Information Privacy and Security Considerations in Internet Marketing Research

***Tsiakis, T., Kargidis, T., Belidis, A.**
Alexandrian Technological Educational Institute of Thessaloniki (ATEI), Dept. of Marketing, Greece, P.O Box 141, 57400 Thessaloniki

*Corresponding author E-mail: tsiakis@mkt.teithe.gr

Abstract:*Understanding and protecting personal privacy in information systems is becoming increasingly critical with widespread use of networked systems and the Internet. Individuals have become more concerned about handling of personal data, secure purchasing patterns and targeted marketing and research. In this regard, the purpose of this study is to examine the effect of privacy and perceived security as means to improve internet marketing processes and research. The current study is designed to research the relationships of closely related terms such as information privacy and security towards internet marketing and research processes. Thus, it aims to add theoretical and managerial insights in helping understand how an internet retailer can boost business and consumer satisfaction by an increased level of privacy and trust via internet marketing practices.*
Keywords: *Information Security, Privacy, Marketing Research*

1. INTRODUCTION

The plethora of technological advances makes obtaining collection, storing, distribution and analysis of vast amounts of information about consumers easier than ever before. This affluence of data/information consequence in privacy issues (Tsarenko and Tojib, 2009). Privacy consist the primary concern obstructing people from engaging in e-commerce transactions due to the risk involved in disclosing Personally - Identifying Information (PII), like email addresses or credit card information, which is required for most e-commerce transactions (Metzger, 2007). In the e-commerce field two main privacy paradigms exist (Bella et al., 2011):

- The one side concerns the customer's trust that the network conforms to his privacy policy
- The other side is based on anonymity, meaning that data/information are related with a pseudonym and not with the real identity of customer

E-commerce technologies alter the kind of relationships that businesses have with consumers because in difference with classical-traditional direct marketing channels, the internet medium is based on a combination of technologies, protocols and services that allocate the ways in which one part of one relationship may invade the privacy of another (Castañeda et al., 2007). These privacy concerns are heightened especially in the electronic space exactly because consumers are feeling "uninformed about who is collecting their personal information, how companies obtain their information, or for what purposes the information is used" (Youn, 2009). Poddar et al. (2009) have categorized privacy concerns for consumers in two dimensions:

- environmental control - "the consumer's ability to control the actions of other people during a market transaction"
- secondary use of information control - "the consumer's ability to control the dissemination of information related to or provided during such transaction or behaviors to those who were not present"

2. CONCEPT OF INFORMATION PRIVACY

Current security/privacy issues like identity theft, use of unauthorised information, stolen credit card numbers etc bring in the surface personal privacy concerns and that "because concerns with privacy are closely associated with the notion of personal freedom as a basic consumer right" (Tsarenko and Tojib, 2009). Privacy is a dynamic process and privacy concerns do not parallel privacy practices (Hsu, 2006). Privacy concerns are present in different internet contexts like direct and database marketing and particularly are the basic reason that people are not ready to participate in online environment. Privacy concern is defined "as customer's concern for controlling the acquisition and subsequent use of the information that is generated or acquired on the internet about him or her" (Castañeda et al., 2007). Online privacy concerns make consumers circumspect and reluctant to provide personal information online, to repudiate e-commerce, or further incommunicative to use the Internet (Wu et al., 2012). Tsai et al. (2011) in their paper mention that the prime dimensions of consumer privacy concerns are four: collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information and in online marketing, these dimensions of concern are attributed as "the collection of personal information, control over the use of personal data, and

awareness of privacy practices and how personal information is used". Anton et al. (2010) established a baseline of Internet users' privacy concerns comprised of six dimensions.

