Aug 10th, 12:00 AM

How do Habit and Privacy Awareness Shape Privacy Decisions?

Christina Wagner
University of Augsburg, christina.wagner@wiwi.uni-augsburg.de

Manuel Trenz
University of Goettingen, trenz@uni-goettingen.de

Daniel Veit
University of Augsburg, daniel.veit@wiwi.uni-augsburg.de

How do Habit and Privacy Awareness Shape Privacy Decisions?

Completed Research

Christina Wagner
University of Augsburg
christina.wagner@wiwi.uni-augsburg.de

Manuel Trenz
University of Goettingen
trenz@uni-goettingen.de

Daniel Veit
University of Augsburg
daniel.veit@wiwi.uni-augsburg.de

Abstract

Technology companies can benefit from users' habitual technology use as a reinforcement of technology continuance. Such habitual behavior can be amplified through personalized service experiences, for which companies need to request their users' data. However, in the presence of strong habit, users might agree to privacy updates and decide to continue using services without weighing privacy related risks against expected benefits. To date, privacy research has given little attention to technology habit. We aim to fill this research gap by drawing on the privacy calculus theory, contextual privacy awareness (CPA), and prior studies on habit in technology continuance research. We conduct an experiment with mobile app users and find that habit does indeed influence privacy decisions. Further, we find that CPA makes users pay more attention to risks involved with a privacy update. Our framework illuminates the relevance of habit in privacy decision making for users and app providers.

Keywords

Privacy, habit, privacy awareness, continuance, privacy calculus, mobile apps, experiment.

Introduction

Technology has led to tremendous changes in our everyday behavior and routines. Especially mobile phones are subject to frequent and automatic use, and therefore breeding grounds for creating habits. In information systems (IS) research, habits have been identified as an important determinant of technology continuance (Limayem et al. 2007). Therefore, firms have invested significantly into services that foster habitual behavior, such as smart recommendations and personalization features. A necessary prerequisite is an extended access to users' personal data, which needs to be authorized through explicit privacy-related requests and updates. Despite these requests, a strong technology habit might lead users to disclose their personal information to continue using the technology - even if their personal information will be handled in a way that is not in alignment with their privacy needs and preferences. Studies on information privacy have started to consider factors outside of rational decision making (Kehr et al. 2015). Yet, little attention has been given to technology habit, which has been characterized in prior research as opposite to cognitively-effortful actions (Hou et al. 2019). Based on prior studies on technology continuance (Kim et al. 2005), we look at ways in which habit can influence continuance intentions. Applied to the context of privacy, habit can, on the one hand, influence continuance directly. On the other hand, habit can influence privacy decisions through affecting its situation-specific antecedents.

The goal of our study is twofold. First, we aim at identifying how habit affects the evaluation of a privacy update in the context of continued mobile app use. Second, we intend to identify the contextual boundaries of these influences, starting with an investigation of situations with high and low contextual privacy awareness (CPA). We pose the following research question: *How do mobile app habit and CPA influence privacy decisions for mobile app continuance?* To address this question, we conduct a review of extant

literature on privacy and technology-related habit and propose an integrative model of habit and privacy decisions. In doing so, we draw on the privacy calculus framework (Dinev et al. 2015; Laufer and Wolfe 1977) to represent the conscious evaluation of risks and benefits. The impact of habit is derived from the conceptualization of habit as automaticity in prior research. We then introduce the concept of CPA as a way to increase the extent to which situation-specific factors related to a privacy decision are consciously evaluated and investigate its potential to reduce the influence of habit on the privacy decision. To test our proposed model, we conduct an online experiment, confronting current WhatsApp (WA) users in conditions with different CPA with a privacy update and observe their reactions. The major contribution of this work is to illuminate the role of habit in privacy decision making, making both individuals as well as app providers understand how users react to privacy updates in the presence of habits. That can help users make more sovereign privacy decisions to sustain a state of privacy with which they are content, and providers to sustain their user-base in the long-term.

The remainder of this paper is organized as follows. The next section provides a condensed overview of the main results of our review of privacy and habit research. Thereafter, we will outline our research model. The subsequent section displays our research methodology and study design. Subsequently, we present the results of our data analysis. Finally, we discuss these results, as well as the contributions and limitations of this work.

