ISBN: 978-93-90847-08-2

4. Privacy of an Online Consumer

Prof. Dr. C. B. Senthil Kumar

Head, of the Department Commerce,
Dr. M. G. R. Educational,
and Research Institute University,
Chennai, TamilNadu, India.

Abstract:

The purpose of this paper is to pose questions on the factors influencing Indian customers' internet privacy concerns. Perceived vulnerability to illegal acquisition and use of personal information was found to have a positive effect on Indian consumers' online privacy concerns, while perceived control over the collection process and use of information was found to have a negative effect. Consumers in India were less likely to share personal information online due to a heightened awareness of the potential risks associated with doing so, and they were more likely to provide misleading information if solicited for their details. Managerial approaches to easing customers' worries about their personal information online are examined with the goal of making India's online merchants more competitive.

Keywords: *Online Privacy, Information Privacy, E-Commerce.*

4.1 Introduction:

The fact that consumers must reveal personal information (such their date of birth, social security number, home telephone number, credit card information, etc.) when engaging in electronic commerce (e-commerce) transactions raises privacy concerns.

Therefore, ensuring the privacy of customers is crucial to the growth of the e-commerce industry (Liu et al. 2004). However, in order to better understand what customers, want, it is essential for online businesses to collect data on them. Managers face a difficult task, then, in gathering the customer data essential to maximizing sales and profits. Managers must take precautions to protect the privacy of their customers or face public criticism. [1]

4.2 Definition of Consumer Privacy and Reasons for Consumer Privacy Leakage:

Since the idea of privacy touches on so many subfields of sociology, it is necessarily broad. However, experts in various fields have not yet settled on a single, uniform definition of privacy. As one gains life experience, their understanding of what constitutes private space expands and contracts. It's an overlap concept that is discreet, private, anonymous, risk-free, and morally sound.

For online shoppers in the age of big data, the traditional meaning of privacy is shifting from information deemed too sensitive for an individual or group to let others know (such as health and financial details) (such as id number and daily life tracks).

According to the aforementioned definition of consumer privacy, the viewpoint of this study on consumer privacy leakage is situations in which any information relating the identity of consumers, and thus having any economic worth, was misused, deliberately stolen, or unlawfully exchanged.

Lack of personal information protection consciousness, the astonishing economic worth of privacy information, and the imperfections of the appropriate legal framework all contribute to the massive scale and depth of the problem that is consumer privacy leakage.

The aforementioned causes will push internet retailers to adopt biased privacy policies that serve their own interests over those of their customers. [2]

4.3 Current Situation of Privacy Protection:

Safeguarding users' personal information while they're online is also a major concern right now. Online consumer privacy protection faces formidable opposition due to a lack of privacy protection technologies and related legislation on e-commerce platforms.

The following theoretical ideas inform the recommendation of the three research categories depicted in Figure 4.1:

- A trust model provides a comprehensive overview of the factors that contribute to the growth of trust in a given online setting. These models offer a theoretical basis for comprehending the phenomenon of online trust, which is highly contextualized and hence difficult to study in isolation.
- Consumers' capacity to make a transaction in a safe environment is an example of a technological component that reflects a cognitive approach to trust. These elements are in keeping with the idea of institutional trust, which holds that people are more likely to take precautions when they can place their faith in established authorities and procedures (Bachmann & Inkpen, 2011). [3]
- The affective approach to trust is represented by the social elements, which characterize the feelings and opinions that users have about a website's reliability.

