

Don't Be Creepy: Investigating Consumer Intentions to Switch Privacy Settings

Matilde Rapezzi
University of Bologna

Carla Freitas Silveira Netto
Pontifical Catholic University of Paraná

Gabriele Pizzi
University of Bologna

ABSTRACT

When consumers download mobile apps that require consent to use personal data, they are often unaware of what information is being shared or how it will be used. Despite this, many accept the terms and conditions without fully understanding the potential consequences. This research explores what happens after the decision to disclose personal data has been made. Specifically, it investigates the role of perceived creepiness on consumers' intentions to switch the privacy settings of mobile apps. Through a preregistered lab experiment, this research finds that the more consumers feel creeped out by an app, the more likely they are to change its privacy settings, reducing the amount of personal information shared with the service provider. This response is driven by heightened privacy concerns. By focusing on the role of creepiness in influencing consumer behavior, this study uncovers previously underexplored effects of this emotion. Our findings contribute to the emerging literature on creepiness, as well as to research on privacy concerns and consumer switching behaviors. Finally, the results provide managerial insights that can benefit both consumers and firms.

Keywords: switching intentions; privacy settings; creepiness; privacy concerns

INTRODUCTION

Imagine you are at work, and your mobile phone suddenly displays this notification from an app you recently downloaded: “*If you don’t leave your location in the next 10 minutes, due to traffic, you will not arrive home at your usual time.*” You may immediately wonder: How does this app know where my home is? When did I agree to share this information? What else is it monitoring? This situation is not uncommon. Many apps request consent to use data when downloaded, yet consumers are often unaware of what is being shared and how it is being used (Berreby 2017).

Extensive marketing research has studied the factors that influence or deter individuals from disclosing personal data. However, the literature lacks evidence on what happens after the decision to disclose personal data has been made (Pizzi and Scarpi 2020). Further, while the intention to switch privacy settings has received scholarly attention (Antón et al. 2007; Wirtz et al. 2014; Yu et al. 2022), these studies typically consider switching as the termination of a relationship. In contrast, we examine switching intentions as an adjustment to the terms and conditions of the existing relationship with the service provider.

After receiving unpredictable notifications like the one previously described, consumers may feel unsettled, uncertain about potential risks, and lacking control over their data. In other words, they may feel *creeped out* by the app (Langer and König 2018). While scholars often discuss the feeling of creepiness in relation to technology (e.g., the uncanny valley; Kim, de Visser, and Phillips 2022), scant marketing research has empirically studied the consequences of this feeling. Following existing work (Langer and König 2018; Rajaobelina et al. 2021), we define creepiness as the feeling of discomfort or unease that arises when an object (e.g., an individual, a situation, a technology) feels unpredictable. Our research specifically examines the feeling of creepiness elicited by digital service providers (e.g., mobile apps) and explores whether it leads consumers to adjust their previously agreed-upon privacy settings, thereby limiting the disclosure of their personal data to marketers.

To explain the relationship between creepiness and switching intentions, we build on the literature on privacy reclamation (Martin and Murphy 2017; Okasaki et al. 2020; Pizzi and Scarpi 2020) and propose that, as consumers feel increasingly creeped out by the service provider, they become more concerned about their privacy, ultimately leading them to change their privacy settings.

We test our theorizing in a preregistered lab experiment. Our findings offer both theoretical and practical contributions. First, we add to the marketing literature by shedding new lights on the feeling of creepiness. Second, in contrast with existing work, we study switching intentions as an adjustment in the relationship with a service provider (i.e., which data to share with them) rather than the termination of such relationship. Third, we offer new insights by identifying privacy concerns as the underlying process driving consumer switching intentions, even when accounting for an alternative explanation (i.e., privacy violation expectations). Finally, our results may provide managerial insights that benefit both consumers and service providers.

CONCEPTUAL DEVELOPMENT

Creepiness and Switching Intentions

We consider switching intentions as *consumers' willingness to change privacy settings in a mobile application* ("app," hereafter). Said another way, we are interested in investigating why and when consumers who initially allowed an app to use their personal data decide to switch privacy settings to disclose less data. Prior research in the domain of privacy concerns has mainly investigated switching intentions as the willingness to switch service providers—e.g., hotels (Yu et al. 2022), social network sites (Hwang, Shim, and Park 2019), e-commerce live streaming platforms (Ye et al. 2022). However, what drives consumers to modify the terms and conditions of their relationship with a service provider, rather than switching providers entirely, remains underexplored in the marketing literature, despite its important implications for businesses that may face a loss of valuable data to fuel their personalization algorithms. Thus, we wonder: What could drive consumers to change the privacy settings of a mobile app?

