Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics, Istanbul, Turkey, May 27-29, 2006 (pp309-314)

Privacy Online: Research and Recommendations

ELEUTHERIOS A. PAPATHANASSIOU
Business Informatics Lab
Department of Business Administration
Athens University of Economics and Business
76, Patission Str., GR10434 Athens
GREECE
http://www.bilab.aueb.gr

XENIA J. MAMAKOU
Business Informatics Lab
Department of Business Administration
Athens University of Economics and Business
76, Patission Str., GR10434 Athens
GREECE
http://www.bilab.aueb.gr

DIMITRIS K. KARDARAS
Business Informatics Lab
Department of Business Administration
Athens University of Economics and Business
76, Patission Str., GR10434 Athens
GREECE
http://www.bilab.aueb.gr

Abstract: The Internet has created a tremendous opportunity to access a large amount of products, services and information easily in a fast and easy way. At the same time, websites collect personal information (PI) from consumers, in order to fulfil their requests for certain products and services, to send them information, to customise the content and advertise the site etc. The collection of personal data raises some privacy issues that need to be examined. This paper, briefly explains the content of the most important privacy principles, posted since 1973, it makes a proposal on the "Legal and Ethical Website Guidelines" that should be applied when designing a website that collects PI and reports the results of a 100 websites survey that investigates the extent of the proposed guidelines implementation.

Key-Words: E-commerce, Information privacy, Privacy law, Data collection, Personal information, Privacy Policy, Privacy guidelines

1 Introduction

The World Wide Web forms an exciting new market for consumers, since it offers an easy access to a large amount of products, services and information, much faster than in the past. The Internet technologies are also used to collect, use and disclose information of any form, even related to the consumers' behaviour, at a low cost. Personal data is used for business purposes prior to the Internet emergence. The advent though of the Web has led to the development of eCommerce, has increased the flow of personal information (PI), and almost simultaneously has increased the level of concern, with regard to the protection of the personal data [1].

Although there is not a great difference between the nature and use of data that is collected through the Web and the data collected through traditional ways, the consumers are worried about their personal information that is collected by commercial web pages. [2]. Many researches have reported the customers' concerns for the possible misuse of their personal data during their transactions on the Internet. [3], [4], [5].

Since 1973, there have been a number of guidelines, principles, conventions, directives, acts and reports trying to form a framework that should be followed by the organisations that collect personal information.

This paper briefly explains the content of the most important privacy principles, highlighting their similarities and differences. This study also proposes guidelines regarding legal and ethical issues of website design. Finally, it reports on the results of a 100 websites survey that investigates the extent to which the websites in the sample follow the proposed guidelines. The findings of this study are useful to both researchers and websites designers.

2 Privacy Principles and Regulations

This part of the paper presents the privacy principles and regulations since 1973, both in the USA and the EU, explaining their main content and enforcement.

2.1 Hew Report, 1973

In 1973, "The Secretary's Advisory Committee on Automated Personal Data Systems" within the Department of Health, Education, and Welfare, studied the record keeping practices in the computer age. The content of its report, known as "Hew Report", summarises that an individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. The "Hew report" advocated the existence of the "fair information practices" that discussed matters of data collection, usage and security, as well as the individual's rights of data access and correction. [6].

2.2 OECD Guidelines, 1980

In 1980, the Organization for Economic Cooperation and Development (OECD) adopted the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", in support of the three principles that bound the member states of the OECD: the pluralistic democracy, the respect on human rights and the open market economies.

The OECD Guidelines include eight privacy principles which are: the collection limitation principle, the data quality principle, the purpose specification principle, the use limitation principle, the security safeguard principle, the openness principle, the individual participation principle and the accountability principle [7].

All the above principles, that were implemented on 23 September 1980, are recognised by the OECD members, including the EU and the USA, they are not legally bound and are differently implemented by each nation.

2.3 Council of Europe Convention, 1981

The Council of Europe elaborated the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" [8] in order to reconcile the two fundamental rights, the private life and the information [9], and to ensure the same level of protection of these rights beyond the national borders, by legally binding the member states that certify it.