1. personalization,
2. notice/awareness,
3. information transfer,
4. information collection,
5. information storage, and
6. access/participation;

Hsu (2006), ideally state that "researchers study what is privacy (the nature of privacy), the activities that infringe on privacy (privacy risks), how to protect privacy (privacy protection), and people's perception of privacy (privacy concerns)". Moreover Pan and Zinkhan (2006) revealed that research has studied privacy issues from different perspectives such as "how consumers respond to such concerns, consumer willingness to provide personal information, the effect of trust (in the organization) on customers' willingness to provide information, consumer awareness of privacy mechanisms and the contents of privacy disclosures and legal and ethical issues associated with online privacy". The growth of the internet and the attended usage of information media have increased privacy concerns leading researchers to identify that due to that, three primary privacy issues arise (Spake et al., 2011):

1. identification of consumers while they are online;
2. increased unsolicited marketing contacts directed at consumers; and
3. access to customer data by third parties that have had no contact with the consumer

According to Culnan and Bies (2003) three different perspectives on consumer privacy have emerge:

- the corporate perspective – advocating that any restrictions placed on the corporation's ability to access consumers personal information astrict the corporation's ability to operate efficiently in the marketplace]
- the activist perspective – highlight the issue that if both free-market forces and technological advances are left uncontrollable, then information will be conducted by anyone for any purposes, which will violate the fundamental right to privacy
- centrist perspective – this is the golden mean between the corporate and activist perspectives meaning that there must be consumer oriented choices concerning corporate access to personal information.

(O'Neil, 2001) in a review of the literature identified that consumer privacy protection on the Internet is a growing concern for the three following parts: public, business community, and legislators. In our paper the players (conciliating parties) of privacy are: Consumers, business, government and technology (Figure 1)

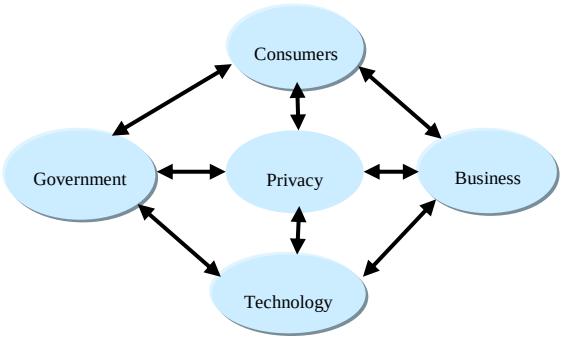

Figure 1: Privacy Players

2.1 Information Security component

Security and privacy concerns weren't an intrinsic value on web; it came much later, with the proliferation of business, marketing, government, etc. Often, erroneously security and privacy are thought of as one and the same but they deal with separate issues. We have to understand that security and privacy issues are closely related, separate but not (e.g. privacy cannot exist without security). Security is a balance between protecting information (organizational assets) and enabling authorized access (prevent/grant access) (Post and Kagan, 2007). The appropriate level of security for consumer data is conditioned by "the degree to which managerial and technical processes exist that restrict unauthorized access or improper use of the data, the potential for loss or destruction of the data, or the accidental or improper provision of the data to others" (Peltier et al., 2010). Security policies are tools used for the implementation of organizational security in two different contexts a) computer/network security and b) information security management (Goel and Chengalur-Smith, 2010).

3. RELATION OF MARKETING RESEARCH WITH PRIVACY AND SECURITY

Marketing is based on the ability the ability to obtain targeted information (e.g. e-mail, phone numbers). Technology provides the efficient means (of communication) by which the process of marketing can occur and distribution channels provide the motivation for the development and utilisation of marketing (Hamilton and Spiller, 1999). Technology enabled firms to explore new applications like data mining, target marketing setting them capable of moving towards one-to-one marketing, delivering cost-effective customized services (Wirtz et al., 2007). Every user's every movement in the internet place is a piece of marketing information. The commercially accepted ways by which businesses gather information on Web users are according to Prabhaker, (2000):

1. through registration – where firms record personal information and address the issue of contact
2. through capturing and collecting the electronic addresses of the Web users – web addresses along with specific pages viewed and the sequence in which these pages are viewed are recorded and stored in a database - web preferences are tracked and stored in file on the user's hard disk
3. through gathering information on customers by using cookies -

