Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings | Proceedings

A Global Perspective of Privacy Protection Practices

Noushin Ashrafi
Boston, MA, United States., noushin.ashrafi@umb.edu

Jean-Pierre Kuilboer
Management Science and Information Systems, University of Massachusetts Boston, Boston, MA, United States., jeanpierre.kuilboer@umb.edu

A Global Perspective of Privacy Protection Practices

Noushin Ashrafi
University of Massachusetts Boston
noushin.ashrafi@umb.edu

Jean-Pierre Kuilboer
University of Massachusetts Boston
jeanpierre.kuilboer@umb.edu

ABSTRACT

The global economy of today, boosted by propagation of e-commerce, has elevated the privacy and security issues to a worldwide platform. E-commerce growth is strongest in the US and the European Union. Recently India and China have also become significant players in the global commercial setting. This research is exploratory in nature and attempts to examine privacy protection practices in the United States, Europe, India and China. The results indicate that information privacy protection practices are prevalent in the USA. On the other side of the spectrum is China with a completely different view of personal privacy reflecting the nations' treatment of information privacy.

Keywords

Privacy Protection Practice, Global, FIPP, India, China, Europe, US.

INTRODUCTION

Today the combination of a global economy and the propagation of e-commerce have elevated the privacy and security issues to a worldwide platform. The international commercial setting necessitates the cross border access to not only B2B but also to B2C information. While this flow of information is essential for the growth of international commerce, its side effect; threats of breach of individual privacy pose a real concern both for the individual and the business community (Birnhack, 2008).

E-commerce is still growing exponentially in the US and the European Union (EIU, 2001). The prevalent privacy protection practices in the United States follow the self-regulatory Fair Information Practices (FIP) guidelines. These guiding principles are primarily concerned about the manner in which personal information is collected and used. They are formulated to assure that the practice is fair and provides adequate information privacy protection. FIP was initiated by the United States' Federal Trade Commission, but the concept of privacy protection was soon spread to other countries in Europe. International institutions took up privacy with a focus on the international implications of privacy regulation. The Organization for Economic Cooperation and Development (OECD) Guidelines, Council of Europe Convention, and European Union Data Protection Directive relied on FIPs as core principles. The "Safe Harbor Agreement," signed by the US and European Union in July 2000, to allow trans-border flow of data (Smith, 2001), is still in effect. The Safe Harbor agreement guides U.S. companies to avoid experiencing interruptions in their business dealings with the EU or face prosecution by European authorities under European privacy laws. Certifying to the Safe Harbor will assure that EU organizations know that your company provides "adequate" privacy protection, as defined by the Directive.

The effectiveness of these practices and the commitment of the companies to online privacy have been topics of research by academics and practitioners. Numerous studies have investigated privacy practices in the US (Milne and Gordon, 1993; Bloom, Milne and Adler, 1994; Culnan and Milberg, 1998; Culnan and Armstrong, 1999; Clarke, 1999; Caudill and Murphy, 2000; Milne and Culnan, 2002; Pavlou, 2003; Culnan and Milne, 2004; Ashrafi and Kuilboer, 2005). Fewer studies have examined European regulatory practices (Armstrong, 2004; Massa-Mias, 2007; Singh and Hill, 2003; Warren and Dearnley, 2005).

Most recently India and China have also become significant players in the global e-commerce environment. Outsourcing and the rapid growth of their economy have intensified the good, the bad, and the ugly of the development and expansion of international companies. To maintain their roles as viable players in the networked market economy, both countries have to pay attention to privacy protection policies. Multinational companies that bank on transnational market as a substantial source of revenue find it necessary to adhere to the cross-border data flow laws of the European Union and consequently Fair Information Practices of the US (Wright, 2011). Yet, the deliberation on privacy protection practices in India and China is a

new concept and not as widespread as those for the western hemisphere. Privacy protection research in India primarily focuses on consumer behavior and their interpretation of the notion of privacy (Basu, 2010; Gupta et al., 2010; Brahmbhatt, 2010; Baja, 2012; Ardhapurkar, 2010.) Similarly, the amount of research on exploring developments in privacy and data protection regulation in China is minimal and concentrates on cultural aspects and the explanation of privacy law and regulations (Xue, 2010; Yoon, 2009; Wu Y, 2011; Medlin, 2010; and Greenleaf, 2009.)

