Abstract

Online users have strong opinions on privacy and state privacy preferences, yet they do not always behave consistently. Prior studies indicated that those online users exaggerate their zero-cost expectation of privacy-protection practices. Instead of looking at stated privacy preferences, this study focuses on variables that have influences on online users’ actual behavioral intentions toward privacy-protection practices. We adopt the IS continuance model to study online users’ continuance intentions toward privacy-protection practices. We propose that online users’ inconsistent behaviors may result from the inappropriate designs of the practices and users’ unwillingness to continue to use the practices. Combining marketing service theories and the IS continuance model, we assume that perceived usefulness and perceived convenience will determine online users’ satisfaction to the design of privacy-protection practices.

Keywords
Privacy-protection practices, User continuance, privacy concerns, practices design, conveniences, behavioral intentions.

Introduction

Berendt et al. (2005) indicated that many online users have strong opinions on privacy and state their privacy preferences, yet they do not always behave consistently. Why do some of those online users act in ways that do not line up with their stated privacy preferences? Hong and Thong (2013) demonstrated that the divergent wording of items that were used to measure information privacy concerns (IPC) might lead to online users’ inconsistent behaviors. Online users’ information privacy concerns are either expectations or perceptions of others’ behavior, where “other” refers to companies or websites. Perception of others’ behavior is defined as an online user’s perception of the privacy-protection or privacy-invasion practices of a company or website. Expectation of others’ behavior indicates that an online user expects a website or company should adopt practices to handle his/her privacy. Therefore, if expectation of others’ behavior is considered as the stated privacy preference, an online user may have higher-level desired privacy-protection practice standards for a company or website than actual behavioral standards. From another perspective, however, the vulnerability of an online consumer’s behavioral standard over time may also lead to his/her inconsistent behavior. Instead of looking at stated or desired privacy preference, this study focuses on variables that have influences on online users’ actual behavioral intentions toward privacy-protection practices.

Privacy-protection practices (e.g. password, privacy statement, and privacy seal) have been exposed to online users for a longtime, even though they were adopted by different organizations. An online user’s behavioral intention toward privacy-protection practice of a website, therefore, can be represented by the user’s willingness to continue using the privacy-protection practice which has been exposed to the online user by other websites. Bhattacherjee (2001) tested expectation-confirmation theory on IS continuance,
which indicated that a user’s continuance behavioral intention is determined by his or her IS usage satisfaction and perceived usefulness of continued IS use. Privacy-protection practices continuance, similar to IS use, may also be explained by the Bhattacherjee’s model. An online user, who has no willingness to continue to use the privacy-protection practice, may ignore the protection practice when he or she is using the website. An online user, who has low continuance behavioral intention and cannot change his or her option on the implementation of the privacy-protection practice, may have resistance toward the whole website. Those online users’ privacy preferences do not change over time, the changing of actual behavioral intentions, however, is the determination of their inconsistent behaviors.

The IS continuance model, however, only focuses on the impact of long-term usefulness and compresses other perceptions (e.g. perceived ease of use) that are only important to acceptance rather than continuance behaviors. Different from IS use, privacy-protection can be treated as a long-term protection service provided by organizations. In the marketing service research, convenience, defined as consumer’s time and effort perceptions, is a significant variable that influences consumers’ satisfaction (Berry et al. 2002). Therefore, perceived conveniences should be added to the continuance model as a new construct to analyze usage satisfaction and behavioral intention toward the privacy-protection practices at the post-acceptance stage.

The information privacy literatures give insufficient attention to designs of privacy-protection practices. Designers or organizations often blame the weakness of online users and forget to consider how they should measure the effectiveness of privacy-protection practices. This study, from the behavioral intention perspective, points out the possibilities that online users’ inconsistent behaviors result from privacy-protection practices’ inappropriate design, which leads to a mismatch of users’ perceptions, instead of online users’ irrationality.

**Theoretical Background**

**An Expectation-Confirmation Model of IS Continuance**

In consumer behavior literature, the Expectation-Confirmation Theory Model (ECT) is widely used to study repurchase behaviors. IS users’ continuance intentions and consumers’ repurchase intentions are quite similar. For IS use, post-acceptance expectation, changes over time, is much more important than pre-acceptance expectation. All organizations desire long-term usage to lower the cost of losing users and searching for new users. Bhattachrjee (2001) extended ECT to the IS continuance model to explain continuance behavioral intentions of IS users. The IS continuance model focuses only on post-acceptance expectation, because the pre-acceptance variables are involved in the confirmation constructs. The post-acceptance expectation is represented by post-acceptance perceived usefulness, combined with Technology Acceptance Model. In sum, an online user’s continuance behavioral intention is determined by their IS usage satisfaction and perceived usefulness with prior IS use, shown as Figure 1.

