PRIVACY CONCERNS IN INTERNET APPLICATIONS

Moshe Zviran, Seev Neumann, Diego Hocksman
Management of Technology and Information Systems Department
Faculty of Management, Tel Aviv University
P.O.Box 39010, Tel Aviv 69978, ISRAEL

Keywords: Internet, privacy, secrecy

Abstract: Privacy is defined as "freedom from unauthorized intrusion". While privacy has been a sensitive issue before the advent of computers, the concern has been further exacerbated by the fact that the Web makes it easy for data to be automatically collected and added to databases and analyzed by sophisticated data mining tools and personalized marketing services. This study explores the nature of the privacy concern in the online environment. The objective of this study is to get a better understanding of the factors that can affect online privacy and how this concern could affect users' behavior.

1 INTRODUCTION

Privacy is defined in the Merriam-Webster Dictionary (2000) as "freedom from unauthorized intrusion", and is related to solicitude, secrecy, and autonomy. It was a sensitive issue long before the advent of computers. Concerns have been magnified, however, by the existence and widespread use of large computer databases that make it easy to compile a dossier about an individual from many different data sources.

Privacy issues are further exacerbated now that the World Wide Web makes it easy for new data to be automatically collected and added to databases. As data mining tools and personalized marketing services become more widely available, privacy concerns are likely to further increase.

Online privacy concerns often arise through a web site operator's collection and dissemination of personally identifiable information about an individual consumer who has visited a particular web site (Hatch, 2000). Specifically, privacy concerns arise when consumers' personally identifiable information is collected online without the consumer's consent or knowledge and/or is sold to third parties without the consumer's consent or knowledge. Thus, online privacy relates to affirmative conduct of the web site visited by the consumer.

2 PRIVACY CONCERNS

In cyberspace, because both purchases and browsing are recorded, not only are organizations able to record traditional consumer interactions such as purchases or explicit requests for information, but because online systems provide the capability to record a consumer's "mouse tracks," organizations are also able to record how consumers move through their web sites and to profile what was formerly a passive, private activity. This practice of tracking the browsing behavior of individuals as they "surf" the pages of various web sites, without disclosing to the consumer what information is being collected, how it will be used or communicating how the consumer benefits from their disclosures, can affect how consumers behave.

Adopting a certain behavior depends on the degree of consumer's privacy concern (Bartel & Grubbs, 1999). For example, as privacy concerns increase, consumers are more likely to provide incomplete information to web sites, to notify Internet Service Providers about unsolicited e-mail, to request removal from mailing lists, and to send a "flame" to online entities sending unsolicited e-mail. Additionally, as privacy concerns increase, consumers are less likely to join web sites requesting information.

Zviran M., Neumann S. and Hocksman D. (2004).
PRIVACY CONCERNS IN INTERNET APPLICATIONS.
In *Proceedings of the Sixth International Conference on Enterprise Information Systems*, pages 592-595
DOI: 10.5220/0002592905920595

3 RESEARCH MODEL AND HYPOTHESES

This study attempts to explore two research issues:

1. Which variables from the online environment affect the degree of online privacy concern? In order to study this issue, the relationships between the degree of online privacy concerns and the following variables were measured: *usage of privacy enhancing mechanisms, Web usage, being a victim of previous online privacy invasions, Web experience and the user's skills with the Web.*
2. How does the degree of online privacy concern affect user's behavior?
   Measures such as *cancelled user online spending* and *refraining from Web surfing for privacy reasons,* together with *the volume of online spending* were used to study this issue. By doing so, it was possible to verify to what extent online privacy is a real or a perceptual problem in Web commerce.

These two questions were operationalized using eight research hypotheses, as follows.

To bridge the gap between the need for privacy on the one hand and the lack of regulatory protection on the other hand, a plethora of privacy enhancing mechanisms has been introduced (Bennett, 2000; Wayner, 1999). The first hypothesis focuses on the effect of the use of privacy enhancing technologies (Huaiqing, et al., 1998), on the level of online privacy concern:

H1: *There is a positive relationship between the use of privacy enhancing technologies (privacy policy, anonymizers and privacy seals of approval) and the degree of privacy concern.*

According to Foxman and Kilcoyne (1993), consumers' perceptions of privacy (and its violations) also depend on their unique social and personal experience. The following hypothesis is aimed at empirically testing this:

H2: *There is a positive relationship between previous experiences with online privacy invasions and the degree of privacy concern.*

People who start to navigate the Internet and don't have prior web experience, or have few web skills, or posses low web usage, may have a higher degree of online privacy concerns. In order to verify this, the following hypotheses were postulated:

H3: *There is a negative relationship between the degree of privacy concern and the level of Web usage.*

H4: *There is a negative relationship between the degree of privacy concern and the user's Web skills.*

H5: *There is a negative relationship between the degree of privacy concern and the user's experience with the Web.*

Novak et al. (2000) express their belief that consumers do not trust most Web providers enough to engage in relationship exchanges involving money and personal information. Moreover, online privacy concerns cannot only inhibit purchasing activity on the Internet, but also inhibit surfing activities. Based on the above, the following hypotheses were formulated:

H6: *A high degree of privacy concern implies higher numbers of users canceling online spending for privacy reasons.*

H7: *A high degree of privacy concern implies higher numbers of users refraining from surfing onto certain Web sites for privacy reasons.*

H8: *There is a negative relationship between the degree of privacy concern and the volume of online spending.*

4 RESEARCH DESIGN

Data for this study were collected by means of a Web-based online questionnaire. The questionnaire included seven parts.

- Part A – *Degree of online privacy concern,* consisted of 16 scenarios that were derived from previous studies and represented the five dimensions of online privacy concern (awareness of information collection, information usage, information sensitivity, familiarity with entity and compensation) (Bartel & Grubbs, 1999, 2000).
- Part B – *Web usage,* measured by a construct adopted from Igbaria (1990), and comprised of two items: actual daily usage and frequency of use.
- Part C – *Usage of privacy enhancing technologies,* included six items adopted from Igbaria (1990), focusing on the existence of privacy policy, seals of approval and anonymizers.
- Part D – *Experience with the Web*, consisted of a set of constructs adopted from Igbaria (1990) and Novak, Hoffman & Yung (2000), taking into consideration the following online activities: e-mail, navigation, online purchases, newsgroups and chats.
- Part E – *Web skills,* comprised of a set of items for the skill construct (Novak et al., 2000), where the respondents were asked to express their assertions about their Web skills.
- Part F – *Factors affected by the degree of*

online privacy concern, focused on possible influences of privacy concerns in the user's behavior, including cancelled online spending, volume of online spending and refraining from Web surfing for privacy reasons.

- Part G – *Demographic information* captured information regarding respondent's gender, age and education.

The instrument was designed as a Web fill-out form and was posted on the Internet. A request to fill the questionnaire, along with the URL of the survey was sent by e-mail to 950 graduate business students at Tel Aviv University. The request was also distributed to 200 computer users in a major international company in the communication sector. In total, 1150 requests were distributed by email and 217 responses (159 students and 58 practitioners) were received. The total response rate was 18.9%.

No demographic differences (gender, education and age groups) were found between the students and the company respondents.

5 FINDINGS

(a) Degree of online privacy concern

Online privacy concern was measured using five dimensions: awareness of information collection, information usage, information sensitivity, familiarity with entity and compensation (Bartel & Grubbs, 1999, 2000; Cranon, et al., 1999). Table 1 depicts the means and standard deviation of each of the five dimensions (1-7 scale) and a meta-variable representing the degree of online privacy concern (aggregation of the five dimensions).

Inter-correlations between each of the five individual dimensions as well as correlation coefficients between these dimensions and this meta-variable, representing the degree of online privacy concern, were found to be significantly correlated (p<0.001).

(b) Hypotheses testing

H1 suggests that there is a positive relationship between the use of enhancing privacy technologies and the degree of privacy concern. A Pearson correlation test supports this hypothesis (r=0.182, p=0.007), indicating that when the degree of online privacy concerns increases, the use of privacy enhancing technology also increases.

H2 suggests that there is a positive relationship between *previous experience with online privacy invasions* and the degree of *online privacy concern.* The results indicate that respondents who experienced previous online privacy invasions exhibited higher levels of online privacy concerns (mean=4.73, compared to 4.05 for respondents who did not encounter online privacy invasions in the past). An ANOVA test further supported this hypothesis (F=22.7, p=0.001).

H3 suggests that there is a negative relationship between the *degree of online privacy concern* and the *level of Web usage* (that is, the more the user uses the Internet, the less he/she is concerned with online privacy). However, when testing H3, the relationship was found to be on the opposite direction than expected - the more the user uses the Internet, the more he or she is concerned with online privacy (*r*=0.189, p=0.005).

