Computers in Human Behavior 53 (2015) 344–353

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full Length Article

Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany

Mark Fodor [a,*], Alexander Brem [b]

[a] University of Erlangen-Nuremberg, Germany
[b] University of Southern Denmark, Sønderborg, Denmark

ARTICLE INFO

Article history:
Received 17 March 2015
Revised 24 June 2015
Accepted 26 June 2015
Available online 18 July 2015

Keywords:
Privacy concern
Location-based services
Mobile commerce
Theoretical models
User adoption
Location data

ABSTRACT

Different studies have evaluated the factors that lead to the adoption of new online services in general and particularly for Location-Based Services adoption (LBS), as this is seen as a key application for smartphones. Recently, several security threats and the disclosure of extensive personal data have raised the question, if location data are considered as sensitive data by users. Thus, we use two privacy concern models, namely Concern for Information Privacy (CFIP) and Internet Users' Information Privacy Concerns (IUIPC) to find out. Our sample comprises of 235 individuals between 18 and 34 years (Generation C) from Germany. The results of this study indicate that the second-order factor IUIPC showed better fit for the underlying data than CFIP did. Overall privacy concerns have been found to have an impact on behavioral intentions of users for LBS adoption. Furthermore, other risk dimensions may play a role in determining usage intention, which should be analyzed by further research.

1. Introduction

In the current "4G era" device vendors are expected to generate more value from services than from hardware or applications (Wilson, 2012). Mobile business is growing and enabling new services like mobile payment, mobile banking or mobile recruiting (Yang, Lu, Gupta, Cao, & Zhang, 2012; Shaikh & Karjaluoto, 2015; Böhm & Niklas, 2012). Location-Based Services (LBSs) provide additional value to users by implementing location information (Junglas & Watson, 2008). Friend finder or tracking services are just some of the services already available today. Location data has evolved from a niche segment to the general public. Smartphones offer sophisticated location technology that enables individuals to take advantage of a vast amount of services. With the development of technology, risks regarding private data have increased as location data can now be accessed online. Privacy risks, individuals' cultural backgrounds, and other potential factors may hinder LBS adoption (Wu, Huang, Yen, & Popova, 2012). Chang and Chen (2014) have found that whether people disclose their location is largely influenced by their friends.

The aim of this paper is to compare two models of privacy concerns on user adoption. Data gathered from a survey will be used to compare the models and to evaluate the impact of individuals' concerns for information privacy on their behavioral intention on LBSs usage.

The rest of this paper is structured as follows. A review of relevant literature on privacy concerns and user adoption is given in the next section. Section 3 presents the analyzed research models and proposed hypotheses. The next section presents the data collection and the methodology of the study. Data analysis and results are presented in Section 5. Next, a comparison of the two models is given in Section 5.5. Section 6 summarizes the findings with managerial implications and their limitations.

2. Literature review

The adoption rate of LBSs is below the predicted rate (Junglas & Watson, 2008). Researchers try to find the causes and identify the reasons for this low adoption. Several models exist that try to explain user's behavioral intention to adopt new technologies. Some of the models include the Technology Acceptance Model (TAM) (Davis, Bagozzi, & Warshaw, 1989), the Theory of Planned Behavior (TPB) (Ajzen, 1991), and the Innovation Diffusion Theory (IDT) (Rogers, 1995). Later, Venkatesh, Morris, Davis, and Davis (2003) have introduced the Unified Theory of Acceptance and Use of Technology (UTAUT), which is based on a combination of several models (Koch, Toker, & Brulez, 2011). These models include different factors that influence user adoption. However, less interest has been paid to privacy concerns and their influence

* Corresponding author.
E-mail address: mark.fodor@me.com (M. Fodor).

http://dx.doi.org/10.1016/j.chb.2015.06.048
0747-5632/

on the behavioral intention of users. In information systems literature, particularly the domain of information privacy, there is a "[...] lack of validated instruments for measuring individuals' concerns about organizational information privacy practices" (Smith, Milberg, & Burke, 1996, p. 168). Thus, the authors developed the concern for information privacy (CFIP) framework. It consists of 15-items that provide an instrument to measure privacy concerns (Smith et al., 1996). Junglas and Spitzmüller (2005) have created a research model that incorporates CFIP and technology characteristics, task characteristics, and personality. Zhou (2011) used the CFIP model to assess the impact of privacy concerns on user adoption of LBSs. The findings show that the four dimensions of CFIP, that are collection, errors, improper access, and secondary use, have an influence on trust and perceived risk (Malhotra, Kim, & Agarwal, 2004; Zhou, 2011). Both of which have been shown to determine usage intention. Stewart and Segars (2002) found that users' information privacy concerns are more complex. The findings show support for a second-order factor CFIP and that consumers are concerned about all four dimensions of CFIP and not particularly concerned about one specific dimension.