![Figure 1. A Post-Acceptance Model of IS Continuance](image-url)
In the real world, the implementation of privacy-protection practices is in the post-acceptance stage, although these practices are adopted by different organizations over time. Online users have been exposed to the same types of privacy-protection practices (e.g. passwords, privacy statements and privacy seal) many times before by other organizations. When an online user has an encounter with a privacy-protection practice of a new website, he or she already has knowledge about the privacy-protection practice. In this situation, the IS continuance model is very appropriate to evaluate the online user’s behavioral intention on the privacy-protection practice, shown as Figure 2. The first hypothesis, same as in IS continuance model, is:

**H1:** Users’ level of satisfaction with prior privacy-protection practices use is positively related to their continuance intention.

For the privacy-protection practices continuance model, however, the confirmation construct will be eliminated. Confirmation construct is used to represent pre-acceptance expectation or initial expectation, which refers to online users’ first time encounter with the privacy-protection practices. As describe before, online users have already experienced each type of privacy-protection practices with other organizations before. It is very difficult for online users to confirm their initial expectation of privacy-protection practices after multiple usages.

Furthermore, the IS continuance model compresses post-acceptance expectation, defined as sum of beliefs, into perceived usefulness; although expectation theoretically may be a broader construct with additional beliefs (e.g. ease of use), based on Technology Acceptance Model. Bhattachrjee (2001) indicated that perceived usefulness is the only belief that impacts users’ behavioral intentions across temporal stages of IS use. In our privacy-protection practice continuance model, perceived usefulness, referring to a cognitive belief salient to privacy-protection practices, represents a user’s post-acceptance expectation of privacy-protection practice. The relationship between perceived usefulness and satisfaction is consistent with the assumption that users’ opinions should be the guidelines of their behaviors. Hence:

**H2:** Users’ perceived usefulness of privacy-protection practices is positively associated with their satisfaction with the practices.

![Figure 2. Privacy-Protection Practices Continuance Model](image-url)
**Perceived Usefulness**

In marketing literature of the service expectation model, consumers' self-service roles increase their expectations of organizational services. Zeithaml et al. (1993) indicated that the higher level of a customer's self-service role is, the higher level of service expectation will be. Adoption of privacy-protection practices is a service provided by organizations to online users. Therefore, perceived usefulness of privacy-protection practice, referring to post-acceptance expectation, is influenced by user-involvement. It has been proved that security becomes more relevant to users when users participate in security risk management (Spears and Barki 2010). For privacy-protection practices, password access is in a higher level of self-involvement than only providing a privacy seal. Changing a password every 30 days is in a higher level of self-involvement than an assigned password by the website. Hui et al. (2007) examined that privacy statements and privacy seals have no significant effects and users have low perceptions toward these privacy practices. Hence:

**H3**: The level of self-involvement in privacy-protection practices is positively associated with perceived usefulness of the practices.

**Perceived Conveniences**

As described before, this study puts other beliefs back into consideration to analyze the potential variables that have influences on privacy-protection practices continuance intentions. Conveniences, defined as online users' time and effort perceptions about the usage of practices (Berry et al. 2002), are very important, because time and effort are resources that online users must give up to use privacy-protection practices continuously. If an online user changes his/her password every 30 days, he or she must put in more time and effort to remember all the passwords. If an online user has a higher level of participation, he or she will give up more time and effort, resulting in lower perceived conveniences. Compared to ease of use, a pre-acceptance perception, perceived convenience is a post-acceptance variable that has a long-run positive influence on an online user’s behavioral intention. If a privacy-protection practice requires too much time and effort, we assume that online users may have emotional resistances toward the practice. Hence:

**H4**: The level of self-involvement in privacy-protection practices is negatively associated with perceived convenience of the practices.

**H5**: Users’ perceived convenience of privacy-protection practices is positively related with their satisfaction of the practices.

In the IS continuance model, behavioral intention is based on cognitive decision rules or heuristics that are invoked without conscious thought. In the model, perceived usefulness has direct influences on behavioral intention. Perceived convenience, as a measure of users’ time and efforts, is a vital heuristic trigger for online users to be less conscious. Therefore, in our model, perceived usefulness and convenience are both the direct references to users’ behavioral intentions.

**H6**: Users’ privacy-protection practice continuance intention is positively related with their perceived usefulness of practice use.

**H7**: Users’ privacy-protection practice continuance intention is positively related with their perceived convenience of practice use.

**Information Types**

Malhotra et al. (2004) pointed out contingent effects of information on online users’ behavioral intention. More sensitive information, compared to less sensitive information, will have a more negative influence on online users' intention to reveal personal information. In other words, if an organization requests more sensitive information, online users will have a higher level of intention to adopt the privacy-protection...
practices and have higher requirements on the practices. Furthermore, the negative effect of emotional resistance from low perceived convenience can also be diluted, if online users deal with more sensitive information. Thus, our final hypothesis is stated below:

**H8:** Information types moderate the relationship between perceived usefulness and perceived convenience and privacy-protection practice continuance intention.

**Methodology**

A between-subject experiment will be conducted to examine participants’ attitudes toward using the privacy-protection practices. The participants will be assigned to different scenarios about setting up and using passwords. After reading the scenario, each participant will be asked to complete a survey related to their attitudes and intentions toward online privacy-protection practices. The data will be analyzed to determine the relationships among these variables.

**REFERENCES**