Conceptual Background

Privacy

In our attempt to study individuals' privacy decisions and their control of access (Westin 1967), we apply the cognate-based view of privacy (Smith et al. 2011) and define information privacy as "an individual's self-assessed state in which external [actors] have limited access to information" (Dinev et al. 2013, p. 299). A well-established perspective on privacy-related decisions is the privacy calculus (Dinev et al. 2015; Laufer and Wolfe 1977). It generally assumes a rational evaluation of positive and negative consequences associated with information disclosure. According to the theory, individuals will only share information with others if the anticipated beneficial consequences of that disclosure outweigh the perceived negative consequences. Laufer and Wolfe (1977), in one of the earliest applications of the privacy calculus, emphasize the importance of situational factors in the evaluation of consequences of information disclosure. We also apply the situational privacy calculus, characterized by a trade-off between perceived risks and perceived benefits related to a specific privacy decision. We define privacy risks as the "expectation that a high potential for loss is associated with the release of personal information" (Malhotra et al. 2004, p. 341). To represent the positive side of the privacy calculus, we follow Kehr et al. (2015) and focus on situation-specific benefits that can only be obtained through a privacy disclosure.

Even though the privacy calculus theory suggests a purely rational evaluation of risks and benefits, the rationality of the behavior observed may be bounded by incomplete information, the inability to process large amounts of data, and systematic psychological deviations from rationality (Acquisti and Grossklags 2005). The resulting dichotomy between privacy attitudes and resulting behavior is termed the privacy paradox (Barth and de Jong 2017; Norberg et al. 2007; Smith et al. 2011). This research introduces habits in our interaction with information technologies as an explanatory factor for deviations from rational privacy decisions.

Habit

Habits are formed and strengthened through repetition and learning in a stable context, producing satisfaction. Once established, they can be triggered by certain external or internal cues (Soror et al. 2015). Habit is characterized by automaticity, distinguishing it from deliberate and planned behavior. Along the dimensions of automaticity, previous research describes habit as being outside of conscious awareness of its trigger or its execution, therefore difficult to control, but also as mentally efficient, requiring little conscious processing, and as distinct from conscious intention formation (Chiu and Huang 2015). The understanding of habit as automaticity is related to dual processing theories, according to which information can be processed in two ways, (1) systematic, high-effort, and conscious processing and (2) heuristic, low-effort, and automatic processing (Chaiken 1980). By its characteristic, habit falls into the category of low-effort processing (Hou et al. 2019). If low-effort processing is used, decision making

becomes more susceptible to the influence of biases (Dinev et al. 2015). Relying on the discussion of the relationship between goals, cues, and habit in previous research, we define habits as "learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states" (Verplanken et al. 1997, p. 540).

Recent research on IS security has looked into the role of habituation as a reason for why users tend to ignore security warnings. Habituation to security warnings is the diminishing of attention due to frequent exposure to such warnings (Anderson et al. 2016). We intend to emphasize that in our understanding habit is distinct from habituation, as the latter lacks its satisfactory element, which distinguishes habit from routines (Limayem et al. 2007). Technology continuance is particularly susceptible to the effect of technology habit, as it relies to a large extent on non-reflective, routinized cognitive processes (Limayem et al. 2007). Recent research in technology continuance and use has investigated various ways in which it may be affected by habit (Bhattacherjee and Lin 2015; Limayem et al. 2007). Relying on the role of habit in continuance research and moving beyond the role of habituation in recent privacy research, we aim to focus on general technology habits and how they affect the evaluation of privacy decisions and thereby the continuance of that technology.

Privacy Awareness

As habits are triggered directly by the environment, they are processed faster, have fewer demands on an individual's limited capacity of self-control, and hence often overrule conscious decision making (Verplanken and Wood 2006). In the case of privacy decisions, habit might therefore lead to unreflective decisions that one might regret in the future. However, certain contextual characteristics could lead to more or less automatic (or conscious) decision making (Dinev et al. 2015; Verplanken and Wood 2006). Previous habit research suggests that habits can best be disrupted through changes in context (Verplanken and Wood 2006). In IS literature, few studies have delved into habit disruption. Some exceptions are Hou et al. (2019), who leveraged on new technological features to interfere with habitual gaming behavior, and Polites and Karahanna (2013), who proposed various strategies to disrupt incumbent IT system use habits in organizations.

Privacy research shows that despite the importance of situation-specific aspects in privacy decisions, global privacy related attitudes that stem from the salience of privacy issues, i.e. CPA, play an important role as well (Kehr et al. 2015). John et al. (2011) show that the disclosure of private information might be impacted by environmental cues that bear little connection to objective hazards. Privacy awareness has been defined as the "extent to which an individual is informed about [...] privacy practices" (Smith et al. 2011, p. 998). Increasing privacy awareness has been identified as a meaningful tool to ensure the consideration of relevant factors in privacy-decision making and is viewed as one attempt to resolve the privacy paradox (Barth and de Jong 2017). CPA needs to be distinguished from privacy awareness that stems from personal privacy dispositions, in that it can be induced through the design of the decision context or salient privacy events in the environment (Benamati et al. 2017).