(Castañeda et al., 2007) mention that practice of firms on the Internet by obtain information either by compiling navigation details (e.g. recording access to the web site) or by asking the customer (e.g. surveys). The redefinition and modulation of the marketing and advertizing process (more informative), due to the advancements of internet, leads consumers to be more uncertain of marketing/advertising means as privacy-invasive or overly intrusive, because consumers are afraid of being tracked too closely by companies and in consequence companies using this information to recondition prices (Tucker, 2012). In a commercial environment the privacy is about ameliorate the conditions of consumers disclosing the personal information needed for relationship marketing (Culnan, 2000). According to O'Neil, (2001) the threats to one's privacy on the Internet can be either immediate or future due to the fact that online activities can be a) monitored by unauthorized parties and b) logged and preserved for future access.

Marketers according to Nowak and Phelps (1995) use consumer information in three major ways:

1. to segment or profile markets and audiences
2. to create, personalize, or direct persuasive messages and advertising and
3. for financial gain.

The details gathered (about individuals, groups or institutions) are concerning issues like (Hewett and Whitaker, 2002):

- who they are or were;
- where they are or have been;
- what they do or have done; and
- when it happened, is happening or will happen.

Information privacy issues embrace both the type of information collected and the intended use and control of this information (Hamilton and Spiller, 1999), (Groene et al. 2011). In a marketing context, information privacy concern refers to "the extent to which a person is worried about the practices of an organization regarding the collection and subsequent use of his or her personal information" representing two facets a) consumers are anxious about potential obnoxious conducts of information collection and b) worried about the honesty of their interaction with a marketer concerning their information (Groene et al. 2011).

Prabhaker (2000) found that there are three specific implications regarding how consumer privacy concerns impact the sales of goods and services.

1. there is the opportunity cost of lost sales – meaning that if consumers privacy anxieties /concerns has not been resolved they will decrease the volume of online transactions or further diverge.
2. there is the shift in demand from online to off-line business channels – some apprehensive customers will converge to familiar traditional ways of purchasing, even if that means paying more due to privacy dysphoria for internet transactions.
3. privacy concerns represent an intangible cost component for those who do business over the Internet – that is if the intangible privacy cost can be minimized or removed, the online demand will be higher.

Canhoto (2009) studying the marketing literature found that there are some (although limited) insights of factors (Attitudes/ Information use/ Policies/ Process design/ Systems of checks and controls/Training initiatives) that explain why failures to protect customers' privacy continue to exist while there is a broad regulation and various technical solutions available. Furthermore, the findings of the combination of the various factors and the dynamics are pictured in the Table 1 explaining that legal tools outline obligations and frame expectations, technical control access and employee enforce measures in order to be effective.

Table 1: Role of regulation, technology and employees on safeguarding customer data

Category	Effect	Observation
Legal	Outlines obligations and expectations	Must be clear, relevant and enforceable
Technical	Reduces variability by controlling access and anonymising data	Has limited application
Employee	Attitudes have major impact on behaviour. Training is necessary but not sufficient	Behaviour is shaped by job requirements and reward schemes, as well as group norms and mental schemes

Source: Canhoto, (2009)

4. REFLECTIONS OF SOLUTIONS

Industry, as (S.E. Kruck, Danny Gottovi, Farideh Moghadami, Ralph Broom, Karen A. Forcht, (2002) "Protecting personal privacy on the Internet", Information Management & Computer Security, Vol. 10 Iss: 2, pp.77 – 84) mention is trying with every way to avoid government privacy regulation in part because it is apparent that it will lose a marketing advantage and/or a significant interest of money by converting personal information into value among companies. It is obvious that market alone, by self regulation is not sufficient enough to solve the privacy problem, it must engage in seeking a solution.

There is a constant trade-off that consumers make between privacy and benefits (e.g. customization that requires personal and transaction-type information) (Wirtz et al., 2007). The target should be to achieve a balance between business information benefits and consumer rights. The collection and use of information have to be guided by a set of internal values that are applied within the cultural expectations and legal environment of the countries in which the certain organisation/company operates (Bradford, 2007). The control measures (privacy or/and security) that could be adopted in relation to the internet (online field) can come from essentially two channels, the government law and the by the ethics of the organisations (these indicate the difference between the protection established by the EU and the US respectively) (Castañeda, 2007).

