Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Regulatory Privacy Practices in Europe

Priyanka Desai
University of Massachusetts Boston, priyankaumass@gmail.com

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

Jean-Pierre Kuilboer
University of Massachusetts Boston, jean-pierre.kuilboer@umb.edu

William Koehler
University of Massachusetts Boston, william.koehler@umb.edu

Regulatory Privacy Practices in Europe

Priyanka Desai
University of Massachusetts Boston
priyankaumass@gmail.com
Noushin Ashrafi
University of Massachusetts Boston
Noushin.ashrafi@umb.edu
Jean-Pierre Kuilboer
University of Massachusetts Boston
Jean-pierre.kuilboer@umb.edu
William Koehler
University of Massachusetts Boston
William.Koehler@umb.edu

ABSTRACT

In today's global economy, the flow of information is essential for the growth of international commerce and for the cross border access for both B2B and B2C services. The e-commerce phenomenon has elevated the privacy issue to a global platform. This paper examines the extent to which sample firms in four European countries post privacy notices on their websites. While posted privacy policy does not necessarily mean compliance with privacy protection policy, the absence of it indicates failure to comply with the most basic principle of privacy protection. We also reviewed the posted privacy policies of 425 firms and evaluated them against their corresponding country's directives as well as fair information policies of the US. Descriptive statistics from the collected data provide a preliminary indication of how privacy practices are observed in our samples of four European countries.

Keywords

E- Commerce, Information Privacy, Self-regulation, European Union Directive

INTRODUCTION

Since the inception of e-commerce, issues regarding consumer privacy have received a great deal of attention. Researchers (Ashrafi and Kuilboer, 2005; Bloom, Milne and Adler, 1994; Clarke, 1999; Culnan and Milberg, 1998; Milne and Culnan, 2002) have identified breach of privacy as one of the most important concerns for Internet-based commercial and non-commercial exchanges.

In the past, online customers provided only pecuniary information in return for the goods or services purchased. Today however, e-commerce often also involves a "second exchange" through which consumers provide private information to obtain higher-quality services, such as personalized offers, or information about promotions and discounts (Culnan and Milne, 2004). Firms benefit by storing and using visitors' information for behavioral marketing and service improvement, but the practice does bring concomitant risks. Consumers may suffer breaches of personal space and such data collection may raise privacy concerns and stifle e-commerce if information is used incorrectly or indiscriminately. Laufer and Wolfe (1977) report that individuals are willing to divulge personal information to obtain monetary benefit or social benefit if they are certain that their personal information will be used fairly, and properly protected. Culnan and Armstrong (1999) argue that a corporation's misuse of private information could make customers reluctant to reveal further information, generate negative publicity for the firm, and discourage new customers from doing business with the firm.

In today's global, networked economy, data necessarily flow across national borders. Trans-border flow of information is essential for the growth of international commerce and for the cross-border access to not only Business to Business (B2B) Services but also Business to Consumer (B2C) services (Birnhack, 2008). In July 2000, the US and European Union signed the "Safe Harbor Agreement" to allow trans-border flow of data (Smith, 2001). As individuals reveal personal data across borders when visiting a foreign site, the privacy issue is elevated to a global platform. One key challenge facing firms globally is to collect the data that businesses need for improving their commercial activities while allowing customers to maintain control over the use of their personal and financial data (Birnhack, 2008).

E-commerce growth is strongest in the US and the European Union (EIU, 2001). While US companies view the European market as a significant source of e-commerce revenue, significance differences in the e-commerce environment between the US and EU have resulted in legal and public-relations difficulties for numerous multinational companies that have not adhered to the cross-border data flow laws of the European Union.

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, however (Armstrong, 2004; Singh and Hill, 2003; Warren and Dearnley, 2005). The only empirical investigation of the adoption and implementation of regulatory policies, initiatives and technological tools for privacy protection of the European companies is that of Massa-Mias, Ashrafi, Koehler, and Kuilboer (2007).

This study examines the privacy policies of 425 of the top e-commerce companies in four European countries and measures their compliance with European Union Data Protection Directives. The four countries- Spain, France, United Kingdom, and Germany- were selected because they are considered e-commerce leaders in Europe (Singh, 2003), and the authors had collective command of the languages in question. Descriptive statistics from collected data provide an empirical view of regulatory privacy practices in these four European countries.