The Convention designates a number of principles for the fair and legal collection and use of data. More specifically, it states that personal data can only be legitimately collected and processed and can only be used for a specific reason. The data must be accurate and secure and it must be securely kept for only as long as it is necessary. The Convention also establishes the right of an individual to know whether personal information is stored, as well as the right of knowledge of the identity and the natural address of the person or organisation responsible for the data processing.

2.4 United Nation Guidelines, 1990

The United Nations General Assembly adopted the "Guidelines Concerning Computerized Personal Data Files" on 14 December 1990 [10]. These Guidelines included the Principle of lawfulness and fairness, the Principle of accuracy, the Principle of the purpose-specification, the Principle of interested-person access, the Principle of non-discrimination, the Power to make exceptions and the Principle of security.

2.5 IITF Report, 1995

In June 1995, the US Secretary of Commerce Ronald H. Brown, President of the White House Information Infrastructure Task Force (IITF), announced a report on the Privacy and the National Information Infrastructure. The report that was administered by the IITF Working Group on Privacy, explains the Principles for providing and using personal information.

The principles proposed by the IITF Working Group on Privacy, are separated in the general principles for all the National Information Infrastructure (NII)

participants, the principles for the users of personal information and the principles for the individuals who provide personal information [11].

2.6 EU Information Directive, 1995

On 24 October 1995, the European Parliament and the Council announced the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The goal of this Directive was the protection of the fundamental freedoms and rights of natural persons and in particular their right to privacy, with respect to the processing of personal data. [12].

The EU Information Directive states rules on the lawfulness of the processing of personal data, relating to data quality, to the criteria for making data processing legitimate, to the information to be given to the data subject, to the data subject's right of access to data and to the confidentiality and security of the processing.

2.7 Federal Trade Commission Report, 1998

The Federal Trade Commission (FTC) is an independent service, which was created by the Federal Trade Commission Act of 1914, having as its goal the consumers' protection from unfair or misleading commercial acts.

In 1998 it published a report entitled "Privacy Online: A Report to Congress", summarising the Fair Information Practice Principles, which were the five core principles of privacy protection and included notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress, and were common to all the previous documents [13].

The same report displays the results of the first Commissions study on the implementation of the Fair Information Practice Principles by the commercial websites. The results showed that although the great majority of the websites (85%) collected private information, only 14% of the sample provided information about their tactics and only 2% provided a comprehensive Privacy Policy.

2.8 EU Information Directive, 2002

On 12 July 2002, the European Parliament and the Council announced the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, which is known as the Directive on privacy and electronic communications.

The scope of the Directive was to harmonise the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector. Moreover, the aim was to ensure the free movement of personal information and of electronic communication equipment and services in the Community [14]. The provisions of this Directive particularise and complement Directive 95/46/EC.

2.9 Online Privacy Protection Act of 2003

"Online Privacy Protection Act of 2003", which was presented to the US Congress on 7 January 2003, prohibits the collection, use or disclosure of personal information without notification from the website, with regard to the identity of the operator, what personal information is collected by the operator, how the operator uses such information, and what information may be shared with other organisations.

Furthermore, it requires the users' to consent to or limit the disclosure of personal information. Additionally, it demands from the operator to provide a list of all the PI that is been sold or transferred, upon request of an individual who has provided PI. Finally, it requires from the operator to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of PI it collects or maintains [15].

3 Legal and Ethical Website Guidelines

It is obvious that from the "Hew Report" of 1973, till the Online Privacy Protection Act of 2003, there has been made a great effort from the European Union, the USA and the United Nations, for safeguarding PI that is collected through the traditional ways, as well as via the Internet.

The guidelines of all the privacy principles and regulations share some common characteristics in all cases, such as the call for the safeguard of the integrity, and the security of the personal data. However, they exhibit also some differences, which pertain to the right of individuals to have access to their PI, which is collected by a third party.

Taking into consideration all the above regulations, it is possible to create a list of guidelines that should be implemented by all websites that collect PI, in order to be considered as legitimate for their visitors in legal and ethical terms.

The following list is a recommendation regarding the legal and ethical guidelines (hereinafter "Legal and Ethical Website Guidelines") that should be followed by the designers of the commercial websites that collect PI.