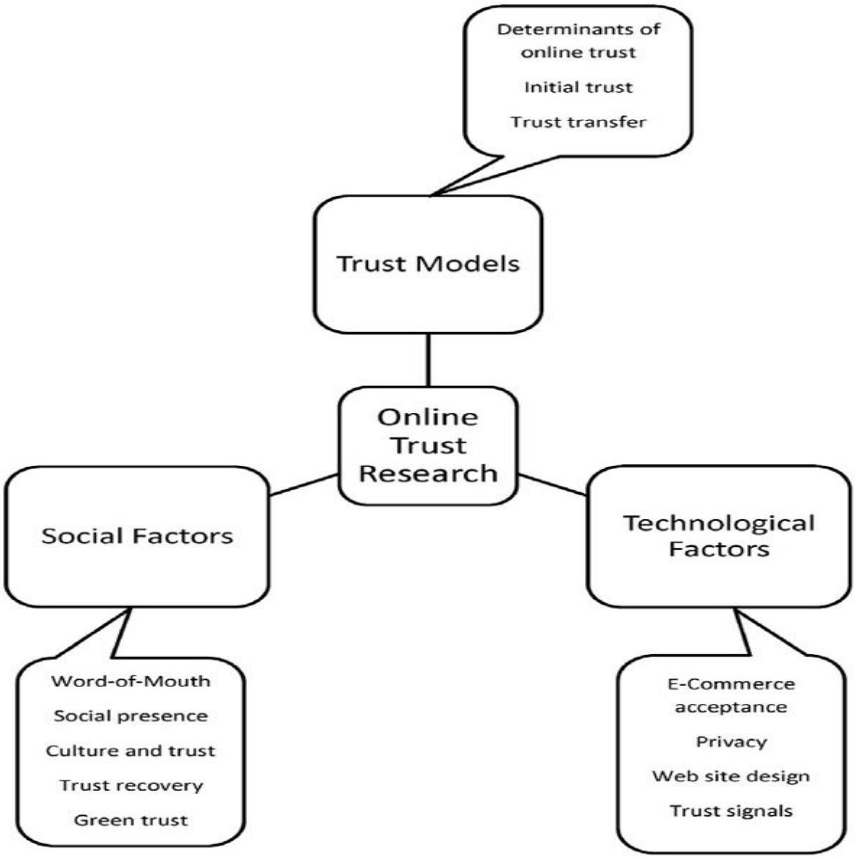


Figure 4.1: Main Categories of Online Trust Research

4.4 Objectives:

- Strengthen your online privacy settings across the board.
- Reduce shoppers' worries about their personal information being shared.
- Thirdly, research into the personal information shielded by the internet.
- Research on measures that might be used to safeguard shoppers from fraudulent internet retailers.

4.5 Research Methodology:

We employed a variety of secondary sources, such as books, educational and development publications, government papers, and print and online reference resources, to understand the make-up, use, and implications of online consumer privacy.

This study makes a novel suggestion for applying the theory of differential privacy technology and its current practical implementations to the problem of safeguarding customers' personal information on e-commerce sites.

E-commerce has emerged as one of the most important venues for modern data mining and processing, and differential privacy technology benefits from the added layer of privacy ambiguity it provides. Bringing these two together is a natural next step in the big data era's evolution.

4.6 Review of Literature:

As online shopping has become more commonplace, more and more scholarly works have been published on the topic. The focus of studies shifts from the inner workings of the various business platforms to the development of lasting connections with customers.

However, publications that seek to summarize and evaluate existing research are uncommon and sometimes inadequate. With an emphasis on articles published in IS (Information Systems) journals between 1997 and 2003, Wareham, Zheng, and Straub (2005) provided an overview of the most important topics related to electronic commerce.

Reviewing the literature on e-commerce published between 1999 and 2008, Wang and Chen (2010) found that attention has switched from technological issues to managerial ones. [4-5]

Greenaway and Chan (2005) categorized the depths to which privacy studies delve as follows: personal (consumer/employee), business, and government. Researchers have looked into consumers' thoughts and feelings regarding privacy on an individual basis (Culnan 1993; Sheehan and Hoy 2000).

Information privacy in relation to organizational liability, decision outcome, and ethical necessity are all key topics that have been studied at the organizational level (Greenaway and Chan 2005). Information privacy concerns across sectors and nations have been addressed at the sectorial and national levels (Earp et al. 2002). The focus of this research is on individual privacy concerns. [6-8]

A key threat to e-commerce and the digital economy is the fear of, or reluctance to give, personal information (Culnan 2000; Malhotra et al. 2004). One of the most important determinants of privacy apprehensions was the degree to which individuals felt they could manage their own information (Xu et al. 2012).

Consumers may worry about the websites they visit and the personal information they share with those websites, as well as the websites' management of that information (Hong and Thong 2013).

Online shoppers' confidence in services may be affected by factors like their gender, age, and level of education (Riquelme and Roman 2014).

The level of privacy concern among consumers is largely determined by their familiarity with the practices of data gathering and its application beyond the scope of the initial transaction (Sheehan and Hoy 2000).

Self-regulation within industries and procedural fairness are both examples of measures made to safeguard individual data (Culnan 2000; Culnan and Armstrong 1999).

However, the effectiveness of these kind of safeguards for personal privacy is highly questionable. Consumers have resorted to their own methods of privacy protection due to widespread fears over their personal information being compromised.

