5-2009

Consumer Online Privacy Concern and Behavior Intention: Cultural and Institutional Aspects

Xiao Jiang
Dalian University of Technology, businessj@126.com

Shaobo Ji
Carleton University, shaobo_ji@carleton.ca

36. CONSUMER ONLINE PRIVACY CONCERN AND BEHAVIOR INTENTION: CULTURAL AND INSTITUTIONAL ASPECTS

Xiao Jiang
Dalian University of Technology
businessj@126.com

Shaobo Ji
Carleton University
shaobo_ji@carleton.ca

Abstract

With the rapid development of e-commerce and increased number of online transactions in the developing countries, consumer privacy has become an important issue for e-commerce adoption. Although the issue had been addressed in many previous studies, however, these studies were typically conducted in developed countries in different cultural and institutional contexts. The purpose of this paper is to provide a theoretical model of consumer online privacy concern and behavior intention to adopt e-commerce taking into the consideration of demographic, cultural, and institutional factors based on case analysis in a developing country.

Key words

Online privacy concern, behavior intention, e-commerce adoption

1. Introduction

Online transaction has become more popular in developing countries such as China. At the same time, similar to developed countries, it has raised many privacy concern (Caudill and Murphy, 2000) since online transaction requires the disclosure of a large amount of personal information, e.g., credit card information and delivery details. On one hand, acquisitions and possessions of personal information allow businesses to analyze customer data, discovering trends and increasing the efficiency of their business transactions. On the other hand, consumers are understandably concerned about the use and in some case the misuse of their personal information. Internet users are becoming conscious of the power of Internet technologies to monitor their activities and gather information about them with or without their knowledge and consent (Milberg et al., 1995). Consumer's privacy protection as a result to a great extent will determine e-commerce success and ultimately e-commerce adoption. In

addition to consumer's demographics, cultural and institutional factors play critical roles in consumer's privacy concern and online transaction behaviors. For example, compared with consumers in the United States, consumers in China may face different kinds of privacy concerns due to its institutional deficiencies, i.e., lack of rule of law and lack of enforcement, deficiencies in financial infrastructures, and cultural differences, i.e., fundamental views about businesses, and the nature of businesses are conducted (Martinsons, 2008). However, privacy is a relative concept which has different meanings for different individuals in different cultures. Given the diverse definitions of privacy by many, it is important to define the aspect of privacy for specific research purposes and to consider the contextual factors. This paper, by giving operational definition, defines privacy as the control over the disclosure of information about one's self or personal transactions.

The purpose of this paper is to provide a framework of online privacy concern and behavior intention in case of consumers in China so as to understand Chinese consumer's privacy concern and behavioral intent. We adopt the theory of reasoned action (TRA) to address the relationship between consumer privacy concern and subsequent consumer intent responses in cultural and institutional contexts. The paper is organized as follows. We begin with describing a conceptual framework which addresses the relationships between key variables including online privacy concern and behavior intent and demographic, cultural and institutional factors. This is followed by a detailed description of the framework based on case analysis. The paper concludes with a discussion of theoretical and practical implications.

2. Conceptual Framework

Many researchers found that online purchasing intent is significantly influenced by consumer's privacy concern (Ranganathan and Ganapathy, 2002). Privacy concern is determined, at individual level, by one's age, gender, education, and online experience, beliefs and values. Personal beliefs and values are shaped by such broader macro factors as culture and institution. As found in numerous IT and e-commerce adoption literatures, cultural and institutional differences should be considered when developing and implementing IS applications (Dinev and Hart, 2006; Dowling and Staelin, 1994; Malhotra et al., 2004; Martinsons, 2008; Martinsons and Davison, 2007; Milberg et al., 1995; Son and Kim, 2008). Because of interests in social issues and policies, Internet users with high social awareness will closely follow Internet privacy issues. Therefore, one may speculate, with respect to privacy concern that Internet users who are more socially aware will tend to know more about the privacy debate, privacy policies, privacy risks associated with the Internet, and the legal implications of privacy invasions (Dinev and Hart, 2006). At the same time, institutional factors such as public policy and legal approaches to privacy protection policies will also affect consumer's intent and actual use of online transaction (Caudill and Murphy, 2000; Clarke, 1999; North, 1991; Pincus and Johns, 1997). The stages of social and economic development of a particular country may also affect consumer's privacy concern and behavioural intent of using online transactions. For example, Martinsons (2008), after an in-depth analysis of e-commerce adoption and development cases in China, concluded that e-commerce adoption is easier in a country such as USA where the fundamental social and