Difference exists between how USA and EU view the concept of privacy. Characteristic is the reference of Wirtz et al., (2007) where "in the USA, "privacy" is used to include everything from anonymity, to control over personal information, and to limiting government intrusions into the home and in Europe, the term more commonly used is "data protection," and today, the various terms tend to be used synonymously worldwide".

Hsu (2006) found in her research that the solution of privacy may be a situational paradigm (Table 2)

Table 2: Two paradigms of privacy research

	Adversarial paradigm	Situational paradigm
The nature of privacy	1. Being let alone (Liberty) 2. Being alone (Solitude) 3. Psychological privacy/accessibility (autonomy) 4. Accessibility limited in certain context (secrecy)	Natural and normative privacy
Privacy protection	1. Non-intrusion theory 2. Seclusion theory 3. Control theory 4. Limitation theory	Control/restricted access theory of privacy
Privacy risk	Data user v. data subject	Contexts Sectors (Website category) Technology data
Privacy concerns	Data user v. data subject	Privacy concerns/privacy practices Individual contexts: demographics Social contexts: Culture Social group Policy regulations Space/place Websites' performance/category

Source: Hsu, (2006)

To gain and furthermore to retain consumer trust, web merchants must prove to (potential) customers that PII obtained through e-commerce transactions will remain secure. And these can be done by two security mechanisms (Peterson, et al., 2007):

1. privacy policy statements - self-reported guarantee or a privacy policy statement
2. third-party seal verification programs – third party seals (graphics) are displayed on a web site to verify that the certifying organization has examined the privacy policy

Kruck et al. (2002) lastly suggest that until perfect legislation or the perfect socially responsible corporation exists, individual at a personal level, should take measures to ensure their personal privacy in three major areas:

1. e-mail privacy - an individual can use some type of encryption software packages like Pretty Good Privacy (PGP) to ensure only the intended recipient can read the message
2. access and security – there are many tools (with payment, free or freeware) to prevent from privacy threats from cookies, http, browsers, search engines, e-mail, and spam.
3. personal information and unsolicited marketing – precaution measures in protecting the confidentiality of your PII as social security number, securing, inspection and correction of files concerning PPI, confirmation of the address of the merchants site (uniform resource locator - URL) etc.

References

Antón, A., Earp, J. and Young, J. (2010) "How Internet Users' Privacy Concerns Have Evolved since 2002", *IEEE Security and Privacy*, Vol. 22, No. 2, pp. 21-27.

Bella, G., Giustolisi, R., Riccobene, S. (2011) "Enforcing privacy in e-commerce by balancing anonymity and trust", *Computers & Security*, Vol. 30, No. 8, pp. 705-718.

Bradford, M. (2007) "Personal credit information Privacy and information security issues − the Experian view", *Business Information Review*, Vol. 24 No. 4, pp. 253–256.

Canhoto, A. (2009) "Safeguarding customer information: the role of staff", *Journal of Consumer Marketing*, Vol. 26 No. 7, pp. 487–495.

Castañeda, A., Montoso, F., Luque, T. (2007),"The dimensionality of customer privacy concern on the internet", *Online Information Review*, Vol. 31 No. 4 pp. 420 – 439.

Culnan, M., & Bies, R. (2003) "Consumer Privacy: Balancing Economic and Justice Considerations", *Journal of Social Issues*, Vol. 59 No. 2, pp. 323-342.

Goel, S. & Chengalur-Smith, I. (2010) "Metrics for characterizing the form of security policies", *Journal of Strategic Information Systems*, Vol. 19 No. 4, 281–29.

Groene, N., von Wangenheim, F., Schumann, J. (2011) "Interest-Based Internet Advertising and Privacy Concerns: How to Increase the Acceptance of a Rising Marketing Phenomenon", *in Proceedings of the Productivity of Services Next Gen - Beyond Output/Input*, 7-10 September 2011 Hamburg, Germany.

