Telematics and Informatics xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Telematics and Informatics

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

Websites, data types and information privacy concerns: A contingency model

Jih-Hsin Tang *, Yi-Jen Lin

National Taipei University of Business, No. 321, Sec.1, Chi-Nan Rd., Taipei, Taiwan, Republic of China

ARTICLE INFO

Article history:
Received 28 October 2016
Accepted 25 May 2017
Available online xxxx

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

Although the growth of e-business over the past years, the online users' privacy concerns is a critical inhibitor of e-business. The owners of e-businesses have to collect consumers' information in order to provide "personalized" service; however, some consumers feel their privacy is threatened (Culnan and Armstrong, 1999; Dinev and Hart, 2005). Consumers show even higher privacy concerns on the big data environment (Shin and Choi, 2015) and on the location-based service of e-business (Aloudat et al., 2013).

Users are motivated to conduct online activities such as to collect information, to make friends, to purchase goods/services or to play online games. Some online activities require users to register in order to provide services. For example, users are required to provide customers' basic information in order to complete a transaction; sometimes, users are requested to fill in more personal information such as personal interests and hobbies in order to acquire personalized services. Previous scholars have contributed in designing a scale for information privacy concerns (Smith et al., 1996; Stewart and Segars, 2002), or in the relationship between privacy and online transactions (Dinev and Hart, 2005), or extend calculus privacy model (Dinev and Hart, 2006).

Recently, the popularity of social-networking sites such as Myspace or Facebook makes online users' privacy concerns a hot topic (Dwyer et al., 2007; Hoadley et al., 2009). But our questions are: do the users have the same privacy concerns over the different Websites? And, whether the individuals show different privacy concerns on required data types and optional data types? This study attempts to investigate the relationship between Website types, data types and online consumers' privacy concerns, and develop and validate a contingency model accordingly. The results may be of theoretical and practical importance because the literature is still scant in describing the relationship between Websites, data type and information privacy concerns.

2. Literature review

Information privacy has long been considered a critical ethical issue in the information age (Mason, 1986). Anecdotes of personal information leaks have covered the daily headline news and frightened some online users. Zuckerberg, the founder of Facebook, said in an award "privacy was no longer a social norm" (Johnson, 2010). The young CEO's remarks make infor-

* Corresponding author.
E-mail addresses: jefftang@ntub.edu.tw (J.-H. Tang), jen_lin074@hotmail.com (Y.-J. Lin).

http://dx.doi.org/10.1016/j.tele.2017.05.012
0736-5853/© 2017 Elsevier Ltd. All rights reserved.

Please cite this article in press as: Tang, J.-H., Lin, Y.-J. Websites, data types and information privacy concerns: A contingency model. Telemat. Informat. (2017), http://dx.doi.org/10.1016/j.tele.2017.05.012

mation privacy another hot-debated topic. Trust and privacy were compared in different social-networking sites (Dwyer et al., 2007), and some authors considered that information privacy is just an illusion(Hoadley et al., 2009).

Information privacy is usually defined an "individual's control of personal information and use"(Westin, 1967; Stone and Stone, 1990). With the advance of internet technology, an individual may find out the control and use of personal information over the Internet challenged.

2.1. Concerns for information privacy

Concern for Information privacy is a complex construct and many researchers attempted to clarify this concept in the IS literature (Culnan and Armstrong, 1999; Hann et al., 2007; Smith et al., 1996; Stewart and Segars, 2002). Smith et al. (1996) developed and validated an instrument, concern for information privacy (CFIP) that identifies and measures the major dimensions of individuals' concern about organizational information privacy practices. And they suggest that individuals with a high concern for information privacy perceive that: (1) too much data are collected, (2) much of the data is inaccurate, (3) corporations use personal information for undisclosed purposes, and (4) corporations fail to protect access to personal information. CFIP has been examined (Stewart and Segars, 2002) and applied to ease individual's privacy concerns (Hann et al., 2007), and how it may affect individual's intention of transaction online (Van Slyke et al., 2006).

The efforts of developing a valid scale for information privacy have been relentless. For instance, Culnan and Armstrong (1999) suggested a concept of "privacy calculus" and argued that individuals will disclose personal information if they perceive that the overall benefits of disclosure are at least balanced by, if not greater than, the assessed risk of disclosure, thus equaling a cost-benefit analysis with privacy calculus(Culnan and Bies, 2003). Dinev and Hart (2006) extended and validated the concept of privacy calculus to e-commerce settings and claimed that the cumulative influence of trust and personal Internet interest are important factors that can outweigh privacy risk perceptions in the decision to disclose personal information online. Malhotra et al. (2004) developed an Internet version of information privacy scale consisting of collection, control, and awareness of privacy practices. Although the dimensions of information privacy concerns are still under debate, this study adopted CFIP for it is widely-used and clarity. The major dimensions of CFIP are described below

(1) Collection: amounts of identifiable information to be collected and stored in the database.
(2) Errors: the improper protection and violations of individual's personal information.
(3) Unauthorized secondary use: the data collected from an institution but used in a different institution without consumers' consent.
(4) Improper access: individual's personal data is without appropriate protection, and some "illegal parties or users" may gain access to it.

2.2. Website types and information privacy

But, online users feel that "privacy is no longer a social norm"? Or do they have different levels of information privacy? We would like to investigate this interesting research question by comparing users' information-privacy concerns on two Websites: one is relation-based (Facebook.com), and the other is transaction-based (Ruten.com, Taiwan's version of eBay).

2.3. Website types and information privacy concerns

While individuals may engage in different online activities, they may register for membership. For instance, if an individual would like to engage in an online community, he or she has to provide personal information in order to become a member. Similarly, if an individual would like to complete a transaction online, he or she has to provide "necessary personal information" such as delivered address, e-mail address, and phone numbers in order to make the transaction complete. Users are motivated to join a membership, thus they might have various information privacy concerns. Based on the motivation to join an online community, Armstrong and John (1996) classified online communities into four types: transaction, interest, fantasy, and relationship. Based on the business model, Rappa (2001) classified Websites into two groups: one is transaction-based and the other relation-based. The main purpose of a transaction-based Website is to complete a business transaction, while the relation-based Website is to maintain or extend personal social relations. Since Websites serve different purposes, and possibly ask for different personal information for corporate use or online self-presentation, we derive that individuals show the different level of information privacy concerns as Hypothesis 1.

H1. While engaging in different Websites (relational vs. transactional), individuals show different level of information privacy concerns (collection, improper access, errors and unauthorized secondary use).

2.4. Data types and information privacy concerns

Several surveys confirm that the Internet users generally feel differently about the disclosure of different types of information (Kobsa, 2007a,b). They are usually willing to disclose basic demographic and lifestyle information as well as personal

Please cite this article in press as: Tang, J.-H., Lin, Y.-J. Websites, data types and information privacy concerns: A contingency model. Telemat. Informat. (2017), http://dx.doi.org/10.1016/j.tele.2017.05.012

Download English Version:

https://daneshyari.com/en/article/6890026

Download Persian Version:

https://daneshyari.com/article/6890026

Daneshyari.com