The organization of the paper is as follows: the next section provides a brief description of global information privacy and fair information practices. The following section offers an account of EU data protection directives. We then explain our data collection method and offer analysis of our data. We conclude by outlining the limitation of this research and suggesting directions for further research.

INFORMATION PRIVACY AND FAIR INFORMATION PRACTICES

Information privacy constitutes an individual's ability to control the terms and conditions and the extent to which his or her personal information is attained and used (Westin, 1967). Information privacy is viewed differently in Europe and the US. 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 in contrast 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, Earp, He, Stufflebeam, Bolchini, and Jensen, 2004) and health care (Song and Zahedi, 2007; Zahedi and Song, 2008).

The growth of information technologies and globalization processes in the US, coupled with several well-publicized breaches of consumer privacy protection, has led to recognition that personal data requires more effective safeguards. Fair Information Practice Principles (FIPPs), a self-regulatory enforcement initiative, is the result of such reorganization. Culnan and Bies (2003) 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). The US Federal Trade Commission 2000 (FTC, 2000) has outlined these practices consisting of five guidelines:

- Notice (consumers have the right to know what information is being collected)
- Choice (consumers can object when information is utilized for purposes other than those authorized)
- Access (consumers have the right to view their information and correct any erroneous information)
- Security (organizations should secure data from unauthorized access during transmission and storage)
- Enforcement/Redress (self-regulation, as well as private, civil, and criminal remedies, can provide the means to ensure that corporations comply with the Principles).

FIPs 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).

THE EUROPEAN UNION DATA PROTECTION DIRECTIVE

Europe took a very serious stand on privacy in July 1995 when the European Union (EU) adopted the "Data Protection Directive" (DPD) to coordinate the data protection laws within the European Union. This new directive required all EU member states to have legislation and rules for the protection of personal data. Each country has flexibility in implementing the laws and may enact additional measures as it sees fit. The DPD bestows the right of the consumer/individual to exercise

control globally over the data that they reveal about themselves. Birnhack (2008: 508) argues that the DPD has emerged as the most influential standard, internationally, in information privacy:

> The 1995 EU Directive on data protection regulates the collection, processing and transfer of personal data within the EU, with the dual goal of enabling the free flow of data while maintaining a high level of protection. …Thus, countries that wish to engage in data transactions with EU member states are indirectly required to provide an adequate level of protection. … [T]he Directive has had a far greater global impact than thus far acknowledged and…is currently the main engine of an emerging global data protection regime.

The directive does indeed prohibit the transfer of personal data to any country which fails to have an *adequate level of protection* of personal data. The DPD contributes to the formation of laws and regulations through which data collected beyond the European Union are protected. Several major multinational firms have already faced legal action when violating the DPD. The Spanish government sued software giant Microsoft in 1999 because Microsoft was not in compliance with Spanish privacy laws (Kuner and Simpson, 2005), while the European Commission required Microsoft to enhance its security provisions for its ".NET Passport" Internet browsing password system (European Commission, 2003). Google also faced the wrath of the EU when it was found to be in violation of European laws by keeping its data for two years- twice as long as the EU allows (O'Brien and Cramton, 2007). The European Union has also taken action against eBay after receiving complaints that eBay customers were having trouble closing their accounts and erasing their trading histories. The EU eventually forced eBay to modify its services and data protection policies (O'Brien and Cramton, 2007).

The DPD requires member states to enact and enforce laws reflecting information protection principles. Our investigation seeks to determine the extent to which major European firms comply with the DPD and other EU privacy regulations.

Table 1 illustrates when each county passed its first data protection law and when the law was revised to comply with EU DPD. Each country has the liberty of adding its own set of rules apart from the laws set forth by the EU; hence, each nation employs a different name for its version of the DPD. Table 1 provides the URL for the websites that describe the data protection act for each country and it its history in detail.

Country	**United Kingdom**	**Spain**	**Germany**	**France**
Name	The Data Protection Act	The Organic Act 15/1999	Federal Data Protection Act	French Data Protection Act
Year initiated	1998	1992	1990	1978
URL	**http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1**	**http://www.privacyinternational.org/survey/phr2003/countries/spain.htm**	**http://www.iuscomp.org/gla/statutes/BDSG.htm**	**http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf**
Compliance with EU Directive	As of 2004 not meeting European Union standards	As of 2003 in full compliance with EU directive	As of 2003 in full compliance with EU Directive	As of 2002 in full compliance with EU Directive

Table 1. Profile of Data Protection Act for our sample countries

Note: while each country studied has been continuously revising its information privacy laws, we have determined national conformity with EU DPD guidelines through 2004, the cutoff for our data collection.

