



An empirical investigation of privacy breach perceptions among smartphone application users



Stanislav Mamonov^{a,*}, Raquel Benbunan-Fich^{b,1}

^a Montclair State University, IOM Department, School of Business, 1 Normal Ave, Montclair, NJ 07043, United States

^b Baruch College, CUNY, Statistics & CIS Department, Zicklin School of Business, One Bernard Baruch Way, Box B11-220, New York, NY 10010, United States

ARTICLE INFO

Article history:

Available online 28 March 2015

Keywords:

Privacy
Perceived privacy breach
Mobile applications
Psychological contract theory

ABSTRACT

This study examines four factors affecting perceptions of privacy breach among smartphone application users. The four factors drawn from psychological contract theory are: the type of information perceived to be misappropriated by the application, the presence of a legal agreement giving application developers rights to use the information, the source of information suggesting that a privacy breach may have occurred and the application type (free or paid). An experimental examination of these factors indicates that perceptions of misappropriation of financial information are more distressing than perceived misappropriation of geo-location data. In addition, the existence of legal contracts giving application developers rights to information only partially attenuates perceptions of privacy breach among application users. This study offers a novel theoretical perspective toward understanding perceptions of privacy breaches and it shows that privacy breach perceptions vary according to the characteristics of the breach. At the methodological level, this study offers a new focal construct to measure perceived privacy breach. At a practical level, the empirical results highlight the limitations of legal contracts in preventing perceptions of privacy breach.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

In recent years, the pervasive use of technology in all spheres of human activity along with the ease of collecting and potentially misusing personal information have heightened privacy concerns. As a result, there are a number of recent studies examining different aspects of privacy including integration frameworks (Floridi, 2005; Li, 2012) as well as empirical studies (Baek, 2014; Kisekka, Bagchi-Sen, & Raghav Rao, 2013). The opportunities to provide and misuse private information are amplified when mobile technologies are involved (Moll, Pieschl, & Bromme, 2014; Park & Mo Jang, 2014). The rapid adoption of smartphones is evidenced in recent estimates indicating that smartphone shipments have exceeded deliveries of personal computers and that nearly a billion smartphones were sold worldwide in 2013 (IDC, 2013). This trend is fueled by technological advances in smartphone devices and by the wide availability of mobile applications provided by third-party developers. For example, over 1.2 million applications have been approved for Apple's app store (Sacco, 2015). These apps

allow users to carry out a variety of tasks from their mobile devices including banking and shopping. Not surprisingly, mobile commerce represents an important segment of the U.S. economy and a growing market opportunity (Empson, 2013). While smartphones offer many benefits, they also expose smartphone users to growing privacy risks. In fact, a recent survey found that 70% of smartphone users were concerned about their privacy (TRUSTe, 2013). Although these concerns might be justified, it is important to assess how users perceive specific privacy breaches.

Much of prior research in Information Systems has focused on privacy concerns as the focal construct (Li, 2011; Pavlou, 2011; Smith, Dinev, & Xu, 2011). Privacy concerns play an important role at the onset of relationships which potentially compromise participants' privacy. Nevertheless, practice has shown that despite high levels of privacy concerns, people still disclose their own personal information because the perceived benefits of doing so often outweigh perceived risks (Dinev & Hart, 2006; Premazzi et al., 2010). Anecdotal evidence and research on privacy indicate that voluntary private information disclosure is prevalent in modern society (Barnes, 2006).

Personal experiences affect the level of privacy concerns (Laufer & Wolfe, 1977). In particular, a prior exposure to a privacy breach shapes individuals perceptions by making people more cautious about sharing their personal information (Bansal & Gefen, 2010).

* Corresponding author. Tel.: +1 973 655 3512.

E-mail addresses: stanislav.mamonov@montclair.edu (S. Mamonov), rbfich@baruch.cuny.edu (R. Benbunan-Fich).

¹ Tel.: +1 646 312 3375.

A breach occurs after the exchange relationship has been established and personal information (collected or shared) is misused. This is the case in many contexts nowadays. For example, Viber, a smartphone messaging application, attracted over 90 million users within 6 months of application re-launch in July 2012 (Wauters, 2013). Notwithstanding the success of the application, many users thought that the application infringed on their privacy when it was revealed that Viber copied users' address books without giving any notice to the users (James, 2013). Given the variety of technology-mediated instances where personal information is collected and leaked, people may experience different privacy breach incidents. However, little is known about the factors that affect how a privacy breach is perceived. This study seeks to investigate whether specific characteristics of a privacy breach result in different perceptions of severity of the breach. To this end, the construct of perceived privacy breach is defined and examined through different privacy breach scenarios involving smartphone application users.