economic relationship is based on the rule of law and institutional assurance as compared with a country such as China where the fundamental social and economic relationship is "relationship-based".

We propose a conceptual framework, shown in Figure 1, for understanding the consumer privacy and behavior intention which, in our belief, is more suitable in case of China. We adopt the theory of reasoned action (TRA) as the theoretical foundation. There are six variables in the proposed framework, including online privacy concern, online privacy behavior intention to conduct online transaction, cultural factors, institutional environment factors, demographic factors and online privacy risk beliefs. As shown, online privacy concern and online privacy behavior intention are determined by demographic, cultural, and institutional factors. Online privacy risk beliefs moderates the relationship between online privacy concern and online privacy behavior intention. Table 1 lists the explanation of each component.

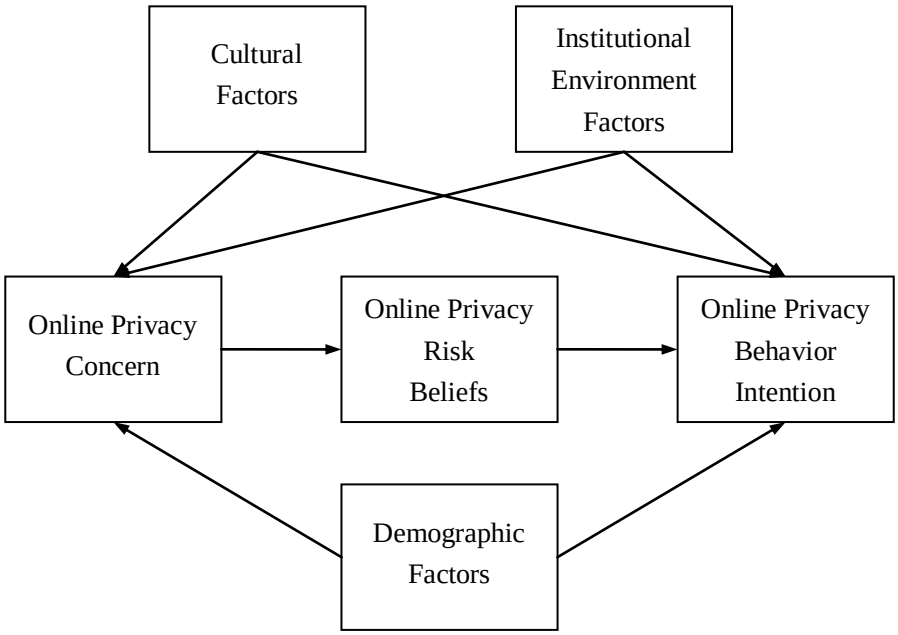

Figure 1: A conceptual framework of online privacy concern and behavioural intention

Table 1 Definition of component

Dimension	Description
Cultural factors	Mostly psychological dimensions, or value constructs, which are mostly related to online privacy issue. It explains the values of a particular culture and how they affect customer online privacy concern and behavior.
Institutional environment factors	It includes informal constraints such as website privacy policy, and formal constraints, such as constitutions, privacy laws, and property rights.
Online privacy concern	Consumer's concern for controlling the acquisition and subsequent use of the information that is generated or acquired on the Internet about him or her.
Online privacy behavior intention	A set of Internet consumer's readiness responses to their perception of online privacy threats on transactions.
Online privacy risk beliefs	Expectation that a high potential for loss is associated with the release of personal information to the firm.
Demographic factors	Statistical socio-economic characteristics or variables of a population, such as age, gender, educational level, income level, marital status, occupation, religion.