EMPIRICAL OBSERVATION

Our study involves collecting data from 425 e-commerce companies in four countries: England, France, Germany, and Spain—to determine if these companies have posted their privacy policies and if their posted policies are in compliance with

their national DPD laws. Posting privacy policies is the first step in protecting privacy. Without such transparency, individuals have no information about a site's information practices and no basis for deciding whether or not to interact with a web site (Milne and Culnan, 2002). The results demonstrate that not only the percentages of companies' websites that currently include statements about their information privacy policies, but also the content of these posted policies, vary widely among countries. First, we present the details of our data collection.

Data Collection

Data collection for this study began with a 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, also proved to be very helpful. The first website is run by 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 solely 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.

Regulatory Practices: Compliance with Data Protection Act

The first task was to determine the percentage of companies in each country that comply with the Data Protection Act of their respective countries.

	Germany	UK	France	Spain
In compliance with the Data Protection Act	50%	77%	56%	64%
No clear indication of compliance	50%	23%	44%	36%

Table 2. Compliance with the Data Protection Act

The data in Table 2 shows the UK leading with 77% of the companies complying with the Data Protection Act. France and Spain had 56% and 64% of the companies following their country's laws, respectively. Surprisingly, 50% of the German companies studied did not comply with DPA of their country.

Published Privacy Policies

Privacy policies can usually be found on company websites, and they describe how data collected will be used and stored. The valuable information provided by the privacy policies helps a consumer choose whether or not to disclose personal information to the company. It also helps potential customers decide whether or not to transact with the company in question (Culnan and Milberg, 1998). Hence, we sought to establish the extent to which the selected European firms actually inform their customers about the existence and nature of their privacy policies through on-line posting. In the US, firms' privacy policies are normally posted directly on their main websites, however some European firms tend to publish their privacy policies under "Terms and Conditions" or "Legal Notes", making them less accessible to consumers.

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

Table 3. Published Privacy Policy

Our results clearly show that UK again leads the list with 76% of the company websites 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 Policies: Content

Usually privacy policies provide the consumer an option to "opt out" of a newsletter or promotional events, offer the customer an option to inspect and correct data, describe provisions to third parties, notify how the data are stored, and indicate when personal information is discarded. These policies may also identify security measures which inform customers if "cookies" are used to track on-line habits. Following, we provide a brief description for each of these policy contents.

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 onto 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).

Opt in/opt out

Companies also give the customer a right to avoid receiving any promotions or stop any communication from the company's side, and even the ability 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 message, 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. These capabilities give the consumer control over how their personal data may be used.

Legal Notice

Legal notices play an equally important role in informing the customer about the company's responsibility towards the data collected on the site. Such notices make it clear that the website may contain links to other sites for which the company is not responsible. A company's limitation on liability and legal information about the exchange, release, publishing, and distribution of the data collected are explicitly delineated. It is very important that a customer dealing online with a company read the legal notice to understand the company's terms, conditions and liability.

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. Table 4 shows the percentage of companies in each country whose privacy policy contains information on cookies, opt in/opt out procedures, legal notices, and security.

	Germany	UK	France	Spain
Cookies	28%	57%	24%	34%
Opt-in/opt–out policies	14%	21%	<5%	<5%
Notice	63%	89%	61%	76%
Security	48%	13%	15%	31%

Table 4. Privacy policies: content

UK companies ranked the highest in informing their customers about how and to what extent their personal information may be shared with other organizations. German companies noted security measures to protect user information on 48% of their sites. The opt-in/opt-out policies are still in the emerging phase. The percentage of company websites that mentioned the use of cookies was highest in the UK. In France, only about a quarter of websites surveyed informed customers that the firm stored cookies.