Research Model and Hypotheses

In the following, our hypotheses are developed and visually displayed in our research model (see Figure 1). Building on prior research, we will consider a privacy update that changes the features of the technology, as well as the potential of user information being accessed by a third party. The resulting perceived privacy risks and benefits represent the theoretical perspective of the privacy calculus, whose relationships will not be explicitly hypothesized due to consistent findings in prior research (e.g. Kehr et al. 2015).

When using a technology has become a habit, the automaticity of that behavior is expected to positively affect the continued use of that technology. Previous research on technology continuance has found that habit directly affects continuance intentions (Hong et al. 2011). We expect technology habit to be positively related with continuance intentions as well.

H1: Habit will be positively related to continuance intentions.

Based on the discussion of prior literature above, technology habit might influence the way that this privacy and the subsequent continuance decision are formed. Our aim is to uncover how habit impacts privacy and continuance decisions. Therefore, we integrate the impact of technology habit on perceptions related to a

privacy update as well as on technology continuance. When habit is strong, expectations of the environment in which the behavior is performed have already been formed and influence how the actual performance environment is perceived. Thus, the sensitivity to small changes in the performance environment decreases, the search for new information is biased towards information that supports the habitual behavior, and complexity and deliberation of decision making are lower as well (Verplanken et al. 1997; Verplanken and Wood 2006). Dinev et al. (2015) propose various biases that may affect the privacy calculus in conditions of low level of effort in privacy decision making. As introduced above, the automaticity inherent to habit is associated with low-effort processing, making decisions more susceptible to the influence of biases. One bias that may become apparent if habit is strong is the optimistic bias (Dinev et al. 2015; Taylor and Brown 1988). Accordingly, factors are evaluated overly optimistic, wherefore the probability of "winning" is affected positively, whereas risk will be underestimated (Dinev et al. 2015). For example, college students posting pictures of themselves drinking excessively on Facebook often underestimate the consequences this might have when these pictures fall into the "wrong" hands, such as those of a potential employer (Dinev et al. 2015). Subsequently, we expect that if technology habit is strong, any privacy update that will be received via that technology will be perceived as less risky and more beneficial, in order to support the habitual behavior. Based on that reasoning, we hypothesize:

H2: Habit will be negatively related to perceived privacy risks.

H3: Habit will be positively related to perceived benefits.

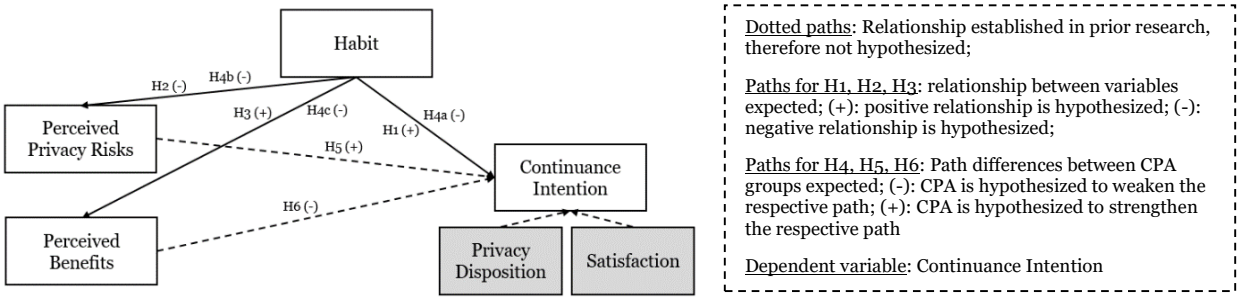

Figure 1. Research Model

As discussed above, both privacy decisions and habit are susceptible to contextual changes. We manipulate CPA to find out, how it affects both the privacy decision and the influence of habit on that decision. CPA can be induced through privacy events in the environment, such as media reports about recent privacy breaches, excessive data collection, security issues, or online surveillance. Alternatively, CPA can be stimulated through regulatory changes by public policy, such as the introduction of new data protection laws (Benamati et al. 2017; Malhotra et al. 2004). We induce CPA by displaying information about general privacy risks that are unrelated to objective risks involved with a privacy request. Increasing CPA might change the way in which habit affects the privacy decision. By changing the context in which the privacy update takes place, the influence of habit on the privacy decision might be disrupted (Verplanken and Wood 2006). Increasing a user's CPA before asking them to disclose information is therefore expected to decrease the effect of habit.

H4: CPA will decrease the effect of habit on (a) continuance intentions, (b) perceived privacy risks, and (c) perceived benefits.