To answer this question, we turn to the literature on creepiness (Langer and König 2018; McAndrew and Koehnke 2016; Rajaobelina et al. 2021). Creepiness is a relatively unexplored research topic. Recent works in psychology identify two dimensions of this construct: "emotional creepiness" and "creepy ambiguity" (Rajaobelina et al. 2021). The former refers to "a rather unpleasant affective impression elicited by unpredictable people, situations, or technologies," while the latter refers to "a lack of clarity on how to act and how to judge in such situations" (Langer and König 2018; p. 3). In the present research, we are particularly interested in emotional creepiness (but we refer to it simply as "creepiness").

While there is no clear consensus in the existing literature on the specific causes and effects of creepiness (e.g., Leander et al. 2012; Langer and König 2018; Rajaobelina et al. 2021), it is generally recognized as an unpleasant and confusing sensation that frequently occurs in everyday life (McAndrew and Koehnke 2016). Various factors can trigger different levels of creepiness, including nonverbal cues such as behavioral mimicry (Leander et al. 2012), personal traits like age (Brink et al. 2019), and situational elements such as uncertainty (Langer and König 2018). Regarding the latter, creepiness often emerges from the perceived risk associated with ambiguous situations that are difficult to assess (Langer and König 2018; McAndrew and Koehnke 2016). This ambiguity may stem from uncertainty about the nature of the threat or its likelihood, leaving individuals feeling powerless in the face of the situation (Rajaobelina et al. 2021). Existing research investigated creepiness in relation to perceptions of strangers' actions (McAndrew and Koehnke 2016), human-like robots (e.g., the uncanny valley; Kim, de Visser, and Phillips 2022), and AI-based technologies mimicking human behaviors (Davenport et al. 2020). However, this stream of research is more associated with the concept of eeriness (Langer and König 2018), which is out of the scope of our paper.

Some studies suggest that individuals may feel creeped out when their activities are being monitored by others (McAndrew and Koehnke 2016). In the realm

of technology, data collection can be perceived as unsettling because it involves tracking individuals' activities (Tene and Polonetsky 2015). This discomfort stems from the perception that technology has agency, autonomously collecting data and providing feedback based on its analyses, which can make users feel both uneasy and threatened (Rajaobelina et al. 2021).

Heightened creepiness can increase negative feelings, arousal, and focused attention (McAndrew and Koehnke 2016; Rajaobelina et al. 2021), preparing the body to react or escape. But what *actions* might consumers take when confronted with the feeling of creepiness? Drawing on existing research, we propose that, once consumers experience feelings of creepiness due to unexpected behavior by a service provider, they should be more motivated to change the terms and conditions of their relationship with the service provider. In particular, the feeling of creepiness elicited by an app may drive consumers to change its privacy settings because this emotion signals a sense of unease and potential threat. When users perceive that the app is monitoring their behavior in unexpected or intrusive ways, it should trigger a feeling that their personal information may be at risk. This sense of vulnerability may make them more likely to take protective actions, such as adjusting privacy settings.

Therefore, we suggest that, in the situation where consumers have accepted an app's terms and conditions, they should be increasingly more willing to switch privacy settings when they perceive the app to be more creepiness. Formally:

H1: *As the level of perceived creepiness increases, consumers will be more willing to switch privacy settings.*

The Mediating Role of Privacy Concerns

We predict that an increased feeling of creepiness elicited by an app will heighten consumers' willingness to change its privacy settings. But why may this happen? We propose that when an app is perceived as highly creepy, consumers become more concerned about their privacy, ultimately switching the privacy settings. As previously noted, creepiness raises consumer concerns. In the context of data collection by technologies such as apps, these concerns should be primarily centered around privacy. The literature offers various definitions and conceptualizations of privacy concerns (Taylor, Ferguson, and Ellen 2015). Some studies view privacy concerns as a personality trait, while others treat this variable as situational. In our research, we approach privacy concerns elicited by situational factors.