Privacy Seal/Certificate

Privacy certificates or logos allow companies and consumers to engage in trusted communications and e-commerce. Trust logos are awarded to company websites by independent review entities to confirm the presence of solid privacy policies, security practices and methods for transactions. Such logos boost consumer confidence in the company's site and are usually awarded, for a fee, after third-party verification. The major privacy logos that were noted in Europe were AECE, SSL, VeriSign, TRUSTe, PKI, ISIS, TrustUK, DMA, ISIS, IDIS, ABCE, DTI and 'Peace of Mind' Guarantee. Table 5 shows that not many leading European firms have privacy certificates endorsed by such a third party, however.

	Germany	UK	France	Spain
Privacy Seal/Logo	<10%	11%	10%	19%

Table 5. Privacy Logo

Spain took the lead in the percentage of companies that had privacy logos on their sites, while Germany had the smallest percentage of companies that employed a third-party certificate.

Accessibility

Publicly and prominently displaying a website's privacy policy statement imbues consumers with trust. However, finding a firm's privacy policy is not always an easy task. The table below displays the results. We rated a firm's privacy policy access as "easy" when three or fewer clicks were needed to reach their privacy policies; websites requiring four or more clicks were considered "difficult".

Access	Germany	UK	France	Spain
Easy	62%	70%	60%	76%
Difficult	38%	30%	40%	24%

Table 6. Easy Access

Spanish companies led in flexibility and ease of finding the policy on the site pages. 76% of the Spanish sites studied made it very easy for the user to find the privacy policy and a majority of them had privacy policies on their home pages. Some sites had the privacy policy embedded in the legal notice. The difficult-to-find privacy policies were located only in the companies' annual reports or on the investor relations, employment, or "contact us" pages, or had a vague policy mentioned on irrelevant pages.

US Comparison

To conclude the presentation of our findings with data collected in 2004, we offer a table displaying the results of a survey of the Fortune 50 American companies by Peslak (2005) with data collected in 2003.

	US 2003	UK 2004	Germany 2004	France 2004	Spain 2004
PPP (Published Privacy Policies)	94%	76%	63%	62%	74%
Legal Notice	94%	89%	68%	61%	76%
Choice	62%	NA	NA	NA	NA
Opt-out	86%	21%	14%	<5%	<5%
Cookies	79%	57%	28%	24%	34%

Access	57%	NA	NA	NA	NA
Security	74%	13%	48%	15%	31%
Privacy Logo/Seal	NA	11%	<10%	10%	19%

Table 7. Companies of US and five European Countries

Table 7 shows that the US has a great advantage in every aspect of data privacy measures. We also include a comparison table based on previous research (Massa-Mias *et.al*, 2007) for the same European countries with data collected in 2001. Table 8 shows a slight improvement for published privacy policies (PPP) in the four countries overall. It indicates significant differences in compliance with the EU DPD: Germany and UK have improved significantly, while France has declined slightly and Spain has remained the same. The results for easy access to privacy policies (EA) are mixed, but do not vary significantly.

	Germany		**UK**		**France**		**Spain**	
	2001	2004	2001	2004	2001	2004	2001	2004
PPP	59%	63%	75%	76%	61%	62%	71%	74%
DPD	12%	47%	43%	76%	58%	55%	62%	62%
EA	59%	62%	75%	70%	61%	60%	71%	76%

Table 8. Comparison between 2001 and 2004

CONCLUSION AND LIMITATIONS

The results of this study indicate that EU regulatory information protection policies are taken somewhat seriously in the four major European countries examined, but the level of adherence and transparency in communicating policies to customers, and reliance on external verification of compliance, vary significantly amongst these four countries. Based on our sample data, the UK is leading when posted privacy policies are compared to the Data Protection Act. Spain and the UK are almost equal in terms of the percentage of firms actually posting their privacy policies. While the content of privacy policies varied amongst sample firms in four countries, more than two thirds posted "Notice" about information collection. When compared to US firms, the data indicates that many more American firms are observing the privacy protection policies than Europeans, although Europeans seem to improve between data collections in 2001 and 2004. This study should help us better understand the trend over time and across the Atlantic.

One possible limitation of this study – as with any other empirical study- is the sample biases. The 425 firms were among the 500 largest interactive companies and may not be fully representative of how these four countries observe privacy in their e-commerce efforts as a whole.

The paper covers the study of websites of only four EU countries; we nevertheless expect that the percentages in the four countries studied significantly exceed those for the EU as a whole, with the widest margins between these four and the newest EU members. Finally, 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) would enable more widely generalizeable and nuanced conclusions to be drawn.