1. Collection of personal data Principle
According to the first principle, PI must be collected only after the data subject's consent. In addition a relevant notification must be published on the website. The data subject must be informed about the kind of the personal data that is collected and about the ways that are used for the data collection.
2. Purpose of collection Principle
The PI must be collected under concrete, specific and legal purposes and its subsequent processing must comply with these purposes.
3. Data accuracy Principle
The personal data must be accurate, current and in accordance to the purpose of its collection.
4. Consent Principle
The PI can be processed and used only with the data subject's consent. The websites must provide choices about whether and how the personal data can be used for purposes other than the initial ones.
5. Awareness Principle
The data subject must have the right to know if its personal data has been collected and processed and if any PI has been sold, disclosed or transferred to third parties.
6. Access-modification Principle
The data subject must have the right to access its data that has been collected and to correct or modify the file that contains its PI.
7. Security Principle
The processing operators must take reasonable steps to safeguard the integrity and security of the personal data, both during the input and transfer of the data, and during their storage.
8. Notice Principle
The data subject should be informed through the website about the identity and the natural address of the organisation that collects personal data, as well as about ways of communicating privacy issues.

All websites should share a common design element i.e. to present all the necessary information in a simple, sufficient and comprehensible way, in order to ensure uniformity among websites and to prevent any users' difficulties in finding information concerning the above guidelines. This common element can be the Privacy Policy, which must be visible in all websites.

4 Research on the Implementation of the Guidelines

In order to find whether the websites that exist nowadays collect personal information and to find the degree in which they implement the "Legal and Ethical Websites Guidelines", an exploratory research took place.

4.1 Research methodology

An instrument was used to collect data regarding the extent to which the selected 100 websites meet the proposed guidelines. In order to minimise bias in collecting data, a group of 124 students from the Athens University of Economics and Business was trained and asked to answer the questionnaire. Each student was given a list of six websites to evaluate from the "top 100 sites" according to www.web100.com. Provision was made so that students do not fill in data for the same list of websites. However, in order to minimise errors in data collection, the lists of websites given to students were designed to that each website was evaluated on average 7 times by the 124 students. The top 100 websites represent business sectors, such as entertainment, commerce, education, health, technology etc.

The instrument consisted of three basic issues that focused on:
1. The number of websites that collect personal information from their visitors, along with the type of the PI.
2. The number of websites that include a Privacy Policy.
3. The degree in which the websites implement the "Legal and Ethical Websites Guidelines".

In order to ensure the accuracy of the results, the answers of each question from each student were compared against each other. In the case of discrepancies in answers for the same website, the specific website was evaluated once more. SPSS 12 was used to check the data consistency and to perform the data analysis.

4.2 Analysis of the Results

From the 100 websites that were evaluated, 7 were found unsuitable for further examination, since they either had the same URL with another website, their access was impossible, they targeted "adults" only, or they were Business to Business (B2B) sites.

The analysis of the remaining websites (93) showed that 87 sites (93,5%) collect PI, while all of them collect at least the visitor's e-mail address. Apart from the list of possible PI types that was mentioned in the evaluation form, 19 websites collect a different type of personal data, such as driver's license number, passport number, nationality, religion, bank account number etc. Table 1 shows the types of PI collected by the examined websites.

Data type	No of websites	Percentage
Name	83	95,4%
E-mail	87	100,0%
Address	76	87,4%
Zip code	76	87,4%
Phone	64	73,6%
Fax	17	19,5%
Credit card	58	66,7%
Age	49	56,3%
Gender	41	47,1%
Education	10	11,5%
Occupation	32	36,8%
Income	17	19,5%
Interests	34	39,1%
Other	19	21,8%

Table 1 – Type of collected PI (base=87)

From the 87 websites that collect PI, 85 post a Privacy Policy, 91,8% of which on their Home Page and 89,4% on at least one page that collects personal data.

Further analysis of the results showed the degree in which the websites implement the "Legal and Ethical Websites Guidelines". Table 2 shows the number and percentage of the websites that post a Privacy Policy and completely implement each one of the proposed guidelines.

Table 2 shows that the Guidelines with the greatest implementation are the "Purpose of collection Principle" and the "Data accuracy Principle". The same Table also shows that the "Awareness Principle" is not totally implemented by any website and as a result, it forms the Guideline with the biggest implementation problem.