This study is exploratory in nature and attempts to examine information privacy protection practices in the United States, some European countries, India and China. Four European countries that are considered e-commerce leaders in Europe were selected; Spain, France, United Kingdom, and Germany (Singh, 2003). We investigated the website of 400-500 companies in each country and studied their compliance with the most basic requirements of Fair Information Practices principles (FIPP) such as notice, choice, access, and security. Data collection for each country was performed by an individual proficient in the language of the country. Descriptive statistics from collected data provide an empirical view of privacy protection practices in these countries.

The results confirm the anecdotal evidence that information privacy means a lot to Americans, hence the strong industry responses to the concern of the citizens by improving their online privacy practices. On the other side of the spectrum are Chinese with a completely different view of personal privacy which reflects on the industries' treatment of individual information.

The organization of the paper is as follows: the next section provides a brief description of global information privacy followed by description of fair information practices. We then explain our data collection methods and results in the USA, four European countries, India, and China. We conclude by outlining the limitation of this research and suggesting directions for further research.

INFORMATION PRIVACY IN A GLOBAL SETTING

Information Privacy is the right of an individual to determine when, how and to what extent he/she will share his/her personal information (Westin, 1967). This statement constitutes the individual's ability to control the terms and conditions and the extent to which his or her personal information is attained and used. Information privacy is viewed differently by different cultures. Europeans are generally firm believers in strict legislation governing information privacy. They view the protection of their personal information as a "general privacy right" and perceive controlling personal data as a matter of basic human right. In the US, privacy refers to the constitutional right protecting citizens against governmental encroachment (Whitman, 2004). Information privacy in the US is viewed as "contractual negotiation" (Smith, 2001) and specifies regulations in specific sectors such as financial (Anton et al., 2004) and health care (Song and Zahedi, 2007; Zahedi and Song, 2008).

Asians perceive privacy mostly in terms of physical, home, and living space. India enjoys a robust growth and continues to be a key emerging market across the world. The growth rate of foreign companies operating in India was estimated to be 100% every year (Brahmbhatt, 2010). Interest in privacy is strong among firms that provide Business Process Out-Sourcing (BPO) for foreign firms, especially for European firms. It is, however, much weaker when it comes to privacy rights of Indian consumers. According to Kumaraguru et al. (2005, p. 8), the typical attitude towards concerns about information privacy by an Indian is "Data security and privacy are not really a problem because I have nothing to hide." A comprehensive interview with Indian subjects regarding privacy laws for online shopping revealed similar outlook that "Why do you need laws for it?" (Kumaraguru et al., 2005, p.10). In May 2000, the Indian government passed the Information Technology Act, 2000. The Act contains a set of laws intended to provide a comprehensive regulatory environment for electronic commerce such as legal recognition of electronic records and digital signatures, the settlement of cyber-crimes, and dealing with breach of confidentiality (Kumaraguru, 2005.) However, the IT Act 2000 has no provision for the protection of personal data.

As we noted earlier E-commerce is an international concept now, and since China is emerging as a global economic power (Stylianou, 2003; Xue, 2010), it can play a substantial role in privacy protection arena. The literature search for information privacy practices in China revealed very little on information privacy (Yoon, 2009; Xue. 2010; Wu, 2011). Similar to India, the focus was the interpretation of individual privacy and the government's role, or lack of it, to protect individual privacy. Based on our sample data, Indian and Chinese companies pay little attention to FIP guidelines and only few are in compliance with the principles. Clear differences in cultural and regulatory aspects of privacy could be the reason; however, one may assume that sooner or later the concept of information privacy will draw the attention of multinational companies in both countries.