Privacy concerns play a crucial role in the decision-making process regarding the sharing of personal information with technology (Martin and Murphy 2017; Pizzi and Scarpi 2020). They are often linked to the perceived level of control over shared data or uncertainty about how the technology manages that data (Okasaki et al. 2020). Relatedly, prior research has shown that privacy concerns decrease individuals' willingness to share personal information (Aiello et al. 2020; Martin and Palmatier 2020).

Building on previous research and the definitions of the creepiness construct, we suggest that privacy concerns should increase as a consequence of heightened

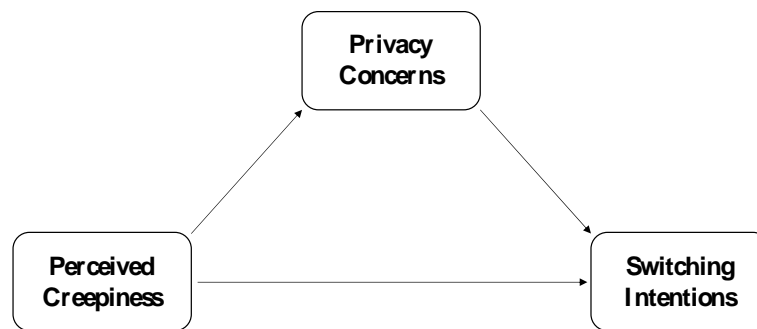
perceived creepiness because creepiness signals a feeling of uncertainty and threat that should be related to the fear of being observed or manipulated without consent. When consumers perceive something as creepy, they sense a potential violation of boundaries or an unexpected use of their personal information. This emotional response might raise alarms about privacy, prompting concerns about how their data is being collected, used, or shared. Consequently, consumers might become more protective of their personal information and wary of potential privacy violations, thus switching the privacy settings of the technology collecting their data (e.g., an app).

Hence, we expect privacy concerns to be intensified when consumers experience heightened creepiness toward the service provider, ultimately driving them to switch privacy settings. Formally:

H2: *Privacy concerns mediate the relationship between perceived creepiness and switching intentions.*

Figure 1 summarizes our proposed conceptual model.

Figure 1. Full conceptual model



EMPIRICAL STUDY

Study 1

The goal of Study 1 is twofold: First, we aim to find support for our proposed conceptual model. Specifically, we test the chain of effects triggered by creepiness on consumers' intention to switch privacy settings through privacy concern. Second, we control for a variable that may represent an alternative explanation for the proposed effects—i.e., privacy violation experiences. In this way, we rule out the possibility that the observed effects are due to individuals' idiosyncratic prior experiences.

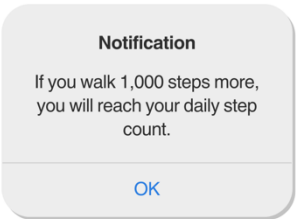
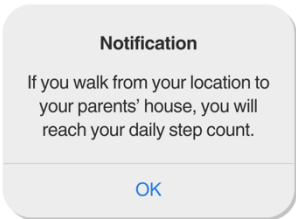
Study 1 was preregistered: https://aspredicted.org/PVD_WFN.

Method

Participants and Design. We collected a sample of 201 U.K. participants on Prolific. One participant failed the attention check included at the end of the survey. The final sample includes 200 participants ($M_{\text{age}} = 38.39$, $SD = 12.11$; 56.5% female). We randomly assigned participants to two experimental conditions in a single factor (creepiness: low, high) between-subject design.

Stimuli and Procedure. We asked participants to imagine themselves receiving an unexpected notification on their smartphone from an app they recently downloaded. In the low creepiness condition, the notification read: “*If you walk 1,000 steps more, you will reach your daily step count.*” In the high creepiness condition, the notification read: “*If you walk from your location to your parents’ house, you will reach your daily step count.*” Figure 2 shows the full experimental stimuli.