3. Applying the framework: the case of consumers in China

Previous researchers have focused on general consumer concern towards privacy in various contexts. Culture has been incorporated as a demographic factor in many works and has rarely been studied in isolation as an antecedent to privacy concern (Bellman et al., 2004). As stated by some, research on public policy and legal approaches to privacy protection policies were mainly evaluative, approaching the problem from legal and ethical viewpoints (Caudill and Murphy, 2000), and concentrated on how governments coped with or should respond to privacy concern (Clarke, 1999; Pincus and Johns, 1997).

Online privacy concern can be defined as Internet consumer's concern for controlling the acquisition and subsequent use of the information generated or acquired on the Internet about him or her (Castañeda et al., 2007). According to Castañeda et al. (2007), two dimensions are considered: concern for control over the collecting of personal information and concern for control over its use on the electronic market. "Control" is related to online security. Use refers to the inadequate use of the information by those firms that have been authorized to use personal data.

A variety of consumer responses to privacy concern in general and to online privacy in particular have also been noted. Individuals who claim they are concerned about their personal information act in different ways when an information-sensitive situation actually arises. Some complete transactions anyway, without actually protecting personal information. Some falsify the information they provide to others. Some avoid information risks altogether by aborting ongoing transactions. These responses can be considered as power-enhancing to

the consumers. These three individual actions are fabricated, protect, and withhold. "Fabricate" refers to consumer efforts in disguising one's identity through the use of fictitious or false information. "Protect" refers to the use of technology to safeguard one's Internet domain from potential intruders. For instance, consumers can use technology to reject cookies. "Withhold" refers to the consumer's refusal to provide information or to patronize web sites (Wirtz et al., 2007).

3.1 Cultural Factors

Culture has recently received more attention in IS research because of the importance of IT application in global and highly heterogeneous cultural environments. Although there are many different definitions of national culture, Hofstede's (2001) typology of culture has been one of the most popular in many different fields of management. Most researchers have intended to rely almost solely on Hofstede's definition. It seems likely that associations between cultural values and information privacy concern may also exist. For example, researchers have found that there are differences in information privacy concern across cultures. However, few studies are available that examine how these privacy concern affect the extent of Internet and e-commerce use and links between cultural values and information privacy concern (Milberg et al., 1995; Dinev and Hart, 2006). Many researchers claimed at the minimum the following three cultural dimensions should be taken into account when studying consumer's online privacy concern: uncertainty avoidance, power distance, and individualism (Milberg et al., 1995; Dinev and Hart, 2006; Shin et al., 2007).

In case of China, the word "privacy" is not rooted in the Chinese culture and the sense of "self" is not considered as essential by many. Some researchers found that Confucianism played an important role in Chinese society and has influenced the concept of privacy (Moore, 1984). On one hand, Chinese culture promotes that the behaviors of noble and persons with integrity should be examined in public. It was found that individuals from higher Confucian dynamism societies tend to emphasize social harmony and exhibit a greater willingness to share their information (Fu, 2002; Li et al., 2007). For example, Chapter 7 of the Analects of Confucius states, "The Superior Man is always at ease with himself", "The inferior man is always anxious". Closely related to this tradition are low "individualism"/high "collectivism" nature of the Chinese society. Not only the concept of "privacy" did not exist, for a period of long time in the history, the collectivism has been reinforced in recent history of communism where group and national interests are emphasized over that of individual. Therefore, it is not surprising for one to find Internet users posting their personal information such as their date of birth, cell phone number, even identity card number in the public domain. The implication of this on online privacy concern is that Chinese may be less concerned about their personal information being disclosed unless they are financially or otherwise being damaged. On the other hand, *guanxi*, or relationship, plays a major role in Chinese society. The word "*guanxi*" refers to the concept of drawing on connections in order to secure favors in personal relationships (Li et al., 2007). It has a strong impact on privacy and privacy concern. The concept "*guanxi*" may hinder Chinese to share information within incognizant group on the Internet and may result in a more public concern on privacy. Due to