Malhotra et al. (2004) have proposed the construct of Internet Users' Information Privacy Concerns (IUIPC) which consists of three dimensions: collection, control, and awareness. They argue that CFIP was intended for an offline context, and that privacy concerns of Internet users and offline users are probably not alike. IUIPC was found to be "[...] a useful tool for analyzing online consumers' privacy concerns and reactions to various privacy threats on the internet" (Malhotra et al., 2004, p. 338).

Liu, Marchewka, Lu, and Yu (2004) have taken a different approach on privacy concerns. A model was developed that included privacy and its relationship to behavioral intention while using trust as a moderator. The privacy dimensions were adapted from the US Federal Trade Commission which proposed fair information practices. The privacy construct consists of four dimensions: notice, access, choice, and security.

3. Research model and hypotheses

The construct of privacy concern is multi-dimensional. CFIP includes four dimensions: improper access, errors, secondary use, and collection (Smith et al., 1996; Stewart & Segars, 2002). IUIPC consists of three dimensions: collection, awareness, and control (Malhotra et al., 2004). It is not the intention to draw causal inferences from the findings, since correlation does not imply causation.

Improper access reflects the concern of users that their private data may be accessed by employees that should not have access. Company policy on handling private data regulates access rights for employees. Technically, assigning access rights should not pose any problem, although privacy policies vary among companies. Errors reflect concern by individuals that companies do not take enough measures to remove errors from personal data. The question also remains how companies deal with errors. Whether manually or automatically through software, which may discourage some individuals who believe to be at the mercy of a machine. Unauthorized secondary use internally and externally is a concern for customers. Internal secondary use happens when a company is collecting information for one purpose but uses that information for another purpose. External secondary use happens when a company provides personal information to a third party. Collection represents the concern of consumers that too much information is collected. Individuals might feel that they provide more value through their private data than they receive by using the service.

Junglas and Spitzmüller (2006) have found that privacy concerns have an influence on perceived risk. Thus, users' concerns on improper access, errors, secondary use, and collection will increase perceived risk. Users may worry that their private data is provided to unauthorized third parties or fear opportunistic behavior by companies that collect too much information. Consequently, the following hypotheses are proposed:

H1	CFIP will have a positive effect on perceived risk.
H1.1	User concern on improper access will have a positive effect on perceived risk.
H1.2	User concern on errors will have a positive effect on perceived risk.
H1.3	User concern on secondary use will have a positive effect on perceived risk.
H1.4	User concern on collection will have a positive effect on perceived risk.

Trust, is the belief of one party that the other party will fulfill its transactional obligations (Suh & Han, 2003). Essentially, it is a "[...] willingness to be vulnerable [...]" (Kim, Ferrin, & Rao, 2008, p. 545) by individuals, as they have to trust the company to behave with his/her best intentions in mind. Trust in a company will decrease with increasing user concern for information privacy. Thus:

H2	CFIP will have a negative effect on trust.
H2.1	User concern on improper access will have a negative effect on trust.
H2.2	User concern on errors will have a negative effect on trust.
H2.3	User concern on secondary use will have a negative effect on trust.
H2.4	User concern on collection will have a negative effect on trust.

Control over private information reflects the existence of voice, i.e., approval or opting-out (Malhotra et al., 2004). Caudill and Murphy (2000) have found that individuals are not primarily concerned about data collection in general, but about whether companies are open about their practices on data collection or not. When a company has the possibility of opportunistic behavior, by taking advantage of private data, individuals are particularly concerned with the issue of control. Awareness of privacy practices is, in contrast to control, a passive dimension of privacy. This is also reflected in the definition that awareness of privacy practices is "the degree to which a consumer is concerned about his/her awareness of organizational information privacy practices" (Malhotra et al., 2004, p. 339). Generally, procedures are perceived to be fair as long as customers are aware (Culnan, 1995).

IUIPC, and its three dimensions, will have an effect on trust and perceived risk. Increased privacy concerns will increase perceived risk for individuals and also reduce trust. Individuals who do not feel that they have control over their private data will have less trust in the service and higher risk perception. When an LBS offers no way for a user to remove his/her information, individuals will doubt the trustworthiness of the service. Thus, the following hypotheses are proposed:

H3	IUIPC will have a negative effect on trust.
H4	IUIPC will have a positive effect on perceived risk.

Trust is interwoven with risk. Some level of risk must be present for trust to be effective (Doney & Cannon, 1997). When individuals have trust in a service, their perceived risk associated with the usage of the service decreases. Gefen (2000) has found that trust