Winter 12-5-2005

The Protection of Privacy in Internet Banking

Ziqi Liao

The Protection of Privacy in Internet Banking

Ziqi Liao
Department of Finance and Decision Sciences
Hong Kong Baptist University
Renfrew Road, Kowloon, Hong Kong
Telephone: (852) 34115227 e-mail: victor@hkbu.edu.hk

Abstract: This paper explores the consumer concerns about privacy in Internet e-banking and examines the impacts of several variables in relation to perceived privacy protection. The findings suggest that commercial banks must effectively minimize transaction errors, eliminate unauthorized use of personal data, control offensive access and maintain transactions records. Preventive management is vital to the enhancement of privacy of Internet banking and the consumer acceptance of Internet banking services.

Keywords: e-finance, Internet banking, consumers, privacy.

I. Introduction

Internet banking provides an effective electronic channel for delivering banking and financial services and enables individuals to access accounts anytime and anywhere. However, the spread of e-commerce activities increasingly causes privacy concern, which considerably affects the success of different e-businesses. As far as this is concerned, it is important for e-banking service providers to appreciate consumer expectation in privacy protection. This paper examines several variables in relation to the protection of privacy in the case of Internet banking. It also explores the impacts of these variables on consumer acceptance of the e-banking services.

II. Hypotheses

Numerous existing studies have examined the protection of privacy [3] [8] [9] [14] [15] [17]. For instance, Smith, Milberg and Sandra [17] measure individual's concerns about information privacy using several dimensions such as collection, unauthorized secondary use, errors and improper access. On the basis of previous work, this study applies several variables in relation to the perceived privacy and examines their influences in operational environments of Internet banking. These include personal data collection, data errors, unauthorized use of personal data, offensive access control, data loss, perceived privacy, attitude and behavioral intention to use Internet e-banking. Firstly, commercial banks have collected a large amount of personal data for different banking and financial services. Customers may be offended by the request of providing some sensitive data in relation to individual privacy. Hence, Hypothesis 1 is proposed:

H1: The collection of customer data has a positive impact on perceived privacy.

Secondly, it is practically difficult to completely eliminate deliberate and accidental errors in business transactions. The assurance of data correctness and data integrity remains an important issue [9]. However, some firms have not taken enough steps to minimize errors in data processing [17]. The concern about transaction errors in banking environment may considerably affect individual perceptions of privacy. Therefore, Hypothesis 2 is proposed:

H2: The minimization of transactional errors has a positive impact on perceived privacy.

Thirdly, consumers might worry about that the information collected from individuals is used for unusual purposes without permission. Even within a company, for example, the information collected for research purposes may be used for marketing promotion [2]. In the banking industry, the data collected from loan applications may be used to sort customers into different categories for service promotion. In terms of unauthorized use of personal data, it may include secondary use of information and shares of customer contacts with other firms. As a result, it leads to a negative response from individuals [3] [17]. Therefore, Hypothesis 3 is proposed.

H3: The elimination of unauthorized use of personal data has a positive impact on perceived privacy.

Fourthly, there is a concern about offensive access, because someone is not properly authorized, may be able to view or work with a particular data [15]. The access to individuals account should affect the privacy level especially in e-banking environment. How to effectively control the unauthorized access is a critical administrative issue of an organization [17]. Hence, the following is proposed:

H4: The control of offensive access has a positive impact on perceived privacy.

Moreover, personal data and transaction records might be lost due to the removal of electronic data while it is transited. It might also be lost when someone accidentally erases the data in a database. If an individual assumed that there would be a loss of personal data through the use of an information system, little privacy of the application should be perceived [9]. The storage and data maintenance of

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 515 - 517.

individual data remains an important task especially for bank operations management. Therefore, Hypothesis 5 is proposed.

H5: The elimination of data loss has a positive impact on perceived privacy.

Numerous studies suggest that attitude has a significant effect on behavior intention [1] [4] [5] [6] [7] [10] [11] [12] [13] [16] [18]. Attitude can mediate effective responses between beliefs and usage attention [4] [5]. Increasingly, consumers are seriously concerned about the protection of privacy associated with electronic commerce activities. Empirical work indicates that privacy is a significant factor influencing consumer willingness to use e-banking [15]. In general, those expecting a higher level of perceived security usually have a more favorable attitude towards the service [8]. Therefore, the Hypotheses 6.1 and 6.2 are proposed.

H6.1: Perceived privacy has a positive impact on consumer attitude towards Internet banking.

H6.2: Consumer attitude influences behavioral intention to use Internet banking.

III. Methods

The research methods include survey and statistical data analysis. The questionnaire includes a number of questions in relation to perceived privacy, consumer attitudes and behavior Intention to use Internet banking. In order to ensure content validity of the scales adopted, the items within the questionnaire were developed with reference to the existing literatures. The respondents were asked to indicate whether they have experience on the use of Internet banking. They were also asked to give their observations using a seven-point Likert-scale ranging from 1 to 7. Moreover, they were requested to provide demographic data such as gender, education, income and occupation. As a result, two hundred and ten useful responses were received at this stage. Finally, several procedures of the Statistical Package for Social Science were used to analyze the data collected.

IV. Results and Discussion

Multiple regression analysis has been conducted to test to the above-mentioned hypotheses. The results in Table 1 indicate that several exogenous variables have significant impacts on the endogenous variable (F = 26.92, $Sig.$ < 0.001) and H2, H3, H4 and H5 are supported. The R^2 value of 0.383 suggests that 38.3% of the variance can be explained. In other words, the minimization of transactions errors, the elimination of unauthorized use of personal data, the control of offensive access, and the protection of customer data significantly affect the perceived privacy of Internet banking. In turn, the perceived privacy significantly affects consumer attitude towards Internet banking (F = 29.06, β=0.35, $Sig.$ < 0.001) which also considerably influences their behavioral intention to use e-banking services (F = 100.41, β=0.57, $Sig.$ < 0.001). Therefore, H6.1 and H6.2 are supported.