We draw on psychological contract theory to develop the theoretical foundation for our research model. Psychological contract theory posits that virtually all exchange relationships involve unwritten expectancies that comprise psychological contracts (Rousseau, 2001). Subjective perceptions that one or more expectancies comprising a psychological contract have been broken constitutes a psychological contract breach (Morrison & Robinson, 1997). Morrison and Robinson (1997) developed a process model of psychological contract breach which suggests that a number of factors such as anticipated impact, attribution, salience and type of exchange influence how a psychological contract breach is perceived (Morrison & Robinson, 1997). Privacy-related expectancies are inherent to private information disclosure; therefore a perceived breach of privacy would constitute a breach of psychological contract.

We define perceived privacy breach as a perception that a leak of personal information has occurred. To investigate the factors influencing the perception that privacy has been breached and the severity of the perceived breach, we conduct two complementary experimental studies. The first study examines the effects of the type of information collected by the mobile app (financial versus geo-location), claims of legal rights to information in legal contracts which accompany the applications, and the source of information suggesting that a privacy breach had occurred (a blogger or *Wall Street Journal*). The second study examines type of information and presence of legal claims along with the type of the application (free or paid).

The rest of the paper proceeds as follows. The next section reviews psychological contract theory, and develops the research model and associated hypotheses. The description of the methodology and the results follow. The paper concludes with discussion, limitations, and contributions to theory and practice.

2. Theory background and hypotheses

As a topic of research, privacy has generated interest in different disciplines including law (Solove, 2008) and organizational studies (Culnan, 1999), as well as information systems (Belanger & Crossler, 2011; Pavlou, 2011; Smith et al., 2011). Originally, the legal definition of privacy was established by Warren and Brandeis who defined privacy as “the right to be left alone” (Warren & Brandeis, 1890). Over time, this seemingly straightforward concept has evolved to accommodate a more precise legal definition in statutes and case law (Solove, 2008). This study is focused on information privacy, which is defined as the individual ability to control personal information disclosure to others (Westin, 1967). In lieu of general privacy concerns, this study is

about specific factors affecting perceptions of a privacy breach. These factors are identified from psychological contract theory.

The roots of psychological contract theory can be traced to organizational contexts where researchers found that formal employment contracts had little predictive value in explaining employee performance and turnover intentions (Rousseau, 1989, 1990). To account for the discrepancy, psychological contract theory posits that virtually all exchange relationships involve unwritten expectancies that encompass psychological contracts (Rousseau, 2001). A perceived breach of unwritten expectancies, psychological contract breach, triggers attitudinal and behavioral changes (Rousseau, 2004).

Psychological contracts not only point to the limitations of legal contracts as a governance mechanism, but also provide a practically appropriate perspective to examine exchange relationships across different contexts. In Information Systems, psychological contract theory has been applied to virtual teams, online marketplaces, and outsourcing relations, among others. The results have been consistent despite the variety of contexts. Apparent breach of expectancies among virtual team members had negative consequences on team performance (Piccolli & Ives, 2004). Likewise, apparent psychological contract breach among buyers in online marketplaces increased perceptions of risk and reduced intentions of future transactions (Pavlou & Gefen, 2005). On the positive side, fulfillment of psychological contracts was positively associated with success of outsourcing relationships (Koh, Ang, & Straub, 2004). Psychological contract theory has also been applied in less formal relationship contexts. For example, a study of recommendation system adoption showed that a perceived breach of psychological contract affects users' intentions to follow recommendations (Goyal, Limayem, & Davis, 2012). Together, the findings of these studies underscore the importance of considering psychological contracts in different technology-mediated contexts. As prior research has shown (Goyal et al., 2012), psychological contracts affect technology adoption and use. In the next section, we draw on psychological contract theory to discuss the factors that impact the perceptions of a psychological contract breach among mobile application users.

2.1. Hypotheses development

Private information disclosure enabled by technology is premised on users' expectations of privacy and trust in technology. Since privacy expectations are essential for the individual sense of dignity (Post, 2000), perceptions of privacy breach affect individual sense of control and have negative impact on self-esteem and emotional well-being (Diener, Suh, Lucas, & Smith, 1999). Therefore, we argue that privacy-related expectancies comprise a core domain of psychological contracts associated with technology-enabled information disclosure. In other words, technology users who entrust their personal information expect their privacy to be respected and any perceived breach of privacy will constitute a breach of psychological contract. Accordingly, perceived privacy breach is defined as individual perceptions that privacy-related expectancies have been broken. It is worth noting that a *perceived* breach of privacy may occur even in the absence of an actual privacy breach because it depends on how users interpret the situation. Consequently, in the case of an actual breach it is crucial to investigate how users perceive it.

Psychological contract theory provides the foundation to identify the factors that affect privacy breach perceptions. Morrison and Robinson (1997) proposed a process model of psychological contract breach (Morrison & Robinson, 1997). The model suggests that the following four factors affect perceptions of a breach: (1) the anticipated impact of breach, (2) the attribution of breach to either incongruence regarding the terms of agreement or renegeing by the counterparty, (3) the salience of information suggesting

Download English Version:

<https://daneshyari.com/en/article/350341>

Download Persian Version:

<https://daneshyari.com/article/350341>

[Daneshyari.com](https://daneshyari.com)