a powerful obstacle of the entrenched nature of the *guanxi* system (Seligman, 1999), it will be even harder to get 1.3 billion people to trust the system and abide by the rule of law when doing business (Martinsons, 2008). Closely related to "*guanxi*" and "collectivism" nature of the Chinese society are power distance and uncertainty avoidance. Chinese society can be generally categorized as "high power distance" and moderately high "uncertainty avoidance". The hierarchical nature of the Chinese society is contrary to the very nature of "e-commerce" which demands and in fact faltering the hierarchies. One potential implication is that Chinese may be less concerned about using government and some corporation's websites that are deem to be more "authoritative" as compared with less reputable websites. As for uncertainty avoidance, China is moderately high in uncertainty avoidance and thus the assumption is that Chinese consumers may be in general demonstrating high anxiety about ambiguous situations and unfamiliar risks such as online transaction.

3.2 Institutional Factors

For consumer's online privacy concern and behavior intent, institutional factors generally refer to the regulatory policies and laws of how various government agencies, the other key power holders, devise Internet privacy regulation, and direct and police the use of consumer data. The state is generally seen as having the responsibility to ensure the well-being of consumers in cases of power imbalance and data protection concern (Smith, 1994). For example, higher levels of privacy concern were found to be associated with more moderate regulatory environments (Milberg et al., 1995). Regulation is seen as essential in protecting online privacy (Rust et al., 2002). At industry and organizational level, privacy policy deals with company's policy as perceived by consumers of how an industry or a firm exercises ownership and power over the use of consumer data. A recent study conducted by Liu and Arnett (2002) suggested that only slightly more than 50% of large business websites provided privacy policies or appropriate links to them on their home pages. When website operators provide a safe environment, they reduce consumer's privacy concern, and hence enhance its use. In order to protect consumer's privacy, organizations must protect all the personal information which they collect either directly or indirectly from other organizations (Liu and Arnett, 2002).

In China, with the long history of the empire system of government, Chinese people tend to disclosing their information and observing others' behavior until the introduction of Western culture (EPIC, 2001). Presently, some related articles are presented in Chinese Constitution. For instance, Article 37 of the Constitution stipulates that "the freedom of citizen of the People's Republic of China is inviolable", and Article 40 states, "Freedom and privacy of correspondence of citizen of the People's Republic of china are protected by law". Other non-juristic systems also begin to emerge. For instance, the rules concerning the administration of provision of internet bulletin board service (2000) are seen as a more specific regulation than any others in China on personal data protection (Fu, 2002). It requires service providers to keep consumer's information confidential and should not disclose to any other third party without the consumer's consent except if the disclose is required by law.

However, authorities across China may manipulate e-commerce development so as to maintain their privileged positions. Remarkably, it focuses more on protecting state property (from below-value appropriation by private interests) than private or intellectual property (Martinsons, 2008). So that consumer's privacy is less significant and sometimes negligent in China. In reality, the issue of "unauthorized use of personal information by businesses" and the "buying and selling" of consumer information by business such as mobile phone operators has become "epidemic" in recent years in China. In fact, in most recent survey, "unauthorized use of consumer information" was ranked as one of the top problems in consumer protection in China (http://business.sohu.com/20090316/n262814719.shtml). There seems to be an urgent need for government agencies and businesses to take immediate action in order to protect consumer's information and ease their privacy concern.

3.3 Demographic Factors

Differences in online privacy concern have been suggested across demographic groups by age, gender, education level, income level and Internet experience (Graeff and Harmon, 2002; Sheehan, 2002; Bellman et al., 2004). We speculate that demographic factors, although to certain extent, related to cultural and institutional factors, are relatively universal. In China, with more than 210 million Internet users in Chinese total population, mostly has not enough Internet experience, while their educational experience is lower (CNNIC, 2008). In addition, the eastern part of China has larger population than the western part, while the eastern economy is more developed.