Increasing CPA might not only diminish the influence of habit, but also change the privacy decision making process per se, through increasing the conscious effort with which a privacy decision is made (Dinev et al. 2015). Thereby, the search for new information will be less biased towards information that supports the habitual behavior (Verplanken et al. 1997; Verplanken and Wood 2006). CPA is therefore expected to make users evaluate potential risks and potential benefits from a privacy update more critically.

H5: CPA will increase the effect of perceived privacy risks on continuance intentions.

H6: CPA will decrease the effect of perceived benefits on continuance intentions.

Our model considers two control variables, satisfaction and privacy disposition. Satisfaction with a technology has been found an important explanatory factor of technology continuance in prior research (e.g. Bhattacherjee and Lin 2015). By controlling for satisfaction with the technology, we want to avoid confounding effects with technology habit. Additionally, our focus is on how users perceive the privacy update itself and the value added through it. Controlling for technology satisfaction allows us to control for individual differences in user satisfaction with the technology before the update. Users' personal dispositions towards privacy will affect the way they evaluate a privacy update, as well as the way that they perceive CPA. Prior research has found that privacy disposition is a personality characteristic that is independent of situational privacy events (Karwatzki et al. 2017). To avoid these personality differences confounding our model, we will control for privacy disposition as well.

Research Methodology

Our research model is situated in a mobile app context as one that frequently requires information disclosure and at the same time is prone to habitual behavior. Habit therefore refers to a mobile app habit that possibly infers a privacy decision regarding an update on that mobile app. The privacy calculus has been applied to a mobile phone context by various studies already (e.g. Kehr et al. 2015), wherefore when introducing the new construct habit, we can rely on an environment where the relationships between these privacy constructs have already been empirically validated. Specifically, we chose the mobile messaging app WA as our research context. Consistent with our definition of habit, WA habit is the automatic use of WA in a situation where one wants to communicate with another, to reach the goal that one wants to achieve through that communication, such as strengthening a relationship or interpersonal awareness (Lowry et al. 2011).

As we aim to investigate the potential of shifting privacy decision making from automatic to conscious through a change in CPA, we conducted a between-subjects online experiment, manipulating CPA. We asked users to read an article prior to presenting them with the privacy update. The experimental group received an article that describes general privacy risks involved with disclosing data to online firms prior to the privacy decision. These risks are unrelated to instant messaging or WA and should therefore not objectively change the perceived risks from the subsequent privacy update (Extract: "(…) When sensitive information, such as your credit card information stored by [firm x], is accessed by third parties (e.g. hackers), you can suffer from immense financial losses (…)") The control group was asked to read an article on the same firm, but focusing on renewable energy rather than privacy issues (Extract: "(…) Last year, [firm x] consumed as much energy as the city of San Francisco. Next year, it said, all of that energy will come from wind farms and solar panels (…)"). Participants were randomly assigned to one of the two groups in our experimental design. Figure 2 represents the experimental process.

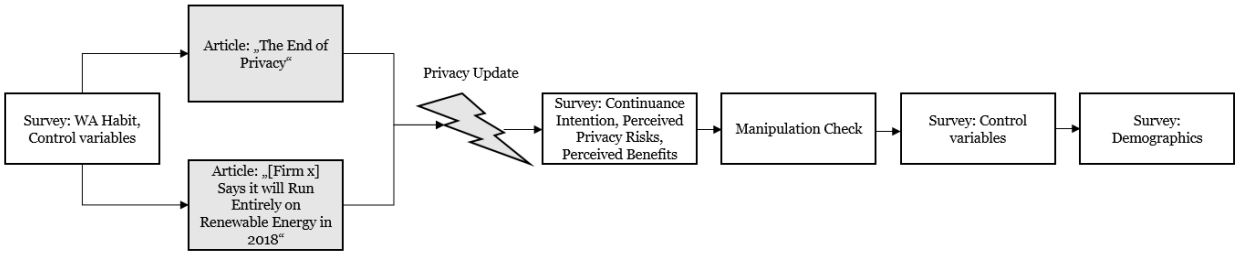

Figure 2. Experimental Process

The privacy decision was modeled through a description of an allegedly forthcoming update to the WA messaging app. To make our experiment as realistic as possible, participants were presented with realistic details on the update (see Figure 3), designed and worded similarly to previous ones. Agreeing to the privacy update was described as necessary to continue using the app. This represents the reality of many privacy requests. Subsequently, participants were asked for their intention to continue and the risks and benefits they associated with the information disclosure necessary for this update.

All constructs in this study are of reflective nature. To ensure construct validity, we adapted scales from previous studies to the context of WA. Habit is operationalized through the Self-Report-Habit-Index developed by Verplanken and Orbell (2003) (e.g., HABT02: "Using WhatsApp is something I do automatically."). Perceived privacy risks and benefits are measured with scales adapted from Dinev et al.

