Variable Privacy Concerns	Model 1	Model 2	Model 3
Controls			
Gender	-.005	.002	.107
Age	.022	.071	.042
Income	-.002	-.003	-.003
Privacy Victim Experience	.073	.033	.051
General Privacy Concerns	.654***	.535***	.526***
Independet variables			
Level of Information Privacy (LIP)^a		-1.679***	.669
App Type^b		-.108	.621**
Moderation			
LIP^a x App Type^b			-1.488***
R^2	.275	.468	.506
Adj. R^2	266	.459	.497
F-value for R^2 difference	31.274***	74.872***	31.574***

* p<0.05;** p<0.01 ; *** p<0.001.

Notes: Unstandardized coefficients are shown.

^{a}0 = Low Level, 1 = High Level; ^{b}1 = Existing App, 2 = New App

Table 1. Hierarchical Moderated Regression Results

Model 3 reveals a significant moderating effect of app type on the main effect (β = -1.488, p < .001, H_2). Specifically, we see that the effect of offering a high LIP compared to low LIP leads to a significantly stronger reduction of consumers´ privacy concerns in the new app scenario (ΔM = 2.66; F = 51.168, p < .001) in comparison to the existing app scenario (ΔM = 1.13; F = .431, p < .001). Consequently, we also find support for H_2.

6. Overall Discussion and Conclusion

Although information privacy and data security topics are increasingly in the focus of information systems research (Pavlou, 2011), previous studies put only limited attention to how specific company- or app-related aspects influence privacy related concerns in the mobile app environment. In this particular environment, especially new applications are launched at a rapid pace but face profound challenges to reduce consumers´ privacy concerns (Featherman & Pavlou, 2003; Konya-Baumbach et al., 2019). Thereby, start-ups cannot build upon familiar brands, a record of accomplishments or high credibility and thus, need to find other measures to overcome these liabilities (Kuester et al., 2018).

Existing research that mainly builds upon privacy calculus theory (e.g. Dinev & Hart, 2006; Wang et al., 2016), finds mixed results regarding the effectiveness of privacy seals or assurances to reduce consumers´ privacy concerns (e.g. Feng & Xie, 2019; McKnight et al., 2004). Within our study, we test the effect of different information privacy levels on consumers´ privacy concerns, by following the logic of CPM theory. For our experiment, CPM theory drives the operationalization of privacy that ties on the understanding of data ownership and control. While CPM has mainly been investigated in the context of personal relationships, we apply the theory in the context of human-computer interaction regarding privacy management in mobile apps. Specifically, we show that high information privacy standards in terms of data ownership and control do work as a powerful instrument to reduce users´ privacy concerns.

Additionally, our present findings also reveal that the value of privacy enhancements varies among different app settings. While former studies already reveal that privacy perceptions vary across different app categories or businesses (e.g. Arora et al., 2017; Kang & Namkung, 2019), we enlarge the current understanding by illustrating that high privacy levels are of particular importance for the introduction of new apps compared to privacy enhancements of existing apps. Following the CPM perspective of privacy boundaries and turbulences, we deliver support that high privacy standards can work as a risk-reducing tool and substantiate an important value for start-ups in the mobile app industry (Konya-Baumbach et al., 2019). By providing a high privacy level within new apps, start-ups can mitigate disadvantages of missing trust and reputation in the marketplace and fundamentally reduce consumers´ privacy concerns.

7. References

Arora, S., ter Hofstede, F., & Mahajan, V. (2017). The Implications of Offering Free Versions for the Performance of Paid Mobile Apps. *Journal of Marketing*, *81*(6), 62–78.

Bansal, G., Zahedi, F. ‘M.’, & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*(6), 624–644.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce. *Communications of the ACM*, *48*(4), 101–106.

Buchanan, E. M., & Scofield, J. E. (2018). Methods to detect low quality data and its implication for psychological research. *Behavior research methods, 50*(6), 2586–2596.

Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management*, *39*, 49–59.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, *59*(4), 451–474.

Feng, Y., & Xie, Q. (2019). Privacy Concerns, Perceived Intrusiveness, and Privacy Controls: An Analysis of Virtual Try-On Apps. *Journal of Interactive Advertising*, *19*(1), 43–57.

Gerlach, J. P., Eling, N., Wessels, N., & Buxmann, P. (2019). Flamingos on a slackline: Companies' challenges of balancing the competing demands of handling customer information and privacy. *Information Systems Journal*, *29*(2), 548–575.

Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28.

Heng Xu and Hock-Hai Teo. (2004). Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective. *ICIS 2004*, 793–806.

Kang, J.-W., & Namkung, Y. (2019). The role of personalization on continuance intention in food service mobile apps. *International Journal of Contemporary Hospitality Management*, *31*(2), 734–752.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637–667.

Konya-Baumbach, E., Schuhmacher, M. C., Kuester, S., & Kuharev, V. (2019). Making a first impression as a start-up: Strategies to overcome low initial trust perceptions in digital innovation adoption. *International Journal of Research in Marketing*, *36*(3), 385–399.

Kuester, S., Konya-Baumbach, E., & Schuhmacher, M. (2018). Get the show on the road: Go-to-market strategies for e-innovations of start-ups. *Journal of Business Research*, *83*, 65–81.

Liao, C., Liu, C.-C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, *10*(6), 702–715.

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business. *Electronic Markets*, *14*(3), 252–266.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29.

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where are We Now And Where Should We Go? *MIS Quarterly*, *35*(4), 977.

Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. *Communication Theory*, *1*(4), 311–335.

Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure*. *SUNY series in communication studies*. Albany: State University of New York Press.

Shilton, K., & Greene, D. (2019). Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal of Business Ethics*, *155*(1), 131–146.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531–542.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring Mobile Users' Concerns for Information Privacy. *International Conference on Information Systems, ICIS 2012, Vol. 3*, 2278–2293.