Consumers' trust in online shopping has been steadily rising, according to a recent survey (Saunders 2004). Consumers have more faith in businesses because, despite privacy worries, they are learning to be more responsible when they shop online. [9-11]

The concept of privacy is nebulous at best. Collection of personal information, secondary use of personal information without consent, inaccurate personal information, and illegal access to personal information are the four aspects of consumer privacy issues outlined by Smith et al. (1996). (see also Stewart and Segars, 2002).

These factors have been understood to refer to the following in the context of internet marketing: the collecting of personal information, the exercise of control over the use of personal data, and knowledge about privacy practices and the ways in which personal data is utilized (Malhotra et al., 2004).

Consumers' worries extend to secondary data use without consent and data entry mistakes (as stated by Brown and Muchira, 2004). If the customer's worries are stoked by the store's actions, the customer may stop putting their faith in the store (Camp,2003).

According to Milne and Gordon (1993), businesses have a "implied social compact" to protect client data. When trust is broken between an organization and an individual, the victim may be entitled to monetary damages (Solove, 2006). The assurance of honest data handling, on the other hand, can ease customers' minds about divulging personal details (Culnan and Artmstrong, 1999; Dinev and Hart, 2006). [12-15]

Most Americans worry that firms may misuse the information they provide to gain competitive advantage, since they view their right to privacy as being "under significant threat" (CBS News, 2005). (Harris Interactive, 2001; CBS News, 2005; P&AB, 2005; Turow et al., 2005; Lebo, 2008; Consumer Union, 2008; Burst Media, 2009). Consumers' propensity to make online purchases or sign up for new websites may be influenced by these worries, according to polls (P&AB, 2005).

To allay customer fears, businesses have begun to use privacy policies (Culnan, 2000) and privacy seals (Benassi, 1999) to explain their data handling procedures. A survey found that 70% of respondents disagreed with the statement that "privacy rules are easy to grasp" (Turow et al., 2005), and even fewer actually take the time to read them (Privacy Leadership Initiative, 2001; TRUSTe, 2006).

Evidence also reveals that consumers do not fully grasp the significance of privacy seals (Moores, 2005). Multiple studies have shown that, in exchange for some type of compensation, the vast majority of people are prepared to disclose personally identifiable information (Acquisti and Gross lags, 2005a). Individuals are willing to give up some privacy in exchange for financial gain (Hann et al., 2007) or greater individualized experience in such situations (Chellapa and Sin, 2005). [16-20]

4.7 Result and Discussion:

Based on the findings of this study, researchers should assess the correlation between privacy and price sensitivity and hone in on the specific psychological and sociological aspects that influence a consumer's choice when privacy information is more easily accessible. Our findings also suggest that companies might utilize technology to promote the positive effects of their privacy policies and win over customers.

While subjects in the control circumstances tended to buy from the vendor offering the lowest price, we discovered that subjects in the privacy information condition were more inclined to make purchases from websites offering medium or high degrees of privacy (even when those sites charged higher costs). This suggests that people will demand a higher price for privacy if it becomes easier to obtain such data.

In addition, consumers were less likely to take privacy indications into account when making purchases when shown the identical indicators as those utilized for the privacy group but disguised as unimportant merchant attributes.

This proves that the observed behavior can't be ascribed solely to a preference for shopping on websites displaying appealing signs.

People who are exposed to the privacy information condition are more likely to make purchases from sites that display privacy indicators than those who are not.

The purpose of this research was, in part, to ascertain whether or not shoppers would prefer to make purchases from sites displaying privacy indications if they were made aware of such signs. This is demonstrated in Table 4.1 below.

Table 4.1: Comparison of the proportion of purchases made from sites

	Conditions		**Fisher's Exact *p***
	Condition 1: No Privacy Indicator	**Condition 3:** Privacy Information	
% of battery purchases made from sites with icons	11.1% n=2/18	77.8% n=14/18	<.0001
% of sex toy purchases made from sites with icons	16.0% n=4/25	66.7% n=14/21	<.005

The percentage of sales from sites that matched the privacy information symbols was compared between the two situations. We utilized Fisher's Exact test to determine if there was a statistically significant difference in these percentages.

Worries about privacy had a greater impact on risk perception than did concerns about security. Consumers' perceptions of danger may change as they grow familiarity with online activities; initially, they may have been overly cautious.

They may have taken preventative measures on their own to safeguard their anonymity on the internet. One such action could be giving fake information to websites that request identification details.

Concerns about security, on the other hand, can be traced back to evolutionary theory. A greater understanding and familiarity with the Internet may lead to a shift in these ideas.