3.4 Perceived Privacy Risk

Internet has given us the ability to conduct business online with those who live thousands of miles away at the same time it has also brought cyber criminals. Most are resulted from unauthorized and fraudulent use of personal identity information. As misuse of personal information (such as credit card numbers, bank account numbers) increases, people's concern about privacy increases. It's obvious that some have suggested that while users may view the Internet as a marketing channel, security and privacy issues are very influential on decisions to buy online (Smith and Rupp, 2002). Given the growth of online identity theft and identity fraud, a tendency of concern over online privacy will influence how a person perceives a given privacy risk (Cockcroft et al., 2005).

From public policies, rule of law and the enforcement of law perspective, special privacy risks do exist in China. For instance, the "human flesh search engine", a literal translation of the Chinese, is a phenomenon of mobilizing the Internet population to track down specific individuals or facts. It has become a familiar term for most of Chinese Internet users as the engine has been frequently used recently to find and punish those who are believed to have published inappropriate materials. In most cases, personal details about those people could be post on the Internet. In some cases, the individuals who were exposed online perceived as the gross invasion of their privacies. A debate has started recently about whether the country

should issue relevant privacy laws or rules to regulate the use of the "human flesh search engine".

Sharing personal information online may also be risky in China. It needs to provide national identification card numbers for many online transactions. This raises acute privacy concern. Some sensitive and proprietary information collected and warehoused by state agencies seems to be accessible to others with good *guanxi*. Consequently, consumer's information is usually actively traded and frequently misused in China. As mentioned in 3.2, this has become a serious problem. In one occasion, as reported by CCTV, a reporter spent RMB 100 and was able to obtain over 1000 pieces of information (this is equivalent to under USD $0.02/piece of information) containing such personal data as name, cell phone number, and national identification card number.

From technological and infrastructural perspective, Chinese top level domains (TLDs) are generally considered less safe. For example, in its annual report, Mapping the Mal Web, McAfee (Keats, 2008) ranked China (.cn) second most risky TLD in 2008, a ranking only after Hong Kong which was considered the most risky TLD (.hk).

4. Conclusion

This paper presents a conceptual framework of online privacy concern and behavior intention in the context of demographic, cultural and institutional factors using the case of China. The framework integrates the culture and institution perspectives that are unique to China, discusses some of the key factors in affecting online privacy concern and behavior intent, speculates some of relationships between the risk factors and privacy concern and behavior intention. We tried to show that, in the world of growing importance and presence of e-commerce, cultural and institutional factors must be regarded as key factors for consumer's online privacy concern and behavior intent. In order to test our claims, we intend to, in our future studies, empirically test our claims and the relationships we postulated in this paper.

In conclusion, privacy protection on the Internet demands a multi-tier approach, involving organizations, governments and individual consumers. Our conceptual framework can be used as a general guideline for conducting comprehensive research into online privacy concern and behavior intent from the consumer's point of view.

References

Bellman, S., Johnson, E.J., Kobrin, S.J. and Lohse, G.L. (2004) International differences in information privacy concerns: A global survey of consumers. The Information Society, 20(5), 313-324.

Castañeda, J.A., Montoro, F.J. and Luque, T. (2007) The dimensionality of customer privacy concern on the Internet. Online Information Review, 31(4), 420-439.

Caudill, E.M. and Murphy, P.E. (2000) Consumer online privacy: Legal and ethical issues. Journal of Public Policy & Marketing, 19(1), 7-19.

China Internet Network Information Center (CNNIC) (2008) Survey report on the development of China's Internet (semi-annual publication) and other documents. [WWW document]. http://www.cnnic.net.cn and http://www.cnnic.org.cn

Clarke, R. (1999) Internet privacy concerns confirm the case for intervention. Communication of the ACM, 42(2), 60-67.

Cockcroft, S.K.S. and Heales, J. (2005) National culture, trust and Internet privacy concern. Proceedings of the 16th Australasian Conference on Information Systems, Sydney.

Dinev, T. and Hart, P. (2006) Internet privacy concern and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10(2), 7-29.