Website Guidelines	No of websites	Percentage
1. Collection of personal data	78	91,8%
2. Purpose of collection	82	96,5%
3. Data accuracy	82	96,5%
4. Consent	70	82,4%
5. Awareness	0	0,0%
6. Access-modification	51	60,0%
7. Security	27	31,8%
8. Notice	53	62,4%

Table 2 – Websites that post a Privacy Policy and completely implement each Guideline (base=87)

The frequency of the Guidelines implementation on websites is a very important research result. Table 3 shows the number and the percentage of the sites that apply from none, to all eight Guidelines.

From Table 3, it is seen that 2,4% of the websites in the sample does not implement any of the proposed Guidelines, while 0% implements all eight Guidelines. The largest percentage of the evaluated websites (30,6%) applies 6 of the Guidelines, while the overall image shows a great space for improvement of the "Legal and Ethical Websites Guidelines" implementation.

Implemented Guidelines	No of websites	Percentage
0	2	2,4%
1	0	0,0%
2	2	2,4%
3	6	7,1%
4	14	16,5%
5	18	21,2%
6	26	30,6%
7	17	20,0%
8	0	0,0%
Total	85	100,0%

Table 3 – Frequency of Guidelines implementation (base=87)

4.3 Further work

In order to ensure the validity of the research outcomes, two more website samples were evaluated about the extent of the Guidelines implementation. For this purpose, two samples of 15 sites each were used, taken from the list of "top 100 websites in English" of Alexa Internet [16]. All 30

websites (different from the first research's 100 sites) were evaluated by the use of the same evaluation form, they collected PI and they posted a Privacy Policy.

The results of the two new samples were very close to the results of the first research, indicating the "Purpose of collection Principle" and the "Data accuracy Principle" as the highest implemented Guidelines and leaving the "Security Principle" and the "Awareness Principle" at the bottom level of development.

It is important to notice though, that all three studies showed the degree of the Guidelines implementation, as presented in the websites' Privacy Policies and they do not necessarily reflect how privacy issues are indeed treated by the organisations that collect personal information.

5 Conclusion

This paper discussed the content of the most important privacy principles, both in the EU and the USA, it suggested the "Legal and Ethical Website Guidelines" that should be implemented by websites that collect PI and presented the results of a survey made on 100 websites, investigating the extent of the proposed guidelines application. The results of the research revealed space for improvement regarding the implementation of the Guidelines, as presented in the Privacy Policies.

References:

[1] Volokh E., Personalization and privacy, *Communications of the ACM*, Vol. 43, No. 8, August 2000, pp. 84–88.

[2] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace*. A Report to Congress, May 2000.

[3] Forrester Research, *Forrester Technographics Finds Online Consumers Fearful Of Privacy Violations*, October 1999. Available at http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html. Last accessed 22 September 2005.

[4] Earp JB, Baumer DL, Innovative web use to learn about consumer behavior and online privacy, *Communications of the ACM*, Vol. 46, No 4, April 2003; pp. 81-83.

[5] Furnell, S.M., and Karweni, T., Security implications of electronic commerce: A survey of consumers and businesses, *Internet Research*, Vol. 9, No. 5, 1999, pp. 372–382.

[6] The Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, The United States Department of Health, Education and Welfare's seminal, July 1973.

[7] Organisation for Economic Cooperation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Privacy Online, *OECD Guidance on Policy and Practice*, 23 September, 1980.

[8] Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981.

[9] Council of Europe, *European Convention of Human Rights*, 1950.

[10] United Nations, *The Guidelines Concerning Computerized Personal Data Files*, adopted by the General Assembly, 14 December 1990.

[11] The Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, 6 June, 1995.

[12] Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Directive 95/46/EC of the European Parliament and of the Council*, 24 October, 1995, Official Journal of the European Communications, No. L. 281/31-95, 23 November, 1995.

[13] Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998.

[14] Directive on privacy and electronic communications, *Directive 2002/58/EC of the European Parliament and of the Council*, 12 July, 2002, Official Journal of the European Communications, No. L. 201/37-47, 31 July, 2002.

[15] *Online Privacy Protection Act of 2003*, 108th Congress of the United States of America, 1st Session, H.R. 69, 7 January, 2003.

[16] Alexa Internet, *Top Sites English*, http://www.alexa.com