FAIR INFORMATION PRACTICE PRINCIPLES (FIPPS)

The growth of information technologies and globalization processes in the US, coupled with several well-publicized breaches of consumer privacy protection (Desai, 2009), has led to the realization that personal data require more effective safeguards. Fair Information Practice Principles (FIPPs), a self-regulatory enforcement initiative, is the result of such awareness. Culnan and Bies (2003, p. 330) describe FIPPs as consisting of "procedures that provide individuals with control over the disclosure and subsequent use of their personal information and govern the interpersonal treatment that consumers receive." The FIPPs are designed so that the organization implementing the FIPPs will abide by a set of ethics and values that are widely accepted by most consumers (Folger and Bies, 1989; Folger and Greenberg, 1985). FIPPs serve as a basis for privacy laws and self-regulation mechanisms in the US and other countries and for the European Privacy Directive (Milne and Culnan, 2002).

Publishing Privacy policies on a company's website is the first and necessary step for information privacy protection (Culnan, 2000). Privacy policy principles are guidelines to give the consumer the right to know what information is being collected, object when information is utilized for purposes other than those authorized, view their information and correct any erroneous information. These policies may also identify security measures to inform customers if "cookies" are used to track on-line habits. In what follows, we provide a brief description for each of these information privacy principles.

Notice

Notice is the heart of the fair information practices. When consumers provide their personal information, they have the right to know why this information is being collected, how it is being used, and the steps that have been taken to protect its confidentiality and integrity. Privacy notices represent the manner in which the collector acquires, uses, shares, protects and provides access to an individual's personal information. The rest of the information practices likes choice, access and security only become meaningful when the consumer has notice of an entity's policies and his/her rights with respect to their personal information.

Choice

Choice also referred to as Consent is a widely accepted information practice to acquire consumer consent regarding the secondary uses of the personal information that has been collected. This guideline gives the consumer control over how personal data may be used and allows them to remove their names from existing marketing lists before such lists are shared with third parties (Culnan and Bies, 2003). Thus, an "opt in" approach represents a confirmation that the consumer has agreed to receive marketing offers or messages whereas an "opt out" policy means that the consumer's information is freely shared and distributed unless the consumer takes specific measures, outlined in the policy, to object to such sharing.

Access

Access refers to the individual's ability to access personal information collected by a company. Access as defined in the Fair Information Practice Principles includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. Furthermore the access must be inexpensive and timely in order to be useful to the consumer.

Security

According to FIPP (FTC, 2000), websites are required to take reasonable measures to protect the security of customer personal information. The data collector is obligated to protect personal data against unauthorized use as well as loss or destruction. Although security requirements vary depending on the nature and sensitivity of collected data, the firm must maintain security programs to minimize threats as well as inform customers about companies' security practices, In other words, the companies are required not only to have a security program, but also to disclose their security practices in order to enhance consumer confidence.

Cookies

Cookies are instruments through which the browsing and buying habits of consumers can be tracked (Rogers, 2004; Wang, Lee and Wang, 1998). Cookies are small pieces of code which are forwarded to a consumer's computer by web servers and stored there so that the consumer becomes identifiable the next time he or she logs on to that web server (King, 2003).

Cookies are primarily used to store passwords or trace visits to a website by anyone who browses through a particular computer (Culnan and Bies, 2003).

Empirical Study

In our attempt to investigate the application of fair information protection principles, we looked for the listing of top 500 interactive companies in each country. Our first task was to ensure that the selected companies do have an active website. We then investigated to see what percentage of interactive companies had published privacy policies on their websites. We drilled further to check if their private protection policy addressed the four basic principles of FIP namely Notice, Choice, Access, and Security, and finally we wanted to see what percentage of firms are installing cookies to trace electronic "footprints" that consumers leave behind. The significance of cookies relies on the fact the collector can share the captured information with other entities for pecuniary purposes.

Data collection for the United States was straight forward and it became increasingly more difficult for European countries, India, and China. In what follows we describe the source and method of data collection for each country together with our findings for each country. We will compare the results in the conclusion.