Hamilton, R. & Spiller, L. (1999), "Opinions about privacy: Does the type of information used for marketing purposes make a difference?", I*nternational Journal of Non profit and Voluntary Sector Marketing*, Vol. 4 No. 3, pp. 1465–4520.

Hsu, C. (2006) "Privacy concerns, privacy practices and web site categories: Toward a situational paradigm", *Online Information Review*, Vol. 30 No. 5, pp. 569 – 586.

Kruck, S.E., Gottovi, D., Moghadami, F., Broom, R., Forcht, K. (2002) "Protecting personal privacy on the Internet", *Information Management & Computer Security*, Vol. 10 No. 2, pp.77–84.

Metzger, M. (2007) "Communication Privacy Management in Electronic Commerce", *Journal of Computer-Mediated Communication*, Vol.12 No. 2, pp.335–361.

Nowak, G., Phelps, J. (1995) Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters, Journal of Direct Marketing, 9(3), 46–60

O'Neil, D. (2001) "Analysis of Internet Users' Level of Online Privacy Concerns" *Social Science Computer Review*, Vol. 19 No.1. pp. 17-31.

Pan, Y., & Zinkhan, G. (2006) "Exploring the impact of online privacy disclosures on consumer trust", *Journal of Retailing*, Vol. 82, No. 4. pp. 331-338.

Peltier, J. Milne, G., Phelps, J. and Barrett J. (2010) "Teaching Information Privacy in Marketing Courses: Key Educational Issues for Principles of Marketing and Elective Marketing Courses", *Journal of Marketing Education*, Vol. 32 No. 2 pp. 224–246.

Peterson, D., Meinert, D., Criswell II, J., Crossland, M. (2007) "Consumer trust: privacy policies and third-party seals", *Journal of Small Business and Enterprise Development*, Vol. 14 No. 4, pp.654–669.

Poddar, A., Mosteller, J. and Ssholder E. P. (2009) "Consumers' Rules of Engagement in Online Information Exchanges", *Journal of Consumer Affairs*, Vol. 43 No. 3, pp. 419-448.

Post, G. & Kagan, A. (2007) "Evaluating information security tradeoffs: Restricting access can interfere with user tasks", *Computers & Security*, Vol. 26 No. 3, pp. 229-237.

Prabhaker, P. (2000),"Who owns the online consumer?", *Journal of Consumer Marketing*, Vol. 17 No. 2, pp. 158–171.

Spake, D., Finney, Z., Joseph, M. (2011) "Experience, comfort, and privacy concerns: antecedents of online spending", *Journal of Research in Interactive Marketing*, Vol. 5 No. 1, pp. 5–28.

Tsai, J., Egelman, S., Cranor, L., Acquisti, A., (2011) "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", *Information Systems Research* Vol. 22, No. 2, pp. 254–268.

Tsarenko, Y, & Tojib, D. (2009) "Examining customer privacy concerns in dealings with financial institutions", *Journal of Consumer Marketing*, Vol. 26 No. 7, pp.468 – 476.

Tucker, C. (2012) "The economics of advertising and privacy", *International Journal of Industrial Organization*, Vol. 30, No.3, pp. 326-329.

Hewett, W.G., & Whitaker, J. (2002) "Data protection and privacy: the Australian legislation and its implications for IT professionals", Logistics Information Management, Vol. 15 No. 5/6, pp.369-376.

Wirtz, J., Lwin, M., Williams, J. (2007) "Causes and consequences of consumer online privacy concern", *International Journal of Service Industry Management*, Vol. 18 No. 4, pp. 326–348.

Wu, K., Huang, S., Yen, D., Popova I. (2012) "The effect of online privacy policy on consumer privacy concern and trust", *Computers in Human Behavior*, Vol. 28 No. 3, pp.889–897

Youn, S. (2009) "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents", *Journal of Consumer Affairs*, Vol. 43 No. 3, pp. 389–418.