It is generally understandable that an individual customer must provide necessary personal data when opening an account in a respectable financial institution. Therefore, the bank has little problem on the collection of customer personal data. However, it is desirable that the bank is able to identify any data problems and transaction errors and make prompt corrections in data processing. In addition, the elimination of unauthorized use of customer personal data is critical to the protection of customer privacy. It is not uncommon that some banks may intensively analyze the personal data of customers for the purpose of customer relationship management. Based on data-mining, banks may be able to appreciate the need of different customers. Although the banks usually have particular administrative procedures and regulations for data analysis, consumers are still concerned about the use of personal data. As far as this is concerned, the banks should ask the customers whether they are allowed to use the information for product and service promotions.

Table 1 Results of Regression Analysis

	β	t	$Sig.$
(Constant)		4.518	.000
Data collection	.035	.636	.525
Transaction errors	.166	2.566	.011
Unauthorized use	.231	3.363	.001
Offensive access	.138	2.000	.047
Data loss	.259	3.689	.000

Note: Adjusted R^2 = 0.383.

Furthermore, the banks must strictly control offensive access to Internet e-banking systems, in order to effectively protect the privacy of its customers. A consistent investment in the most advanced security technology is critical to enable the banks to immediately identify any unusual attempt to enter an e-banking account and to restrict different offensive attaches to the Internet banking systems. Finally, customers are concerned about the possible loss of transactions data, because it is beyond their control. The banks must be responsible for maintaining transactions records. An effective elimination of data loss should greatly enhance the customers' confidence in Internet banking services. In sum, the findings suggest that commercial banks must minimize transactional errors, eliminate unauthorized use of personal data, stop any offensive access, and maintain the personal data of customers. This will help enhance the perceived level of privacy protection. In order to encourage more people to use of Internet banking, they must adopt a series of security procedures to protect privacy in Internet e-banking services.

V. Conclusion

An understanding of customer concerns and expectations is essential for planning and promoting Internet e-banking services. It is also important for formulating competitive

strategy for business development. This study systematically identifies the privacy concerns from the customer perspective. Preventive management such as minimizing transactional errors, eliminating unauthorized use of personal data, controlling offensive access, and maintaining transactions data are vital to the protection of customer privacy, which also significantly affect individual attitude and behavioral intention to e-banking. The findings have practical implications for managing the existing Internet e-banking systems. Accordingly, commercial banks might develop and implement a series of administrative procedures to protect the privacy and security of e-banking services. Practically, there are various variables associated with the protection of individual privacy in different social and cultural environments. Therefore, the present study can be extended to explore other aspects which might affect consumer acceptance and adoption of Internet e-banking in different contexts.

Acknowledgement

The research support of the Hong Kong Baptist University is gratefully acknowledged.

References

[1] Adam, D.A., Nelson, R.R. & Todd P.A. "Perceived usefulness, ease of use, and usage of information technology: A replication," *MIS Quarterly*, 1992, 16 (2), 227-247.

[2] Cespedes, F.V. & Smith, H.J. "Database marketing: New rules for policy and practice," *Sloan Management Review*, 1993, 34 (2), 7-22

[3] Culnan, M.J. "How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use," *MIS Quarterly*, 1993, 17(3), 341-363.

[4] Davis, F.D. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, 1989, 13 (3), 319-340.

[5] Davis, F.D., Bagozzi, R.P. & Warshaw, P.R. "User acceptance of computer technology: A comparison of two theoretical models," *Management Science*, 1989, 35 (8), 982-1000.

[6] Davis, F.D. "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts," *International Journal Man-Machines Studies*, 1993, 38, 475-487.

[7] Devaraj, S., Fan, M. & Kohli, R. "Antecedents of B2C channel satisfaction and preference: Validation e-Commerce metrics," *Information Systems Research*. 2002, 13 (3) 316-333.

[8] Dutta, A. & McCrohan, K. "Management's role in information security in a cyber economy," *California Management Review*, 2002, 45 (1), 67-87.

[9] Fulkerson, C.L., Gonsoulin, A.M. & Dianne, W.B. "Database security," *Strategic Finance*, 2002, 84 (6), 48-53.

[10] Gefen, D. "TAM or just plain habit: A look at experienced online shoppers," *Journal of End User Computing*, 2003, 15 (3), 1-13.

[11] Gefen, D. & Straub, D.W. "Gender differences in perception and adoption of e-mail: A cross-cultural perspective," *MIS Quarterly*, 1997, 21 (4), 389-400.

[12] Igbaria, M. "An examination of the factors contributing to microcomputer technology acceptance," *Accounting, Management & Information Technology*, 1994, 4 (4) 205-224.

[13] Jackson, C.M., Chow, S. & Leitch, R.A. "Toward an understanding of the behavioral intention to use an information system," *Decision Sciences*, 1997, 28 (2), 357-389.

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

[15] Liao, Z. & Cheung, M.T. "Internet-based e-banking and consumer attitudes: An empirical study," *Information and Management*, 2002, 39 (4) 283-295.

[16] Szajna, B. "Empirical evaluations of the revised technology acceptance model," *Management Science*, 1996, 42 (1), 85-92.

[17] Smith, H.J., Milberg, J.S. & Sandra, B.J. "Information privacy measuring individuals' concerns about organizational practices," *MIS Quarterly*, 1996, 20 (2), 167-196.

[18] Venkatesh, V. & Davis, F.D. "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management Science*, 2000, 46 (2) 186-204.