PRIVACY PROTECTION PRACTICES IN THE USA

The most reliable published data in the US turned out to be a list of 500 interactive companies compiled by Interactive Week magazine. The listing included public and private companies in business at the end of June 2000. Information on nearly 1,500 companies was compiled and ranked based upon their online revenue, and the top 500 companies were published in the November issue. We were fortunate that this listing also included the Web sites for the 500 top companies, which we used as the starting point for our study. We visited the websites in 2000 and once again in fall of 2002 and wrote a paper published in 2005. In Fall of 2009, we visited the Web sites again to check how many of the top 500 companies still had an online presence and whether there was an improvement in regard to extent and content of published policies. Tables 1-3 illustrate our findings.

Companies	Percentage
Appear to have online presence	85.4%
Disappeared	14.6%

Table 1. Interactive Companies that Remain Active in 2009

Data indicates that a little less than 15% of the initial interactive companies disappeared between 2002 and 2009. However the majority of remaining companies had published privacy policy on their website as shown in table 2.

Privacy Policies	Percentage
Published	85%
Not Published	15 %

Table 2. The Percentage of Companies with Published Privacy Policies

Table 3 addresses the percentage of remaining interactive companies that not only have privacy policies published on their websites, but also have clearly addressed the issues of Notice, Choice, Access, and Security.

Privacy content	Percentage
Notice	100.00%
Choice	83.33%
Access	82.25%
Security	96.47%

Table 3. The Percentage of Interactive Companies that Address FIP Principles

A quick comparison between 2002 and 2009 data reveals improvement in all aspect of privacy protection content.

Privacy content	2002	2009
Notice	98%	100%
Choice	73%	83.33%
Access	57%	82.25%
Security	78%	96.47%

Table 4. A comparison between 2002 and 2009

PRIVACY PROTECTION PRACTICES IN EUROPE

To establish the extent to which the European firms actually inform their customers about the existence and nature of their privacy policies through on-line posting we visited roughly 400 to 500 websites for each county and looked for privacy policy posting. Data collection for this study began with the listing of the top 500 companies in Europe (Quality Datenbank Klaus Gebhardt, e.k., n.d.). Two additional websites: www.negocios.com and the www.finance.yahoo.com of each country under study proved to be very helpful. The first one belongs to an independent Spanish business newspaper, which introduced a compiled ranking of the top Spanish companies, both public and private, by type of business. In addition, this website provided the ranking of the top companies from 32 European countries, sorted by different categories. The second website served as a link to the major public European companies listed in the Stock Exchange of each country. The findings brought more surprises than expected: some top companies lacked any online presence, and others employed their websites only to advertise their existence. For the purposes of this study, those samples were discarded, and we focused on those firms actively engaged in Internet-based commerce, whether B2B or B2C.

While in the US, firms' privacy policies are normally posted directly on their main websites, some European firms tend to publish their privacy policies under "Terms and Conditions" or "Legal Notes", making them less easily accessible to consumers. Table 5 illustrates the percentage of these companies in each country.

	Germany	UK	France	Spain
Privacy policy on the website	63 %	76%	62%	74%
No Privacy policy on the website	37%	24%	38%	26%

Table 5. Published Privacy Policy

We then looked into the content of privacy policies to determine the extent to which the principles of Notice, Choice, Security, and Access were addressed. Table 6 shows the results.

	Germany	UK	France	Spain
Notice	63%	89%	61%	76%
Choice	14%	21%	<5%	<5%
Security	48%	13%	15%	31%
Access	NA	NA	NA	NA

Table 6. Content of Privacy Policies

Our results clearly show that the U.K. again leads the list with the 76% of the websites of companies under survey showcasing their privacy policies. Overall, almost one third of the companies surveyed did not have a privacy policy published on their websites.

PRIVACY PROTECTION PRACTICES IN INDIA

As India is becoming a leader in business process outsourcing and its online market is growing rapidly, a large amount of personal data is flowing from other countries into India (Kumaraguru, 2006). Yet, the issue of privacy protection is a

relatively new concept in this country and it is unclear whether it has captured the attention of multinational corporations that do business in India. For this study we took Economic Times 500 list (ET 500) for the year 2008 as reference. Economic Times is the world's second biggest Financial Daily, after the Wall Street Journal. The list is one of India's most awaited lists as it presents the Top 500 Indian companies in the order of decreasing Market Cap.