(2013) to the context of this privacy update (e.g., RISK04: "Agreeing to the new WhatsApp Terms and Privacy Policy could involve many unexpected problems."; BENE03: "I believe that if I agree to the new WhatsApp Terms and Privacy Policy, I will benefit from a better, more customized service."). Continuance intention is adapted from Limayem et al. (2007) (e.g., CONT01: "I intend to continue using WhatsApp rather than discontinue its use."). Additionally, we include several control variables, attention checks, as well as manipulation checks.

Data was collected via the British research platform "Prolific Academic" and limited to WA users from the United Kingdom. In total, 210 users took part in the online experiment. After eliminating responses that failed several attention checks as well as those exhibiting extremely conspicuous response behaviors, 127 observations (71 in the experimental group and 56 in the control group) remained for further analysis.

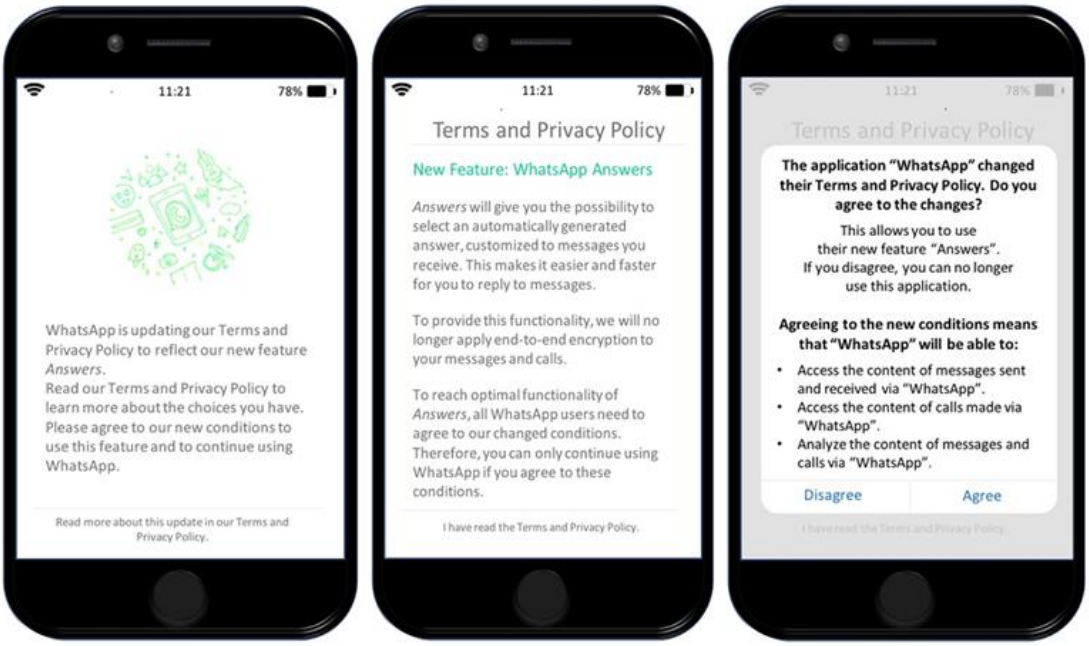

Figure 3. WhatsApp Privacy Update

Results

Both our measurement and structural model were assessed with partial least squares structural equation modeling (PLS-SEM), using SmartPLS 3.2.8. Due to the rather exploratory nature of the study and the complexity of our theoretical model, PLS-SEM was regarded as the most suitable means for analysis (Hair et al. 2017). Henseler's (2007) multigroup analysis (MGA) was used to detect path differences due to CPA.

Manipulation Check, Common Method Bias, and Measurement Validation

Manipulations were checked through an instructional attention check (asking participants to click on the headline of the article instead of the "Next"-button at the end of the page), multiple-choice questions, as well as through perceptual questions that measure the effectiveness of the manipulation. For the perceptual questions, we measured privacy concerns (Kim et al. 2016). Participants in the CPA group indicated significantly higher privacy concerns than the control group, ($t(72,778) = 2.080$, $p = .040$). T-tests further revealed that participants assigned to different groups did not significantly differ regarding their age, income, number of mobile phone apps, privacy disposition, privacy experience, WA experience, WA perceived usefulness, WA satisfaction, mobile phone experience, and WA habit.

Since our endogenous and exogenous variables were collected through the same survey, we conducted several precautions and tests to ensure that common method bias did not influence our results. Regarding our questionnaire design we followed the suggestions by Podsakoff et al. (2003). The marker variable approach showed that the maximum shared variance between the marker variable and another construct is

1.04% for perceived benefits. Therefore, we are confident that common method bias did not influence our findings.