Consumers are more inclined to take precautions when they are aware of the risks to their privacy, such as the prevalence of information-gathering technologies like spyware, malware, and adware.

Examples of preventative actions include setting up a firewall, downloading and installing virus definition files, using anti-spyware software, and so on.

By adopting precautions, shoppers can lessen the impact of their security worries and feel more comfortable engaging in e-commerce.

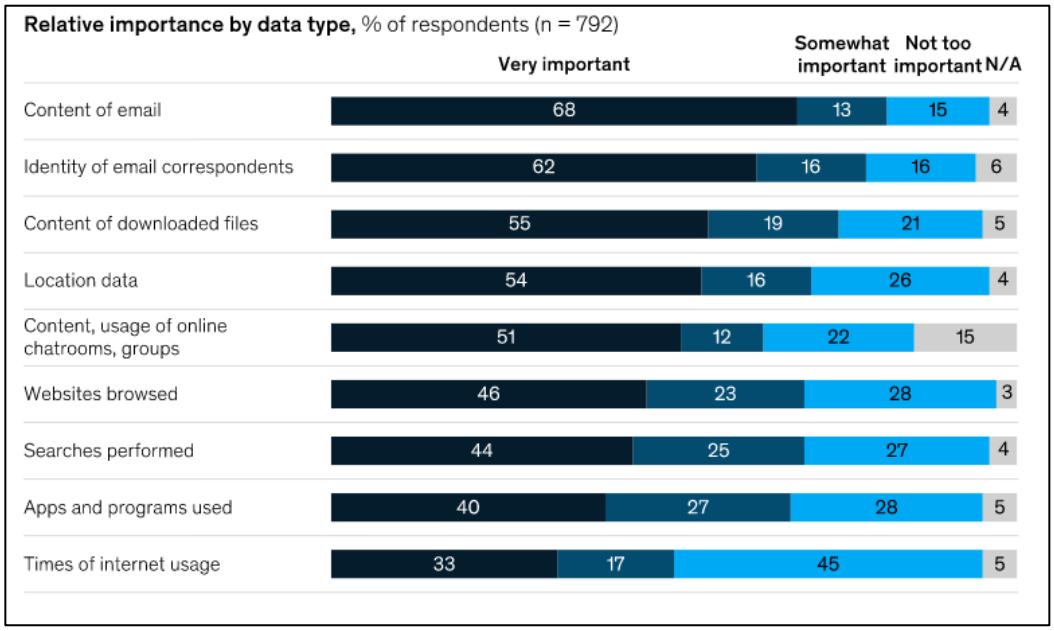
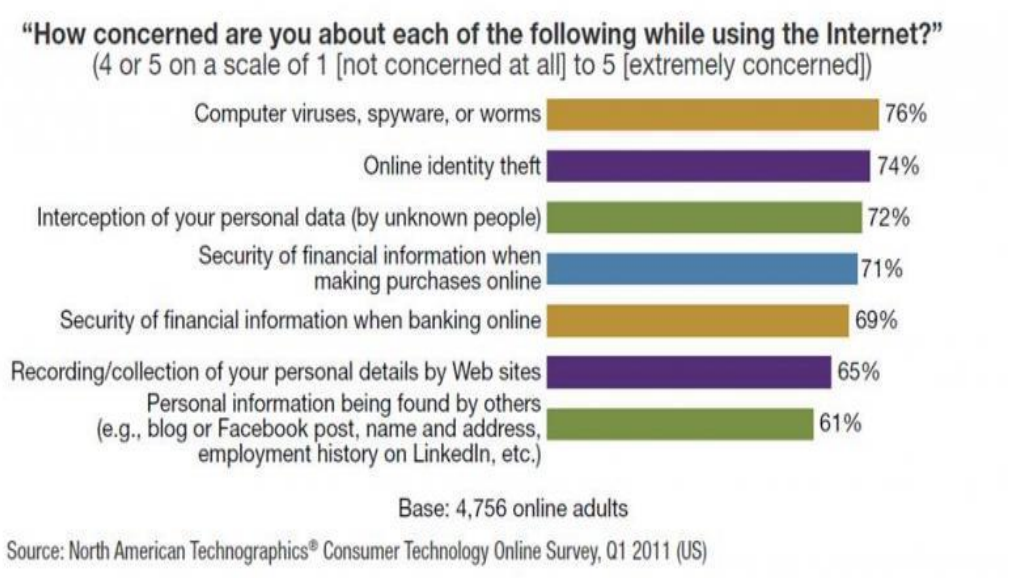