In the future, observations of business websites may be extended to other part of the world (Marsden, 2008). Given the heterogeneity of global legal frameworks and cultures, data from developed and developing countries outside of North America and Europe, such as China, South Korea, India, Australia, and Vietnam, where e-commerce is rapidly expanding,

could be considered. Furthermore, examining the organizational and technological means used by firms could provide a better indication of actual privacy practices.

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* Nov. 1st.
3. 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.
4. Ashrafi, N. and Kuilboer, J-P. (2007a). Implementation of Privacy Protection Policies: An Empirical Perspective. *Utilizing and Managing Commerce and Services Online*. CyberTech Publishing, 2007, Ch. IX: 187-204.
5. Ashrafi, N. and Kuilboer, J-P. (2007b). Is P3P an Answer to Protecting Information Privacy? *E-Business Innovation and Process Management*. CyberTech Publishing, 2007, Ch XV: 331-347.
6. Birnhack, M. D. (2008). The EU Data Protection Directive: An Engine of a Global Regime. Elsevier, *Computer Law and Security Report* 24: 508-520.
7. Bloom, P., Milne, G., Adler, R. (1994). Avoiding misuse of new information technologies: Legal and Societal Considerations. *Journal of Marketing*, 58, 1, 98-110.
8. Caudill, E.M. & Murphy, P.E. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy and Marketing*, 19, 1, 7-19.
9. Clarke, R. (1999). Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM*, 42, 2, 60-67.
10. Culnan, M.J., and Milberg, S.J. (1998). The Second Exchange: Managing Customer Information in Marketing Relationships. Georgetown University, Unpublished Working Paper.
11. 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.
12. Culnan, M.J and Bies, R.J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59, 2, 323-342.
13. 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.
14. 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
15. 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.
16. 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.
17. Federal Trade Commission (FTC) (2000), Privacy Online: Fair Information Practices in the Electronic Marketplace, Report to Congress, May.
18. Folger R. and Bies, R. J. (1989). Managerial Responsibilities and Procedural Justice. *Employee Responsibilities and Rights Journal*, 2, 79-90.

19. 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*, vol. 3: 141-183. Greenwich, CT: JAI: Press.
20. King, I. (2003). Online Privacy in Europe: New Regulation for Cookies. *Information and Communication Technology Law,* 12, 3: 225-236.
21. Kuner C. and Simpson, A. P. (2005). Managing Privacy Enforcement Risks in Europe. *Risk Management*, February, 1st: 42-44.
22. Laufer, R. S. and Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Development Theory. *Journal of Social Issues*, 33, 22-42.
23. Marsden, C. T. (2008). Beyond Europe: The Internet, Regulation, and Multistakeholder Governance – Representing the Consumer Interest? *Journal of Consumer Policy*, 31, 115-132.
24. Massa-Mias G., Ashrafi, N., Koehler W., and Kuilboer J-P. (2007). Privacy Policy Regulations- An Empirical Investigation. 38th Annual Meeting Decision Sciences Institute, November 17-20, Phoenix, AZ.
25. Milne, G. R. and Culnan, M. J. (2004). Strategies for Reducing Online Privacy Risks. Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing*, 18, 3, 15-29.
26. 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.
27. 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 (Fall), 206-215.
28. O'Brien, K. J. and Cramton, T. (2007). Berlin– European Union Warns Google on Possible Violations of Privacy Law. *New York Times*, May 26th: C3.
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. Peslak, A. (2005). Internet Privacy Policies: A Review and Survey of the Fortune 50. *Information Resources Management Journal*, 18, 1, 29-41.
32. Rogers, K. M. (2004). The Privacy Directive and Resultant Regulations? The Effect on Spam and Cookies, Part I. *Business Law Review*, 25, 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. Wang, H., Lee, M. K., and Wang, C. (1998). Consumer Privacy Concerns about Internet Marketing. *Communications of the. ACM*, 41, 3, 63-70.
38. Warren, S. D. and Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, IV (5):193-220.
39. 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.*
40. Westin, A. F. (1967). *Privacy and Freedom.* New York: Athenaeum.
41. Whitman, J. Q. (2004). The two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal*, 113: 1151–221.
42. Zahedi, F. and Song, J. (2008). Dynamics of Trust Revision: Using Health Infomediaries. *Journal of Management Information Systems,* 24, 4, 225-248.