11-17-2003

Differences in Privacy Policies Among Commercial, Educational and Governmental Web Sites: A Cross-Sectional Content Analysis

Rashad Bayramov

DIFFERENCES IN ONLINE PRIVACY POLICIES

Differences in Privacy Policies Among Commercial, Educational and Governmental Web Sites:

A Cross-Sectional Content Analysis

Rashad Bayramov

Paper Presented in Partial Fulfillment of the Master of Science Degree in Communication & Media Technologies

Rochester Institute of Technology

November 17, 2003

The following members of the thesis committee approve the thesis of
Rashad Bayramov on November 17, 2003

Dr. Rudy Pugliese
Communications Department Thesis Advisor

Tona Henderson
College of Computing Information Sciences
Advisor

Dr. Bruce Austin
Communications Department Chair

Permission From Author Required

Differences in Privacy Policies Among Commercial, Educational and Governmental Web Sites:
A Cross-Sectional Content Analysis

I, Rashad Bayramov, prefer to be contacted each time a request for reproduction is made. If permission is granted, any reproduction will not be for commercial use or profit. Please contact the Rochester Institute of Technology's Department of Communication for my updated contact information:

Rashad Bayramov

11/17/03
Date

To my mother and father,
whose love, encouragement, and advice
have made this possible.

Table of Contents

Abstract

The present study investigates the differences in the way commercial, educational and governmental Web sites communicate their informational privacy practices through the privacy policies posted on the Web. Specifically, the research identifies differences in the coverage of the Fair Information Practice principles within the analyzed privacy policies.

The study suggests that the sharpest dissimilarity exists in the coverage of the principles of Access (allowing Web users to review and update the data collected about them) and Security (protecting users' personal information during transmission and subsequent storage), where commercial sites greatly outnumber educational and governmental sites. However, governmental and educational sites use personal information for secondary purposes or share the information with third parties less frequently than commercial sites.

Commercialization of the Internet has brought multiple and unprecedented opportunities both for online users and Web site owners. The appearance of Web sites trading in almost all imaginable commodities and providing a plethora of information on various topics has extended the abilities of consumers to locate and retrieve information. At the same time, the development of online technologies has allowed Web site owners to expand their ability to gather personal data about Web users and develop extensive user profiles (Garfinkel, 2002). The often persuasive and overly inquisitive nature of data collection practices on the Internet, especially with regard to personally identifiable data collected by Web sites from their customers, has prompted negative feedback from ordinary users and ignited numerous advocacy campaigns demanding fair privacy practices online (Lemos, 2000; Schwartz, 2000).

According to the 1998 survey by Business Week and Harris & Associates, protecting personal information on the Internet ranked as the main reason "people stayed off the Web - above cost, ease of use, and annoying marketing messages." The survey reveals that when Web site operators do post privacy policies, "people are still wary": 33% do not trust the policies while 58% are "a little more at ease." Moreover, 62% are "not willing at all" to share any personal information online that may be used for targeted marketing messages and 58% are concerned that the content of their communication will be read by some other person or organization without their knowledge or consent (Business Week & Harris, 1998).

The present study investigates the privacy practices of commercial, educational and governmental Web sites with respect to collection of personal data from users. The

goal of the study is to determine the differences in the way three Web site categories communicate their privacy practices through the privacy policies posted on the Web. To be more specific, it aims at identifying differences in the coverage, within the privacy policies, of basic principles of the Code of Fair Information Practice, a document frequently used by privacy advocates to set standards of desired privacy protection for consumers' personal information. The study also investigates the coverage by privacy policies of three more issues that are not directly a part of the Code's principles but are salient in terms of privacy protection on the Internet. These include the disclosure of information to third parties, the use of cookies, and the publishing of Web site's contact information.

The primary reason to suspect dissimilarities in privacy policies among three Web site categories is the absence (in the United States) of a common set of privacy disclosure standards required from all Web sites irrespective of domain name extension. Several institutions advocating privacy protection for Internet users have established their own criteria for judging online privacy policies and use their own mechanisms to verify compliance. The comparison of results of two recent research projects also suggests that governmental and commercial Web sites may attach different degrees of importance to the coverage of basic privacy issues (Federal Trade Commission [FTC], 2000; General Accounting Office [GAO], 2000).