Figure 4.2: Consumer Privacy and Protection concerns vary by type of digital data

Source: Internet and American Life Project, Pew Research Centre

About half of those polled indicated they would have more faith in a firm if it asked for little more than necessary to provide service and asked just for information directly related to the products it offered. [21]



It's human nature to seek the path of least resistance, so if a customer feels compelled to disclose personal information but isn't sure how it will be used, they're likely to back out of the sale. To avoid losing customers because of this, businesses should figure out what data is essential and what data is great to have, and then design a system that doesn't need users to provide data that isn't essential. [22]

4.8 Conclusion:

The primary value of this review is that it reveals emerging themes in the study of trust in the context of Web 2.0 e-commerce from 2004 to 2014. Examining these tendencies can reveal new study opportunities and illuminate gaps in our understanding of online trust in the Web 3.0 era. Big data's meteoric rise has created both exciting new possibilities and formidable new challenges for the e-commerce industry. As mobile internet technology advances, it has been easier to access the internet's stored information; yet, this has led to an increase in the leakage of sensitive personal data, creating tensions that are more severe than ever before. One of today's most talked-about issues is the leakage of personal information. This article has done the following work to improve the consumer privacy security of this platform based on differential privacy technology, with an eye toward the existing state of consumer privacy security on the e-commerce platform.

4.9 Reference:

1. Liu, C., Marchewka, J., Lu, J., and Yu, C. "Beyond concern: a privacy-trust-behavioral intention model of electronic commerce," Information & Management (42:1), 2004, pp 127-142.
2. Liu Yahui, Zhang Tieying, Jin xiaolong, Cheng Xueqi. Personal privacy protection in the era of big data. Computer research and development. 2015 ,52（1) 229-247
3. Bachmann, R. & Inkpen, A. C. (2011). Understanding institutional based trust building processes in inter-organizational relationships. *Organization Studies, 32*(2), 281-301.
4. Wareham, J., Zheng, J. G., & Straub, D. (2005). Critical themes in electronic commerce research: a meta-analysis. *Journal of Information Technology*, *20*(1), 1-19.
5. Wang, C.-C. & Chen, C.-C. (2010). Electronic Commerce Research in Latest Decade: A Literature Review. *International Journal of Electronic Commerce Studies*, *1*(1), 1-14
6. Greenaway, K.E., and Chan, Y.E. "Theoretical Explanations for Firms' Information Privacy Behaviors," Journal of Association for Information Systems (6:6) 2005, pp 171-198.
7. Greenaway, K.E., and Chan, Y.E. "Theoretical Explanations for Firms' Information Privacy Behaviors," Journal of Association for Information Systems (6:6) 2005, pp 171-198.
8. Earp, J.B., Anton, A.I., and Jarvinen, O. "A Social, Technical, and Legal Framework for Privacy Management and Policies," Eight Americas Conference on Information Systems, 2002, Dallas, TX, pp 605-612.
9. Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," Information Systems Research (15:4), 2004, pp 336-355.
10. Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. "Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. Information Systems Research, (*23*:4) 2012, 1342–1363
11. Riquelme, U and Roman, S. "Is the Influence of Privacy and Security on Online Trust the Same for All Types of Consumers?" Electronic Markets, (24:2) 2014, 135-149.
12. Smith, H. J., Milberg, S., and Burke, S. 1996. Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 20(2): 167-196.

13. Malhotra, N., 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.
14. Milne, G. R. and Gordon M. E. 1993. Direct mail privacy-efficiency trade-offs within an implied social contract framework. Journal of Public Policy Marketing, 12(2): 206–15
15. Culnan, M. J. and Armstrong, P.K. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust. Organization Science, 10(1): 104-115.
16. CBS News. 2005. Poll: Privacy Rights Under Attack. http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml.
17. Harris Interactive. 2001. Privacy On & Off the Internet: What Consumers Want. Tec report. http://www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf.
18. Benassi, P. 1999. TRUSTe: an online privacy seal program, Communication of the ACM, 42(2):56 – 59.
19. Moores, T. 2005. Do consumers understand the role of privacy seals in e-commerce? Communication of the ACM, 48(3): 86 – 91.
20. Acquisti, A. and Grossklags, J. 2005a. J. Privacy and Rationality in Decision Making. IEEE Security and Privacy, 3(1): 26-33.
21. https://www.mckinsey.com/
22. The Data Digest: Consumers' Attitude Towards Online Privacy and Security by Reineke Reitsma, VP, Research Director; Jan 20 2012.