Dowling, G.R. and Staelin, R. (1994) A model of perceived risk and intended risk-handling activity. Journal of Consumer Research, 21(1), 119-134.

Electronic Privacy Information Center (EPIC). (2001) Privacy and Human Rights: An International Survey of Privacy Laws and Developments. Washington, Dc, EPIC.

Fu, Y. (2002) Personal data protection in China. The China Business Review, 29(4), 36-39.

Graeff, T.R. and Harmon, S. (2002) Collecting and using personal data: Consumers' awareness and concerns. Journal of Consumer Marketing, 19(5), 302-318.

Hofstede, G.H. (2001) Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations across Nations. Sage Publications, Thousand Oaks, California: London.

Keats, S. (2008) McAfee Report, Mapping the mal web, revisited, retrieved from http://us.mcafee.com/en-us/local/docs/Mapping_Mal_Web.pdf?cid=45044 on March 22, 2009.

Li, J.P., Shin, S.K. and Sanders, L. (2007) Prediction of information sharing behavior in China: under standing the cultural and social determinants. Proceedings of the 40th Hawaii International Conference on System Sciences.

Liu, C. and Arnett, K.P. (2002) An examination of privacy policies in Fortune 500 Web sites. Mid-American Journal of Business, 17(1), 13-21.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model, Information Systems Research. 15(4), 336-355.

Martinsons, M.G. (2008) Relationship-based e-commerce: Theory and evidence from China. Information Systems Journal, 18(4), 331-356.

Martinsons, M.G. and Davison, R.M. (2007) Culture's consequences for IT application and business process change: A research agenda. International Journal of Internet and Enterprise Management, 5(2), 158-177.

Milberg, S.J., Burke, S.J., Smith, H.J. and Kallman, E.A. (1995) Values personal information privacy, and regulatory approaches. Communications of the ACM, 38 (12), 65-74.

Milberg, S.J., Smith H.J. and Burke, S.J. (2000) Information privacy: Corporate management and national regulation. Organization science, 11(1), 35-57.

Moore, B. (1984), Privacy: Studies in Social and Cultural History. M.E. Sharpe, New York, NY.

North, D.C. (1991) Institutions. Journal of Economic Perspectives, American Economic Association, 5(1), 97-112.

Pincus, L.B. and Johns, R. (1997) Private parts: A global analysis of privacy protection schemes and a proposed innovation for their comparative evaluation. Journal of Business Ethics, 16(12), 1237-1260.

Ranganathan, C. and Ganapathy, S. (2002) Key dimensions of business-to-user websites. Information and Management, 39(6), 457-465.

Rust, R.T., Kannan, P.K. and Peng, N. (2002) The customer economics of Internet privacy. Journal of the Academy of Marketing Science, MSI/JAMS Special Issue on Marketing to and Serving Customers on the Internet, 30(4), 451-460.

Seligman, S.D. (1999) Guanxi: Grease for the wheels of China. China Business Review, 26(5), 34-38.

Sheehan, K.B. (2002) Toward a typology of Internet users and online privacy concerns. Information Society, 18(1), 21-32.

Shin, S.K., Ishman, M. and Sanders, G.L. (2007) An empirical investigation of socio-cultural factors of information sharing in China. Information & Management, 44(2), 165-174.

Smith, A.D. and Rupp, W.T. (2002) Issues in cyber security: Understanding the potential risks associated with hackers/crackers. Information Management & Computer Security, 10(4), 178-183.

Smith, H.J. (1994) Managing Privacy: Information Technology and Corporate America. University of North Carolina Press, Chapel Hill, NC.

SOHU Business, http://it.sohu.com/s2009/gerenxinxi/, accessed on March 22, 2009.

Son, J.Y. and Kim, S.S. (2008) Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quarterly, 32(3), 503-529.

Wirtz, J., Lwin, M. and Williams, J.D. (2007) Causes and consequences of consumer online privacy concern. International Journal of Service Industry Management, 18(4), 326-348.