International Journal of Cyber Research and Education
Volume 3 • Issue 1 • January-June 2021

Privacy Concern and Likelihood of Paying a Privacy Fee

Daniel M. Eveleth, University of Idaho, USA
Lori Baker-Eveleth, University of Idaho, USA
Norman M. Pendegraft, University of Idaho, USA
Mark M. Rounds, University of Idaho, USA

ABSTRACT

This research examined the extent to which social-media users' privacy concerns affected the likelihood that they would pay a fee in exchange for a social-media company promising not to use or sell that user's data. Data to empirically test the theoretical model were collected by administering a survey to social-media users. The sample consisted of 173 usable responses. The results of the analyses, including the structural model show that users' knowledge of privacy issues, personal experience with invasions of privacy, and their levels of risk intolerance, influenced the likelihood that they would pay a privacy fee, indirectly, through their concern for privacy. Furthermore, concern for privacy had a significant, positive effect on the magnitude of an expected privacy fee.

KEYWORDS

Online Privacy, Privacy Behaviors, Privacy Fee, Risk Intolerance, Social Networking Services (SNS)

INTRODUCTION

A recent Pew Research report stated that the number of Americans who use some form of social media has risen from 5% in 2005 to nearly 70% in 2018, and over that time users have become increasingly "anxious about all the personal information that is collected and shared and the security of their data" (Rainie, 2018). In addition to calls for legislation requiring companies to provide opt-out options, disclose how they are protecting and using personal information, and notify users of data breaches, some have pushed for the use of financial incentives; either compensating users for their personal information or giving users the option to pay a fee in exchange for not using or selling their information (Piovesan, 2019). However, in a recent interview Sheryl Sandberg, Chief Operating Officer of Facebook, noted that while giving users an option to opt out of data sharing by paying a fee is an alternative, the user base was thus far unwilling to pay for this option (Johnson & Ortiz, 2018).

What makes this high-anxiety/low-willingness finding an interesting puzzle is that it is clear that users do assign value to the act of disclosing their private information and to a promise by organizations to protect the individual's private information (Acquisti, John, & Loewenstein, 2013). Unfortunately, there is still little understanding about factors that affect these values or that affect users' willingness to pay for such value. Users' levels of concern for privacy, experience with privacy

DOI: 10.4018/IJCRE.2021010101

invasions, tolerance for risk, and familiarity with privacy issues may be some of those factors. In this manuscript we identify a set of hypothesized relationships between social-media users' willingness to pay an opt-out fee and factors that are likely to affect their willingness, and then describe a study that tested those hypotheses and the study results.

LITERATURE REVIEW

Individuals' concern for privacy, as a meaningful construct of interest, has been widely documented across a wide array of settings, including with respect to such domains as telemarketing and the use of do-not-call-lists (Dommeyer & Gross, 2003), e-commerce sites (Liu, Marchewka, Lu, & Yu, 2005), bricks-and-mortar retailers using RFID tags (Ohkubo, Suzuki, & Kinoshita, 2005), location identification (Katz, 2019), facial recognition technology to track shoppers (Ryski, 2019), travel (Tussyadiah, Li, & Miller, 2019), and activity on social-media sites (Osatuyi, 2015). Across all of these settings, it is clear that organizations need a better understanding of the factors that affect users' concerns because their concerns likely affect their behaviors with respect to the organizations (Hong, Chan, & Thong, 2019); something that has been confirmed by previous research that has investigated the relationship between privacy concern and privacy-related intentions and behaviors (Jahangir & Begum, 2007; Kumar, Mohan, & Holowczak, 2008; Li, 2014). However, H. J. Smith, Dinev, and Xu (2011) concluded, from an extensive review of privacy literature, that what is still needed are more empirical studies that "focus on antecedents to privacy concerns and on actual outcome" (p. 989).

A number of outcomes have been investigated since the call by Smith, Dinev and Xu (2011); including willingness to disclose information (Bansal, Zahedi, & Gefen, 2016; Keith, Thompson, Hale, Lowry, & Greer, 2013; Taddicken, 2014), withdrawal behaviors (Choi, Park, & Jung, 2018; Dienlin & Metzger, 2016), technology-use intentions (Shin, 2010; Wang, Asaad, & Filieri, 2019), purchase behaviors (Fortes & Rita, 2016), and defensive behaviors (Ortiz, Chih & Tsai, 2018). However, there remains a dearth of research investigating the effect of privacy concern on users' willingness to pay a fee to a service provider in exchange for a promise not to share personal information.

While some believe that users see privacy as a right (Floridi, 2005), others suggest that users view privacy as an asset that has economic value (Walsh, Parisi, & Passerini, 2017). Discussions about the 'privacy paradox' (Kokolakis, 2017; Taddicken, 2014); (Gerber, Gerber, & Volkamer, 2018), often center on instances when users report a high level of concern for privacy but also display a willingness to disclose information. The assumption is that users perform a risk-reward calculation of the potential costs of sharing information relative to the potential benefits of doing so. This suggests that users treat their information as a resource that can be exchanged for valued benefits; or as a resource that they may be willing to protect in exchange for a fee.

Laufer and Wolfe (1977) postulated that individuals' concepts of privacy are affected by their experiences; and they described those experiences in terms of three dimensions: self-ego, environmental, and interpersonal. Hong et al. (2019) recently applied Laufer and Wolfe's model to concerns for privacy in the online setting and concluded that three 'self-ego' or individual factors that have some effect on users' concerns for privacy are users' knowledge or familiarity with privacy issues, their experience with privacy invasion, and their risk intolerance.

Knowledge of privacy issues has consistently been shown to affect privacy concerns; however, the nature of that effect has varied across studies. For example, a number of early studies of Internet privacy concerns found a negative relationship between knowledge and concern (Harris, Hoye, & Lievens, 2003; Miyazaki & Fernandez, 2001). The assumption was that users with greater knowledge "are more skillful at protecting their online privacy" (Hong, Chan, & Thong, 2019, p. 6), and thus, less concerned. However, given the significant increase in the connectedness of users' lives and the obvious increase in the amount of data that is collected and shared, it is likely that the more