Privacy Policies	Percentage
Published	27.60%
Not Published	72.40%

Table 7. The Percentage of Indian Companies with Published Privacy Policies

A little more than one fourth of companies in India have posted privacy policies on their web site. Further investigation revealed the extent to which issues of Notice, Choice, Security, and Access were disclosed. Table 8 illustrates the results of this investigation.

Privacy content	Percentage
Notice	76.81%
Choice	26.81%
Security	58.70%
Access	NA

Table 8. The Percentage of Indian companies that Address FIP Principles

The table indicates that more than 3/4 of companies that have published privacy policies have Notice, more than ¼ comply with choice principle, and more than ½ publish their security procedure. Access was not even addressed.

PRIVACY PROTECTION PRACTICES IN CHINA

To select top 500 interactive companies we referred to China.org.cn which lists the top 500 enterprises of China. Looking at the websites of these companies there were some interesting findings; (1) percentage of web sites indicating having privacy policy varied between English version of the website versus Chinese's language and (2) many websites had privacy policy indicator, but it was an empty shell without any content. This was even more pronounced for English versions, which almost had no content.

Privacy Policies	China(English)	China(Chinese)
Published	18.4%	28.4%
Not Published	81.6%	71.6%

Table 9. Percentage of Companies with Published Privacy Policy

It is interesting that more Chinese version of web sites have indicated having privacy policies published. Further investigation showed that in the English version there was no content and the very small portion of Chinese version had content as shown in table 10.

Privacy content	Percentage
Notice	19.6%
Choice	14.0%
Access	13.6%
Security	17.8%

Table 10. The percentage of Chinese Companies with Content

The low percentage in table 10 re-enforces our observations that most companies that had a display of privacy policy indicator were not linked to any content. This indicates that the company does realize the importance of privacy policy published in their website, but fails to practice privacy policy protection and follow the guidelines.

CONCLUSION AND LIMITATION

The widely accepted FIP Principles are the basis for privacy protection practices in the United States, Canada, Europe and other parts of the world. Publishing these principles help a consumer choose whether to disclose personal information to the company as well as helping them decide whether to transact with the company in question (Culnan and Milberg, 1998). The discrepancies of the degree of privacy protection practices among the nations chosen for this research are interesting, but not surprising; the United States self-regulatory practices yields the best results, followed by regulated practices of Europe. India and China are lagging behind as they are in the beginning of entering international market. Table 11 illustrates the rate of compliance with FIPPs for each country.

	PPP		Notice	Choice	Access	Security	Cookies
USA (2009)	85%		100%	83.33%	82.25%	96.47%	98.39%
France (2004)	62%		61%	<5%	NA	15%	24%
Spain (2004)	74%		76%	<5%	NA	31%	34%
UK (2004)	76%		89%	21%	NA	13%	57%
Germany (2004)	63%		63%	14%	NA	48%	28%
India (2008)	27%		76.81%	26.81%	NA	58.70%	48.55%
China (2009)	English	Chinese	19.6%	14%	13.6%	17.8%	90%
	18.4%	28.4%					

Table 11. Summary Table

The limitation of this study relates to the accuracy and timing of data collection. The paper covers the study of websites of only four EU countries, so we cannot draw definitive conclusions about privacy regulation and implementation for the entire EU. The latest date for Data collection for the US and China was in 2009, whereas it was 2008 for India and 2004 for four European countries. Despite the five years gap, the intent of research, to provide an overall perception of FIPP in the selected countries is realized. As the European Union is coming up with entirely new set of directives, it would be interesting to investigate the impact of the new directives. It would be also interesting to consider other parameters such as the level and nature of enforcement, firm size and industry, the comprehensiveness of the policy, and whether the policy includes reference to the Platform for Privacy Preferences (P3P).