Regarding measurement reliability and validity, our measures exhibit item loadings above .707, as well as exceed the recommended levels of .5 for the average variance extracted (AVE), supporting convergent validity. Concerning the internal consistency of our measures, Cronbach's Alpha (CA) and composite reliabilities (CR) values are within the acceptable range (Hair et al. 2017) (see Table 1). The discriminant validity of our constructs could be established through comparing item-cross loadings, applying the Fornell-Larcker criterion (see Table 1), and investigating the Heterotrait-Monotrait Ratio of correlations (Hair et al. 2017). Overall, these results provide support for the validity and reliability of our measurement model.

	AVE	**CA**	**CR**	**CONT**	**HABT**	**BENE**	**RISK**	**WSAT**	**PDIS**
CONT	.876	.928	.955	.936					
HABT	.719	.951	.958	.339	.848				
BENE	.711	.800	.881	.512	.165	.843			
RISK	.688	.851	.898	-.436	-.058	-.438	.830		
WSAT	.739	.882	.919	.276	.419	.096	-.065	.860	
PDIS	.636	.811	.874	-.173	.015	-.142	.202	-.019	.797

Table 1. Measurement Validation

Findings

We tested the hypothesized relationships for H1, H2, and H3 by estimating a PLS-SEM for our control group. We estimated the parameter significance by using bootstrapping with n = 5,000 samples. The results are summarized in table 2. For the control group, the results confirm the positive relationship between habit and continuance intentions (β_c = .249, p = .047), which is in line with findings from prior research and supports H1. For the experimental group receiving the CPA, the structural model results do not show a significant path coefficient between habit and continuance intentions. The hypothesized relationship between habit and perceived privacy risks, is not found significant in either of the experimental groups. We therefore cannot support H2. For the relationship between habit and perceived benefits, the path coefficient in the control group is significant and positive (β_c = .272, p = .009), supporting H3. The same relationship in the experimental group is not found significant.

Path	**CPA group (β_{CPA})**	**Control group (β_c)**	**MGA (β_Δ)**
BENE -> CONT	.244	.337**	.093 (H6: not supported)
RISK -> CONT	-.420**	-.102	.318* (H5: supported)
HABT -> CONT	.151	.249* (H1: supported)	.098 (H4a: not supported)
HABT -> RISK	-.088	-.112 (H2: not supported)	.024 (H4b: not supported)
HABT -> BENE	.130	.272** (H3: supported)	.143 (H4c: not supported)
PDIS -> CONT	.004	-.119	.123
WSAT -> CONT	.126	.231*	.105
*p < .05, **p < .01, ***p < .001			

Table 2. Results of Structural Model Analysis

Hypotheses 4, 5, and 6 refer to selected path differences between the experimental group and control group. Comparing the paths between habit and continuance intentions, perceived privacy risk, and perceived benefit, respectively, we find that all paths are lower in the group that received the CPA manipulation. The paths leading from habit to continuance intentions and perceived benefits are only significant for the control groups. One explanation could be that habit is disrupted by CPA, and therefore does no longer influence continuance intentions and perceived benefits. To confirm this, however, the significance of these

differences needs to be tested. Sarstedt et al. (2011), in their comparison of various MGA methods, found that the analysis developed by Henseler (2007) is one of the more conservative means to compare path differences between groups. Table 2 includes the results of the MGA based on Henseler (2007). Even though, the path coefficients between habit and continuance intentions, perceived privacy risks, and perceived benefits differ between the two manipulation groups, these differences are not found significant. We can, therefore, not support H4.

For the experimental group receiving the CPA manipulation, the path between perceived privacy risk and continuance intentions is significant and negative (β_{CPA} = -.420, p = .001). Contradicting with prior research on the privacy calculus, this path is not significant for the control group. As the path between perceived privacy risks and continuance intentions is stronger for the group receiving the CPA manipulation, we again conduct a MGA to test whether this path is significantly higher than the respective path in the control group. The MGA shows that the path coefficient significantly increases when a user receives the CPA (β_{Δ} = .318, p = .032). This finding supports H5.

For the control group, in line with prior research on the privacy calculus, perceived benefits of the privacy update are positively related with continuance intentions (β_c = .337, p = .008). But, when introducing CPA, the path between perceived benefits and continuance intentions is not found significant. This finding is in line with our expectation that benefits will be considered to a higher extent when forming one's continuance intention if habit not disrupted. Our reasoning is that the evaluation of new information received through the privacy update will be less biased towards information that supports the habitual behavior. However, the MGA shows that these differences are not significant, wherefore we cannot support H6. Regarding the control variables, only WA Satisfaction significantly increase continuance intentions in the control group (β_c = .231, p = .043).