The present study analyzes and further compares the content of privacy policies of random samples of commercial, educational and governmental Web sites. The use of a common mechanism to assess privacy policies ensures outcomes in the form of

comparable factual data on coverage of every privacy issue under analysis for all three domains. This is critical since no previous studies have produced comparable statistics covering all major privacy issues for the three domains.

Historical Development of the Notion of Privacy

Privacy as a sentiment, a wish not to be intruded upon, has been most likely known to humankind for a long time, even before it was given a name. John Locke, the influential 17th century British philosopher, believed that privacy was one of the pre-societal natural rights and was preserved when people agreed to form a society by social contract (Locke, 1956). According to Alan Westin (1970), framers of the American constitution also recognized, though indirectly, the right of privacy via a number of amendments in the Bill of Rights including the right not to have to speak, the right of anonymous and pseudonymous expression, and privacy of opinion in the First Amendment; prohibition of quartering of troops in private homes during peacetime without the owner's consent in the Third Amendment; guarantees of personal security against unwarranted searches and seizures in the Fourth Amendment; and privileges against self-incrimination in the Fifth Amendment (Westin, 1970).

Westin further asserts that American society before to the Civil War had an effective set of rules to protect any individual or a group from the then privacy violations of the time. However, the advent of new technologies – the telephone, the dictograph, and photography – and the rapid development of the mass media posed new challenges to privacy protection. It is at this time in American history that two Boston lawyers, Samuel D. Warren and Louis D. Brandeis, published an article in the 1890 edition of *Harvard*

Law Review proposing to legally recognize the right to privacy – the right that should protect "persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity" and "protect all persons ... from having matters which they may ... prefer to keep private, made public against their will" (Warren & Brandeis, 1890, para. 30).

The article by Warren and Brandeis served as the basis for hundreds of legal cases in the century that followed and is considered one of the most influential law review articles ever published (Gregory & Kalven, 1969, p.883). The lawyers framed their argument in terms of "the right to be let alone" (Warren & Brandeis, 1890, para. 1). This right stands supreme and apart from other possible considerations; it presumes that all people can be left alone as much as they desire without restricting others' abilities to exercise their own right to privacy. Inspired by Warren and Brandeis's libertarian thinking some authors later referred to privacy as a "fundamental" and "inalienable" right (Etzione, 1999, p.190).

However, the libertarian view of privacy did not continue to exist without its critics. Representatives of the communitarian school of thought questioned the "inalienability" of the right to privacy by indicating its potential harm to the public good. William Lund (1997) observed that "...any citizen who manages to get an interest wrapped in the cloak of a right appears to have an absolute claim against other considerations" (p. 104). Louis Henkin (1974) made another communitarian point by stressing that "consideration has focused on defining the private right of privacy, with little regard to our other balance, the competing public good" (pp. 1429-1430).

Clarke (1999) provides a contemporary definition of privacy as "the interest that individuals have in sustaining a "personal space," free from interference by other people and organizations" (para. 5). Four major dimensions in privacy are differentiated: privacy of the person, privacy of personal behavior, privacy of communications, and privacy of personal data.

Privacy of the person, also known as bodily privacy, is concerned with the integrity of the individual's body. This dimension covers such issues as, for example, compulsory immunization and blood transfusion without consent. Privacy of personal behavior relates to all aspects of behavior, and especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices. Privacy of personal communications refers to an individual's ability to communicate with others, using various media, without routine monitoring of the communications by other persons or organizations. And finally, privacy of personal data, which is the main area of concern for Internet users and the focus of the present study, stands for a substantial degree of control people can exercise over disclosure of data about themselves to third parties.

Although scholarly debates over the definition of privacy continue even today, the right of privacy has been successfully recognized in all but four American states. Violations of privacy are currently represented by four torts in American law: appropriation, intrusion of privacy, publication of private information, and false light privacy (Pember, 2003). For the purpose of this study we will concentrate only on intrusion, as it appears to be the most frequent practice of invasion of information privacy on the Internet.

In general, intrusion of privacy primarily concerns the collection of data about someone and is thus different from the other three privacy tort categories, which deal mainly with publication of data about an individual (Pember, 2003). One of the most important concepts related to intrusion of privacy is reasonable expectation of privacy; if someone gathered information about a person while the person was enjoying a reasonable expectation of privacy, the process can be qualified as an intrusion of privacy.

Intrusion of privacy in the Internet is different from people's usual understanding of privacy invasion in at least two aspects: Online users often do not know *who* is gathering information about them and *what* information is being gathered. The Pew Research Center for the People and the Press reports that 84% of people express some anxiety about giving out personal information online and 86% of Internet users believe Internet companies should get explicit permission before using personal data (2000).