Figure 2. Experimental Stimuli (Study 1)

Low Creepiness	High Creepiness
	

Measures. After reading one of the two notifications, participants rated how much they perceived the notification to be creepy on a 5-item Likert scale (e.g., “When being shown the notification, I had a queasy feeling;” 1 = strongly disagree, 7 = strongly agree; adapted from Langer and König 2018; $\alpha = .95$), expressed their intentions to switch privacy settings of the app on a 3-item bipolar scale (i.e., “unlikely/likely,” “unprobable/probable,” and “no chance/certain;” adapted from Bansal and Taylor 2002; $\alpha = .97$), and indicated their privacy concerns on a 3-item Likert scale (e.g., “I would not be concerned about my privacy when I use the app;” 1 = strongly disagree, 7 = strongly agree; adapted from Cowan, Javornik and Jiang 2021; $\alpha = .78$). Next, we measured participants’ privacy violation expectations on a 3-item Likert scale (e.g., “I have had bad experiences with regard to my online privacy before;” 1 = strongly disagree, 7 = strongly agree; adapted from Zeissig et al. 2017; $\alpha = .67$). Finally, participants answered an attention check (i.e., “What was the notification about? (a) daily steps, (2) traffic, (3) bank account password, (4) hours of sleep) and some demographic questions.

Results

Manipulation Checks. A one-way ANOVA with perceived creepiness as the dependent variable revealed that participants in the low perceived creepiness condition perceived the notification as less creepy than participants in the high perceived creepiness condition ($M_{\text{low}} = 2.64$, $SD = 1.47$ vs. $M_{\text{high}} = 3.91$, $SD = 1.88$; $F(1, 198) = 28.21$, $p < .001$, $\eta^2 = .125$). Results are consistent when controlling for privacy violation expectations. Tables 1-2 illustrate the results.

Switching Intentions. Further, a one-way ANOVA with switching intentions as the dependent variable showed that participants in the low perceived creepiness condition were less intentioned to switch privacy settings than participants in the high perceived creepiness condition ($M_{\text{low}} = 4.60$, $SD = 2.02$ vs. $M_{\text{high}} = 5.33$, $SD = 1.82$; $F(1, 198) = 7.19$, $p = .008$, $\eta^2 = .035$). Results are consistent when controlling for privacy violation expectations. Tables 1-2 illustrate the results.

Privacy Concerns. Finally, a one-way ANOVA with privacy concerns as the dependent variable indicated that participants in the low perceived creepiness condition were more concerned in relation to privacy than participants in the high perceived creepiness condition ($M_{\text{low}} = 4.61$, $SD = 1.38$ vs. $M_{\text{high}} = 5.02$, $SD = 1.44$; $F(1, 198) = 4.14$, $p = .043$, $\eta^2 = .020$). Results are consistent when controlling for privacy violation expectations. Tables 1 and 2 illustrate the results.

Table 1. Main Effects

DV	Pairwise Comparison	Main Effect
Manipulation Check	$M_{\text{low}} = 2.64$ vs. $M_{\text{high}} = 3.91$	$F(1, 198) = 28.21$, $p < .001$, $\eta^2 = .125$
Privacy Concerns	$M_{\text{low}} = 4.61$ vs. $M_{\text{high}} = 5.02$	$F(1, 198) = 4.14$, $p = .043$, $\eta^2 = .020$
Switching Intentions	$M_{\text{low}} = 4.60$ vs. $M_{\text{high}} = 5.33$	$F(1, 198) = 7.19$, $p = .008$, $\eta^2 = .035$

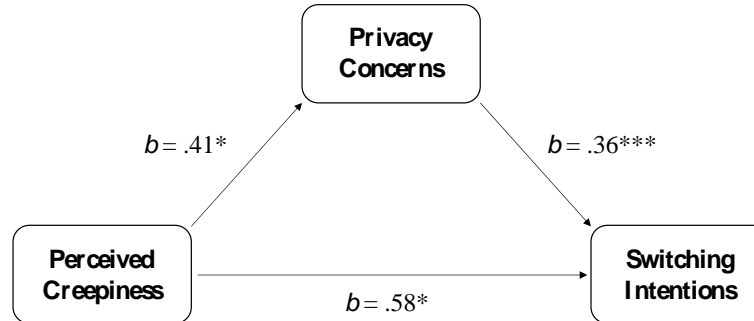
Table 2. Main Effects, Controlling for Privacy Violation Expectations

DV	Pairwise Comparison	Main Effect
Manipulation Check	$M_{\text{low}} = 2.62$ vs. $M_{\text{high}} = 3.93$	$F(1, 197) = 32.97, p < .001, \eta^2 = .148$
Privacy Concerns	$M_{\text{low}} = 4.60$ vs. $M_{\text{high}} = 5.03$	$F(1, 197) = 4.17, p = .032, \eta^2 = .023$
Switching Intentions	$M_{\text{low}} = 4.59$ vs. $M_{\text{high}} = 5.34$	$F(1, 197) = 6.18, p = .006, \eta^2 = .038$