An additional post-hoc analysis, inspired by the findings by Limayem et al. (2007), considered a moderating effect of habit on the relationships between perceived risks and continuance intentions. This moderating effect was found statistically insignificant.

Discussion and Conclusion

This experimental study on privacy decisions and the effects of habit and CPA in the context of mobile apps is, to our knowledge, one of the first attempts at integrating technology habit into IS privacy decision making frameworks. It shows several interesting and surprising results. Habit was found to significantly influence some aspects of privacy and related continuance decisions. This finding implies that habit might be another important factor to explain deviations from fully rational privacy decisions. Most of the relationships in our control group are consistent with prior literature on the privacy calculus and the impact of habit on continuance intentions. One of our most surprising results is that the influence of habit on the privacy decision could not be changed through CPA. Creating awareness to privacy issues, therefore, does not resolve the central issue of habit impacting a user's privacy decision making, distorting their decision towards continuing using a technology. Despite CPA, conscious predictors of continuance intentions might be evaluated in a biased way, being impacted by habit. However, CPA was found to significantly increase the extent to which perceived privacy risks are considered in privacy decision making. Privacy awareness, therefore, despite not changing the influence of habit, does change the conscious effort with which the privacy decision is made. As a result of increased privacy awareness, users pay more attention to risks involved with a privacy update and potentially terminate their use of a service if perceived risks are too high. Perceived benefits, on the contrary, will not be taken into account to a significantly lesser extent if privacy issues are (made) salient in the users' environment. As the influence of habit on perceived benefits does not significantly decrease through CPA, a user's evaluation of benefits might still be biased towards only perceiving positive aspects of the privacy update to support their habitual behavior if they are not privacy aware.

Theoretically, we contribute to both continuance and privacy research. First, we propose and empirically test a framework of how habit can influence privacy decisions in the context of mobile app continuance - combining two streams of research. Second, with the increasing availability and variety of technological devices, it becomes necessary for privacy research to move beyond the acceptance of a privacy request through a disclosure decision. By looking at the effect of a privacy update on technology continuance, we move beyond prior privacy research that focuses on information disclosure. Third, we add to privacy

research by integrating another subconscious factor into rational privacy models, thereby providing theoretical advances on the boundaries of rational decision making, and empirically validating the privacy calculus in the context of mobile app continuance. Finally, we looked at the effect of CPA on the effect of habit on a privacy decision, as well as on the privacy decision itself. Based on our insignificant findings related to the disruption of habit through CPA, future research is needed to continue the development of strategies that disrupt the influence of habit on privacy decisions.

Whether users want to continue using a mobile app can be influenced by their habit of using this app. Mobile app users with strong habits are therefore more likely to continue using the app, and also factor this in more strongly in favor of disclosing information to be able to continue using the app. The contextual change of making users aware of privacy issues can provide both regulators as well as technology providers with means to help citizens and customers be aware of risks involved with a privacy decision. Thereby, users' long-term contentment with both their privacy state as well as with the technology itself can be ensured, which would also benefit technology providers by strengthening their customer base. However, creating privacy awareness alone does not suffice to disrupt the influence of technology habit on privacy decisions. Based on the habit disruption framework by Verplanken and Wood (2006), it might be necessary to develop strategies that disrupt habit over a longer period of time.

This study is also subject to several limitations. The first limitation is related to the external validity of our results. As our study design and the privacy update are very specific to WA, our results might not apply to other contexts. Future research might further enhance this theoretical perspective by considering the contexts of continuous use of wearable and smart devices that are not only susceptible to the creation of habit, but relevant due to their extensive collection of user data. Second, we measured continuance intentions and not continuance behavior. As habit's innate characteristic is automaticity, it is possible that it directly affects behavior. However, measuring actual behavior was not feasible in this study, wherefore future research is needed to validate our results. The third limitation is related to our study design. Analyzing continuance and habit through a longitudinal research design might be interesting for future research to expand on the effect of privacy awareness and possibly other habit disruption strategies through a longitudinal study, measuring how habit changes over time.

REFERENCES

Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26–33.

Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., and Eargle, D. 2016. "From Warning to Wallpaper: Why the Brain Habituates to Security Warnings and What Can Be Done About It," *Journal of Management Information Systems* (33:3), pp. 713–743.

Barth, S., and de Jong, M. D. T. 2017. "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review," *Telematics and Informatics* (34:7), pp. 1038–1058.