History of Privacy of Personal Data in the Computer Age

The issue of informational privacy with respect to interconnected databases was first raised in the 1960s when consumer reporting agencies started computerizing credit, insurance and employment files. The files contained vast personal data assembled over years, often without consumers' prior consent or knowledge. In the 1960s and early 1970s, Congress heard testimony both from agencies collecting personal data and consumers who had received harm from inaccurate reporting. As a result, Congress passed a piece of legislation called the Fair Credit Reporting Act. The new regulations entitled consumers to see their credit reports and learn about the third parties to whom the reports had been sent (Garfinkel, 2002) and protected consumers from the disclosure of

inaccurate and arbitrary personal information held by consumer reporting agencies (*Fair Credit Reporting Act*, n.d.).

In 1968, the Russell Sage Foundation funded the Project on Computer Databanks of the Computer Science and Engineering Board, National Academy of Sciences. The project, directed by the renowned privacy researcher Alan Westin, examined the use of computers by governmental and private organizations for the purpose of collecting, processing, and exchanging information about individuals, as well as the impact of computerized records systems on the privacy of individuals. Some of the main recommendations of the final report were directly related to the issue of personal data privacy. Thus, the report recommended limiting compulsory data collection "so that matters that ought not to be considered in making decisions about individuals do not become part of records maintained about them." It also suggested providing individuals with greater rights to access records maintained about them and fashioning "new rules of data sharing and confidentiality" (National Academy of Sciences, Computer Science & Engineering Board, 1972, p.348-349).

In 1972, Secretary of Health, Education, and Welfare Elliot L. Richardson established the Secretary's Advisory Committee on Automated Personal Data Systems. The committee was tasked to analyze and prepare recommendations on four major issues: harmful consequences that may result from using automated personal data systems; safeguards that might protect against potentially harmful consequences that may result from using automated personal data systems; measures that might afford redress for any such harmful consequences; and policy and practice relating to the issuance and use of

individuals' Social Security numbers (United States Department of Health, Education, & Welfare [USDHEW], 1973).

The final report, issued in July 1973, recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems." The committee stated that such a code should define "fair information practice as adherence to specified safeguard requirements," "prohibit violation of any safeguard requirements as an unfair information practice," "provide that an unfair information practice be subject to both civil and criminal penalties," and "give individuals the right to bring suits for unfair information practices" (USDHEW, 1973, p. xxiii and 50).

By end of the same year, the Code of Fair Information Practice had been developed by the Advisory Committee and approved by the Nixon Administration. The Code stated that there must be "a way for a person to find out what information about the person is in a record and how it is used" and obligated data gathering agencies to provide individuals with mechanisms to correct inaccuracies in the collected personal information and to stop the flow of personal data to a third party initiated without the person's consent (USDHEW, 1973, p. viii).

The next landmark document on privacy protection was adopted in 1980 by the Organization for Economic Development and Cooperation (OECD) under the title OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The OECD Guidelines were built upon the existent Code of Fair Information Practice and expanded by including several new principles, such as the Security Safeguards Principle,

which stated that "personal data should be protected by reasonable security safeguards" (Organisation for Economic Co-operation & Development, 1980, Part 2, para.11).

In the mid 1990s, the Clinton Administration issued a set of recommendations in response to increasing privacy concerns of Internet users; among other things, online businesses were encouraged to post *privacy policies* on their Web sites (Garfinkel, 2002). A privacy policy is an electronic document, located on a Web site, that explains the Web site owner's practices of gathering data about users and how the owner utilizes this information. A Web site's privacy statement is, in a sense, a warning to potential and current users, informing them of what to expect from the site once the user has chosen to interact with it.

The appearance of privacy policies on the World Wide Web seemed to have a positive effect on users' reported level of anxiety during online interactions. Cranor, Reagle, and Ackerman (1999) found out that although approximately 87% of Internet users still experienced some level of discomfort related to Web privacy practices, 28% would be "more likely to provide" some personal information (such as name and postal address) to a Web site if the site had a privacy policy. In a more recent survey, 66% of respondents indicated "increased confidence" in the Web site if a privacy policy was present (Earp & Baumer, 2003). These and similar findings have evidently produced positive results as the reported number of Web sites posting privacy policies rose dramatically from 14% (FTC, 1998) to almost 67% (Culnan, 1999) within one year.