Mediation. To test the mediation by privacy concerns as the underlying mechanism of the effects of perceived creepiness on switching intentions, we conducted mediation analysis using model 4 of the PROCESS macro (Hayes 2013) with 10,000 bootstrap samples. The model included perceived creepiness as the independent variable, privacy concerns as the mediator, and switching intentions as the dependent variable. We found that a notification perceived as creepier drove higher privacy concerns ($b = .41, SE = .20, t = 2.03, p = .043$), which increased participants' switching intentions privacy settings ($b = .36, SE = .27, t = 3.86, p < .001$). The resulting 95% CI indicated significant indirect effect of perceived creepiness on switching intentions through privacy concerns ($b = .15, SE = .09, 95\% CI = [.00, .35]$; Figure 3). Results are consistent when including privacy violation expectations as a covariate.

Figure 3. Mediation Analysis Results

Indirect Effect: $b = .15, SE = .09, 95\% CI = [.00, .35]$



GENERAL DISCUSSION

What happens when consumers accept the terms and conditions of an app without fully understanding what they have agreed to? In the present research, we aim to explore this research question. Specifically, we investigated the role of creepiness in affecting consumers' intentions to change the privacy settings of a service provider (i.e., a mobile app). We hypothesized and found that the more consumers are creeped out by an unexpected notification from an app, the more likely they are to intend to

switch their privacy settings. This effect appears to be driven by heightened privacy concerns, even when accounting for consumers' expectations of privacy violations.

To follow, we highlight the theoretical and practical contributions of our work and identify limitations that could spur future research.

Theoretical and Practical Implications

The findings from Study 1 offer both theoretical and practical contributions. First, we advance the existing literature by shedding new light on the feeling of creepiness. While previous research has acknowledged the potential relevance of creepiness in consumer responses to technology, scant research has empirically investigated its role in consumer behavior. Not only our study extends prior work by demonstrating that creepiness can trigger consumer concerns (e.g., McAndrew and Koehnke 2016; Rajaobelina et al. 2021), but it also finds that creepiness can impact switching intentions, a previously unexplored behavioral outcome.

Second, unlike existing research that typically examines switching intentions as a decision to change service providers (Hwang, Shim, and Park 2019; Ye et al. 2022; Yu et al. 2022), we focus on switching intentions as adjustments to the terms of the relationship with a service provider. This perspective has been less explored and provides new insights into why consumers might alter the terms of their relationship rather than switching providers entirely.

Third, we identify privacy concerns as a key factor driving consumer switching intentions, even when considering alternative explanations, such as privacy violation expectations. Our study adds to the existing literature by showing that creepiness can heighten privacy concerns (McAndrew and Koehnke, 2016) and, for the first time (to our knowledge), reveals that these privacy concerns can influence behavioral responses like switching intentions.

Finally, our results offer valuable managerial insights for both consumers and service providers. On one hand, consumers are becoming increasingly aware of the need to protect their privacy, yet they often overlook or misunderstand the terms and conditions governing their relationship with service providers (Berreby, 2017). Thus, addressing the factors that drive consumer switching intentions (e.g., creepiness, privacy concerns) could help companies to create more transparent and respectful data handling processes. On the other hand, companies depend heavily on user data to power their personalization algorithms and enhance user experiences. When consumers switch privacy settings to restrict data sharing, companies risk losing access to critical information that drives personalized services. Overall, investigating the factors that drive switching intentions is crucial for companies to respect privacy while maintaining the flow of data needed for personalization.

Limitations and Further Research

The results of Study 1 should be considered in light of different limitations, which present opportunities for future research. First, although our findings align with the proposed conceptual model, we cannot generalize them to other apps or service

providers. Apps and service providers may differ in how self-relevant or helpful they are perceived by consumers. For instance, an app providing bank account-related information might be seen as significantly more self-relevant than one tracking daily step counts. In such cases, the impact of an intrusive notification could vary, leading to different behavioral responses. Future research could investigate the self-relevance of the data being shared or the app's perceived helpfulness as potential moderators of these effects.