Benamati, J. H., Ozdemir, Z. D., and Smith, H. J. 2017. "An Empirical Test of an Antecedents – Privacy Concerns – Outcomes model," *Journal of Information Science* (43:5), pp. 583–600.

Bhattacherjee, A., and Lin, C.-P. 2015. "A Unified Model of IT Continuance: Three Complementary Perspectives and Crossover Effects," *European Journal of Information Systems* (24:4), pp. 364–373.

Chaiken, S. 1980. "Heuristic versus Systematic Information Processing and the Use of Source versus Message Cues in Persuasion.," *Journal of Personality and Social Psychology* (39:5), pp. 752–766.

Chiu, C.-M., and Huang, H.-Y. 2015. "Examining the Antecedents of User Gratification and its Effects on Individuals' Social Network Services Usage: The Moderating Role of Habit," *European Journal of Information Systems* (24:4), pp. 411–430.

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box," *Information Systems Research* (26:4), pp. 639–655.

Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts," *European Journal of Information Systems* (22:3), pp. 295–316.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Richter, N. F., and Hauff, S. 2017. *Partial Least Squares Strukturgleichungsmodellierung (PLS-SEM)*, Munich, Germany: Vahlen.

Henseler, J. 2007. "A New and Simple Approach to Multi-Group Analysis in Partial Least Squares Path Modeling," in *Causalities Explored by Indirect Observation: Proceedings of the 5th International Symposium on PLS and Related Methods (PLS'07)*, H. Martens and T. Næs (eds.), pp. 104–107.
Hong, W., Thong, J. Y. L., Chasalow, L. C., and Dhillon, G. 2011. "User Acceptance of Agile Information Systems: A Model and Empirical Test," *Journal of Management Information Systems* (28:1), pp. 235–272.
Hou, J., Kim, K., Kim, S. S., and Ma, X. 2019. "Disrupting Unwanted Habits in Online Gambling Through Information Technology," *Journal of Management Information Systems* (36:4), pp. 1213–1247.
John, L. K., Acquisti, A., and Loewenstein, G. 2011. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research* (37:5), pp. 858–873.
Karwatzki, S., Dytynko, O., Trenz, M., and Veit, D. 2017. "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization," *Journal of Management Information Systems* (34:2), pp. 369–400.
Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607–635.
Kim, D. J., Yim, M., Sugumaran, V., and Rao, H. R. 2016. "Web Assurance Seal Services, Trust and Consumers' Concerns: An Investigation of E-commerce Transaction Intentions across two Nations," *European Journal of Information Systems* (25:3), pp. 252–273.
Kim, S. S., Malhotra, N. K., and Narasimhan, S. 2005. "Two Competing Perspectives on Automatic Use: A Theoretical and Empirical Comparison," *Information Systems Research* (16:4), pp. 418–432.
Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22–42.
Limayem, M., Hirt, S. G., and Cheung, C. M. K. 2007. "How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance," *MIS Quarterly* (31:4), pp. 705–737.
Lowry, P. B., Cao, J., and Everard, A. 2011. "Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures," *Journal of Management Information Systems* (27:4), pp. 163–200.
Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336–355.
Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879–903.
Polites, G. L., and Karahanna, E. 2013. "The Embeddedness of Information Systems Habits in Organizational and Individual Level Routines: Development and Disruption," *MIS Quarterly* (37:1), pp. 221–246.
Sarstedt, M., Henseler, J., and Ringle, C. M. 2011. "Multigroup Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results," *Advances in International Marketing* (22), pp. 195–218.
Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 980–1016.
Soror, A. A., Hammer, B. I., Steelman, Z. R., Davis, F. D., and Limayem, M. M. 2015. "Good Habits Gone Bad: Explaining Negative Consequences Associated with the Use of Mobile Phones from a Dual-Systems Perspective," *Information Systems Journal* (25:4), pp. 403–427.
Taylor, S. E., and Brown, J. D. 1988. "Illusion and Well-Being: A Social Psychological Perspective on Mental Health.," *Psychological Bulletin* (103:2), p. 193.
Verplanken, B., Aarts, H., and Van Knippenberg, A. 1997. "Habit, Information Acquisition, and the Process of Making Travel Mode Choices," *European Journal of Social Psychology* (27:5), pp. 539–560.
Verplanken, B., and Orbell, S. 2003. "Reflections on Past Behavior: A Self-Report Index of Habit Strength," *Journal of Applied Social Psychology* (33:6), pp. 1313–1330.
Verplanken, B., and Wood, W. 2006. "Interventions to Break and Create Consumer Habits," *Journal of Public Policy & Marketing* (25:1), pp. 90–103.
Westin, A. F. 1967. *Privacy and Freedom*, New York: Athenum.