REFERENCES

1. Anton, A. I., Earp, J. B., He, Q., Stufflebeam, W., Bolchini, D. and Jensen, C. (2004) Financial privacy policies and the need for standardization, *IEEE Security and Privacy*, 2, 2, 36-45.
2. Armstrong, J. (2004) Privacy in Europe: the new agenda, *Journal of Internet Law*, 8, 5, 3-7.
3. Ashrafi, N. and Kuilboer, J-P. (2002) Data privacy, U.S. common practices, in Abdelkader Hameurlain, Rosine Cicchetti, Roland Traunmüller (Eds.), DEXA, 13th International Workshop on Database and Expert Systems Applications, September 2-6, 2002, Aix en Provence, France, 488.
4. Ashrafi, N. and Kuilboer, J-P. (2005) Online privacy policies: an empirical perspective on self-regulatory practices, *Journal of E-Commerce in Organizations*, 3, 4, 61-74.
5. Ashrafi, N. and Kuilboer, J-P. (2007) Implementation of privacy protection policies: an empirical perspective, *Utilizing and Managing Commerce and Services Online*. CyberTech Publishing, 2007, Ch. IX: 187-204.
6. Ashrafi, N. and Kuilboer, J-P. (2007) Is P3P an answer to protecting information privacy? *E-Business Innovation and Process Management*. CyberTech Publishing, 2007, Ch XV: 331-347.
7. Birnhack, M. D. (2008) The EU data protection directive: An engine of a global regime, Elsevier, *Computer Law and Security Report*, 24, 6, 508-520.
8. Bloom, P., Milne, G., and Adler, R. (1994) Avoiding misuse of new information technologies: legal and societal considerations, *Journal of Marketing*, 58, 1, 98-110.
9. Caudill, E.M. and Murphy, P.E. (2000) Consumer online privacy: legal and ethical issues, *Journal of Public Policy and Marketing*, 19, 1, 7-19.

10. Clarke, R. (1999) Internet privacy concerns confirm the case for intervention, *Communications of the ACM*, 42, 2, 60-67.
11. Culnan, M. J. (2000) Protecting privacy online: is self-regulation working? *Journal of Public Policy and Marketing*, 19 1, 20-26.
12. Culnan, M.J. and Armstrong, P.K. (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, *Organization Science*, 10, 1, 104-115.
13. Culnan, M.J and Bies, R.J. (2003) Consumer privacy: balancing economic and justice considerations, *Journal of Social Issues*, 59, 2, 323-342.
14. Culnan, M.J., and Milberg, S.J. (1998) The second exchange: managing customer information in marketing relationships, Georgetown University, Unpublished Working Paper.
15. Committee on Consumer Policy [CCP], (2003) *Consumers in the Online Marketplace: The OECD Guidelines Three Years Later,* February. Retrieved December 12, 2003 from: www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-cp(2002)4-final.
16. Desai, P., Ashrafi, N., Kuilboer, J-P., and Koehler, W. (2009) Regulatory privacy practices in Europe, in AMCIS 2009 Proceedings, San Francisco, CA, August 6-9, *2009*: http://aisel.aisnet.org/amcis2009/171
17. Economist Intelligence Unit (EIU) (2001) *Meta Group: Future of e-commerce lies in North America, Europe*, 10 May 2001, Retrieved February 21st, 2009 from: http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_id=3373&categoryid=&channelid=5&search=readiness
18. European Commission (2003) Data *Protection: Microsoft Agrees to Change its .NET Passport System after Discussions with EU Watchdog*. IP/03/151. Retrieved February 21st, 2009 from: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/03/151&format=HTML&aged=0&language=EN&guiLanguage=en.
19. European Parliament, (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, Retrieved January 12th, 2009 from:

    http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT
20. Federal Trade Commission (FTC) (2000) Privacy online: fair information practices in the electronic marketplace, Report to Congress, May.
21. Folger R. and Bies, R. J. (1989) Managerial responsibilities and procedural justice, *Employee Responsibilities and Rights Journal*, 2, 2, 79-90.
22. Folger, R. and Greenberg, J. (1985) Procedural justice: an inspective analysis of personal systems, In K. M. Rowland & G. R. Ferris (Eds.), *Research in Personnel and Human Resources Management*, 3, 141-183. Greenwich, CT: JAI: Press.
23. Gupta, B., Iyer, L.S. and Weisskirch, R.S. (2010) Facilitating global e-commerce: a comparison of consumers' willingness to disclose personal information online in the U.S. and in India, Journal of Electronic Commerce Research, 11,1, 41-52.
24. King, I. (2003) Online privacy in Europe: new regulation for cookies, *Information and Communication Technology Law,* 12, 3, 225-236.
25. Kumaraguru, P., Cranor, L.F. and Newton, E. (2005) Privacy perceptions in India and the United States: an interview study. In The 33rd Research Conference on Communication, Information and Internet Policy (TPRC), 2005.
26. Massa-Mias G., Ashrafi, N., Koehler W. and Kuilboer J-P. (2007) Privacy policy regulations- an empirical investigation, in proceedings, 38th Annual Meeting Decision Sciences Institute, November 17-20, Phoenix, AZ.
27. Milne, G. R. and Culnan, M. J. (2002) Using the content of online privacy notice to inform public policy: a longitudinal analysis of the 1998-2001 U.S. web surveys, *The Information Society*, 18, 5, 345-359.
28. Milne, G. R. and Gordon, M. E. (1993) Direct mail privacy- efficiency trade-offs within an implied social contract framework, *Journal of Public Policy and Marketing*, 12, 2, 206-215.
29. Organization for Electronic Co-operation and Development (1980) *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*, Washington DC: OECD.

30. Pavlou, P.A. (2003) Integrating trust and risk with the consumer acceptance of electronic commerce: technology acceptance model, *International Journal of Electronic Commerce*, 7, 3, 69–103.
31. Pavlou, P. and Ba, S. (2002) Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior, *MIS Quarterly,* 26, 3, 243-268.
32. Rogers, K. M. (2004) The privacy directive and resultant regulations? The effect on spam and cookies, part I, *Business Law Review*, 25, 10, 271-274.
33. Singh, T. and Hill M. H. (2003) Consumer privacy and the internet in Europe: a view from Germany, *Journal of Consumer Marketing*, 2, 7, 634-652.
34. Smith, J. H. (1993) Privacy policies and practices: inside the organizational maze, *Communications of the. ACM,* 36, 12, 105-22.
35. Smith, J. H. (2001) Information privacy and marketing: what the U.S. should (and shouldn't) learn from Europe, *California Management Review*, 43, 2, 8-33.
36. Song, J. and Zahedi, F. (2007) Trust in Health Infomediaries, *Decision Support Systems,* 43, 2, 390-407.
37. Stylianou, A.C., Robbins, S.S. and Jackson, P. (2003) Perceptions and attitudes about E-Commerce development in China: An exploratory study, *Journal of Global Information Management* (JGIM), 11, 2, 31-47.
38. Wang, H., Lee, M. K. and Wang, C. (1998) Consumer privacy concerns about internet marketing, *Communications of the ACM*, 41, 3, 63-70.
39. Warren, S. D. and Brandeis, L. D. (1890) The right to privacy, *Harvard Law Review*, IV, 5,193-220.
40. Warren, A. and Dearnley, J. (2005) Data protection legislation in the United Kingdom: from development to statute, 1969–84, *Information, Communication & Society*, 8, 2, 238–*263.*
41. Westin, A. F. (1967) Privacy and Freedom. New York: Athenaeum.
42. Wright, D., De Hert, P. and Gutwirth, S. (2011) Are the OECD guidelines at 30 showing their age? *Communications of the ACM*, 54, 2, 119-127.
43. Wu, Y., Lau, T., Atkin, D.J. and Lin, C.A. (2011) A comparative study of online privacy regulations in the U.S. and China, *Telecommunications Policy*, 35, 7, 603-616.
44. Xue, H. (2010) Privacy and personal data protection in China: an update for the year End 2009, *Computer Law & Security Review*, 26, 3, 284-289.
45. Yoon, C. (2009) The Effects of national culture values on consumer acceptance of e-commerce: online shoppers in China, *Information & Management*, 46, 5, 294-301.
46. Zahedi, F. and Song, J. (2008) Dynamics of trust revision: using health infomediaries, *Journal of Management Information Systems*, 24, 4, 225-248.