Second, while we measured switching intentions following prior research, we did not ask participants to actually change the settings. Apps may differ in how easy it is for users to modify privacy settings, and switching intentions could decrease if consumers encounter difficulty accessing these settings. Future research could explore how the motivation to switch privacy settings varies based on the ease of accessing and adjusting those settings.

REFERENCES

- Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V., and Viglia, G. (2020). Customers' willingness to disclose personal information throughout the customer purchase journey in retailing: The role of perceived warmth. *Journal of Retailing*, 96(4), 490-506.
- Antón, C., Camarero, C., and Carrero, M. (2007). The mediating effect of satisfaction on consumers' switching intention. *Psychology and Marketing* 24(6), 511-538.
- Bansal, H. S., and Taylor, S. F. (2002). Investigating interactive effects in the theory of planned behavior in a service-provider switching context. *Psychology and Marketing*, 19(5), 407-425.
- Berreby (2017). Click to agree with what? No one reads terms of service, studies confirm. Retrieved March 3, 2017, <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>
- Brink, K. A., Gray, K., and Wellman, H. M. (2019). Creepiness creeps in: Uncanny valley feelings are acquired in childhood. *Child Development*, 90(4), 1202-1214.
- Cowan, K., Javornik, A., and Jiang, P. (2021). Privacy concerns when using augmented reality face filters? Explaining why and when use avoidance occurs. *Psychology and Marketing*, 38(10), 1799-1813.
- Hwang, H. S., Shim, J. W., and Park, S. B. (2019). Why we migrate in the virtual world: factors affecting switching intentions in SNS. *Information, Communication and Society* 22(14) 2127-2137.
- Langer, M., and König, C. J. (2018). Introducing and testing the creepiness of situation scale (CRoSS). *Frontiers in Psychology*, 9 2220.
- Leander, N. P., Chartrand, T. L., and Bargh, J. A. (2012). You give me the chills: Embodied reactions to inappropriate amounts of behavioral mimicry. *Psychological Science* 23(7), 772-779.

- Martin, K. D. and Palmatier, R. (2020). Data Privacy In Retail: Navigating Tensions And Directing Future Research. *Journal of Retailing*, 96(4), 449-457.
- Martin, K. D., and Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135-155.
- McAndrew, F. T., and Koehnke, S. S. (2016). On the nature of creepiness. *New Ideas in Psychology*, 43, 10-15.
- Okasaki, S., Eisend, M., Plangger, K., Ruyter, K. and Grewal, D. (2020). Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review. *Journal of Retailing*, 96, 458-473.
- Pizzi, G., and Scarpi, D. (2020). Privacy threats with retail technologies: A consumer perspective. *Journal of Retailing and Consumer Services*, 56, 102160.
- Rajaobelina, L., Prom Tep, S., Arcand, M., and Ricard, L. (2021). Creepiness: Its antecedents and impact on loyalty when interacting with a chatbot. *Psychology and Marketing*, 38(12) 2339-2356.
- Schnittka, O., Himme, A., Papies, D., and Pellenwessel, D. (2017). Are sponsors blamed for edging off? Consumer reactions to sponsorship terminations. *Journal of Business Economics*, 87, 943-984.
- Tene, O., and Polonetsky, J. (2015). A theory of creepy: technology, privacy, and shifting social norms. *Yale J. Law Technol*, 16, 59-102.
- Wirtz, J., Xiao, P., Chiang, J., and Malhotra, N. (2014). Contrasting the drivers of switching intent and switching behavior in contractual service settings. *Journal of Retailing*, 90(4), 463-480.
- Ye, D., Liu, F., Cho, D., and Jia, Z. (2022). Investigating switching intention of e-commerce live streaming users. *Heliyon*, 8(10).
- Yu, J., Moon, H., Chua, B. L., and Han, H. (2022). Hotel data privacy: strategies to reduce customers' emotional violations, privacy concerns, and switching intention. *Journal of Travel and Tourism Marketing*, 39(2) 215-227.
- Zeissig, E. M., Lidynia, C., Vervier, L., Gadeib, A., and Ziefle, M. (2017). Online privacy perceptions of older adults. In Human Aspects of IT for the Aged Population. Applications, Services and Contexts: Third International Conference, ITAP 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part II 3 (pp. 181-200). Springer International Publishing.