Table 1: Descriptive statistics of the five dimensions of online privacy concern construct

	Average	Standard Deviation
Awareness of information collection	4.12	1.38
Usage of information	4.44	1.52
Compensation	4.14	1.52
Sensitivity of information	4.63	1.59
Familiarity with the entity	3.98	1.56
Degree of privacy concern	**4.26**	

H4 asserts that the more *Web-skilled* the user is, the less he or she is concerned with *online privacy.* H4 could not be accepted since no significant relationship between *the degree of privacy concern* and *the user's Web skills* was found (r=0.032, p=0.636).

H5 suggests that there is a negative relationship between the *degree of privacy concern* and the *user's experience with the Web* (the more experienced the user is, the less he or she is concerned with online privacy). Correlation test results provided no evidence for such a relationship (r=0.079, p=0.249), so this hypothesis could not be accepted.

H6 stated that a high degree of *online privacy* *concern* implies *higher volumes of user cancelled online spending*. A Pearson correlation test did not reveal significant results (p=0.735, r= -0.157). Thus, this hypothesis was not supported and could not be accepted.

H7 suggests that *a higher degree of online privacy concern* implies a *higher level of refraining from surfing to certain Web sites*. A Pearson correlation revealed a significant correlation between the two variables (r=0.663, p=0.001), thus hypothesis H7 was accepted.

H8 states that there is a negative relationship between the *degree of privacy concern* and the *volume of online spending (*the more the user is concerned with privacy, the less he or she is going to spend in e-commerce). Based on a correlation test (r=-0.024, p=0.735), hypothesis H8 could not be accepted.

6 CONCLUSIONS

This study attempted to gain a better understanding of the privacy concern. Among its findings, the novelty of the Internet environment by itself was found not to affect the *degree of online privacy concern*, meaning that *web skills* and *experience with the web* were not related to the degree of that concern. On the other hand, *web usage* and the *degree of online privacy concern* were found to be positively related.

The study found that people who suffered previous online privacy invasions were likely to purchase much less than persons who didn't suffer any previous online privacy *invasion.* Also, people with a high degree of online privacy concern were *more* likely to refrain from surfing in specific sites for privacy reasons, and to purchase less products and services online.

The results of this study imply some efforts that should be taken by governments, businesses and individuals in order to protect privacy and enable online transactions. These include:

- *Voluntary observance of fair information practices including the role of trade associations:*

Since persons with previous experience of online privacy invasions have higher levels of online privacy concern, the observance of fair information practices is vital..

- *Technological approaches:*

Today's privacy enhancing technologies are primitive in nature. Such technologies are often cumbersome to use, unfriendly and require a degree of knowledge exceeding that of the common Internet consumer. The low *level of usage of privacy enhancing technologies* found in this study evidence this fact. Consequently, new, user-friendly, technology-based approaches should be developed to provide consumers with a greater control over the disclosure of their personal information.

- *Government as a customer:*

The government can impact privacy concerns through market forces, promoting strong privacy laws for both the public and private sectors, establishing independent privacy commissions to oversee the implementation of these laws, educating the public about privacy issues and encouraging business self-regulation. In addition, the government is also a major customer and has an opportunity to influence the private sector through its e-procurement policies.

REFERENCES

Bartel, S.K., & Grubbs, H.M. (2000). Dimensions of privacy concerns among online consumers**.** *Journal of Public Policy & Marketing*, *19*(1), Spring, 62-73.

Bartel, S.K., & Grubbs, H.M. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns**.** *Journal of Advertising*, *28*(3), Fall.

Bennett, M. (2000). Online privacy: Europe and America. *Giga Information Group*, Giga World IT Forum 2000, 47461-MB99.

Cranon, R., Reagle, C.J., & Ackerman, H. (1999). Beyond concern: Understanding net user's attitudes about online privacy. *AT&T Labs Technical Research Report TR99.4.3*, April.

Foxman, R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing*, *12*(1), Spring, 106-119.

Hatch, O.G. (2000). *Privacy in the digital age: A resource for Internet users*. U.S Senate Judiciary Committee. http://judiciary.senate.gov/privacy.htm

Huainqing, W., Matthew, K.O.L., & Chen, W. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, *41*(3), March, 63-70.

Igbaria, M. (1990). End-user computing effective-ness: A structural equation model. *Omega, 18*, 637-652.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, *26*, March, 323-338.

Novak, T.P., Hoffman, D.L., & Yung, Y. (2000). Measuring the customer experience in online environments: A structural modeling approach. *Marketing Science, 19*(1), Winter, 22-42.

Wayner, P. (1999). Technology for anonymity: Names by other Nyms. *The Information Society, 15*(2), 91-97.