Although Web sites may differ in their privacy practices, online privacy watchdogs expect the sites to cover a certain number of standard issues within the posted

privacy policies. The standards for compiling privacy statements are, however, not unified across the World Wide Web. One of the most recognized authorities in the USA is the Federal Trade Commission (FTC), which enforces online privacy disclosure standards based on the four core elements of the Code of Fair Information Practice: *Notice*, which requires Web sites to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it, and how they use it; *choice*, which requires Web sites to offer consumers choices as to how their personal information is used beyond the use for which the information was provided; *access*, which requires Web sites to offer consumers reasonable access to the information they have collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information; and *security*, which requires Web sites to take reasonable steps to protect the security of the information they collect from consumers (FTC, 1998).

Several privacy advocacy groups, such as TRUSTe and BBBOnline, have established their own requirements for privacy policies. These organizations developed third-party oversight programs that attempt to alleviate users' concerns about online privacy through the establishment of licensed Web sites (TRUSTe, n.d.; BBBOnline, n.d.). The TRUSTe and BBBOnline standards for disclosure of a Web site's privacy practices are also based on the Fair Information Practices (FIP) although some requirements are extended to include specific issues, such as use of cookies (i.e., whether a Web site uses places cookies on users' hard drive), user registration process (i.e., a description of how the registration process works on a Web site), and contact

information. The Web sites that adhere to enforced standards of privacy practices disclosure receive a seal of approval placed on the site's home page. Like posted privacy policies, privacy seal programs have been found to increase users' willingness to share personal information with a Web site (Cranor et al., 1999).

Although the original 1998 FTC recommendations for disclosure of privacy practices concerned primarily commercial Web sites (FTC, 1998) they have nevertheless widely influenced all categories of U.S. Web sites to adopt and post privacy policies. Today consumers can find privacy statements not only on commercial but educational and governmental Web sites that gather personal data. These sites differ from one another by domain name extensions, such as ".com," which is most often associated with commercial entities (e.g., www.sony.com), ".edu," which is reserved for educational institutions (e.g., www.rit.edu), and ".gov," which is allocated to governmental agencies only (e.g., www.ftc.gov).

Commercial, educational and governmental entities serve distinctly different purposes in selling merchandise, providing higher education and enforcing state laws, respectively. Their online privacy practices may vary as well: Some of the sites may create extensive user profiles, while others may leave a user various options as to how much personal data the user is ready to divulge. The goal of this study is to determine the differences in the way three Web site categories communicate their privacy practices through the privacy policies posted on the Web. To be more specific, it aims at identifying differences in the coverage of fair information practice principles by online privacy policies on commercial, educational and governmental Web sites.

Research Question

Commercial, educational and governmental Web sites often post privacy policies to inform their visitors of the site's practices of treating sensitive personal data. Communication and computer technology scholars have studied the content of privacy statements of commercial (Culnan, 1999), medical (Goldman, Hudson, & Smith, 2000), and governmental (GAO, 2000) Web sites. However, a comparative cross-sectional study of privacy policies involving several Web site categories has yet to be completed.

The present study collects factual data from samples of commercial, educational, and governmental Web sites with the goal of comparing the content of the privacy policies of the three categories and identifying differences in the coverage of the principles of fair information practice on the surveyed Web sites. Thus, the main research question for the study is as follows: *What differences in the coverage of the principles of fair information practice are there among U.S. commercial, educational and governmental Web sites?*

The coverage of fair information practice principles is measured on the basis of data obtained as the result of content analysis of the privacy policies posted on the surveyed Web sites. A privacy policy is defined, for the purposes of the study, as a document describing the site's practices of handling personal information collected from Web users, placed at a certain location on the site, and accessible through a hyperlink (Fig.1 and 2).

Figure 1. **A fragment of eBay's (www.ebay.com) home page with a hyperlink to the privacy policy.**

This definition does not include informational practice statements defined as isolated statements that describe a particular use or practice regarding consumers' personal information and may appear in various locations on the site (Fig. 3).

The rationale for exclusion of isolated privacy statements from the scope of the study is the fact that such statements are often short, closely related to the context of the page on which they are placed, and consequently insufficient to prove the coverage of any fair information practice principle as defined for the study. For instance, if a certain page within a Web site contains the statement "*We will not sell your personal information to third parties*," several questions still remain unanswered: What is the site's definition

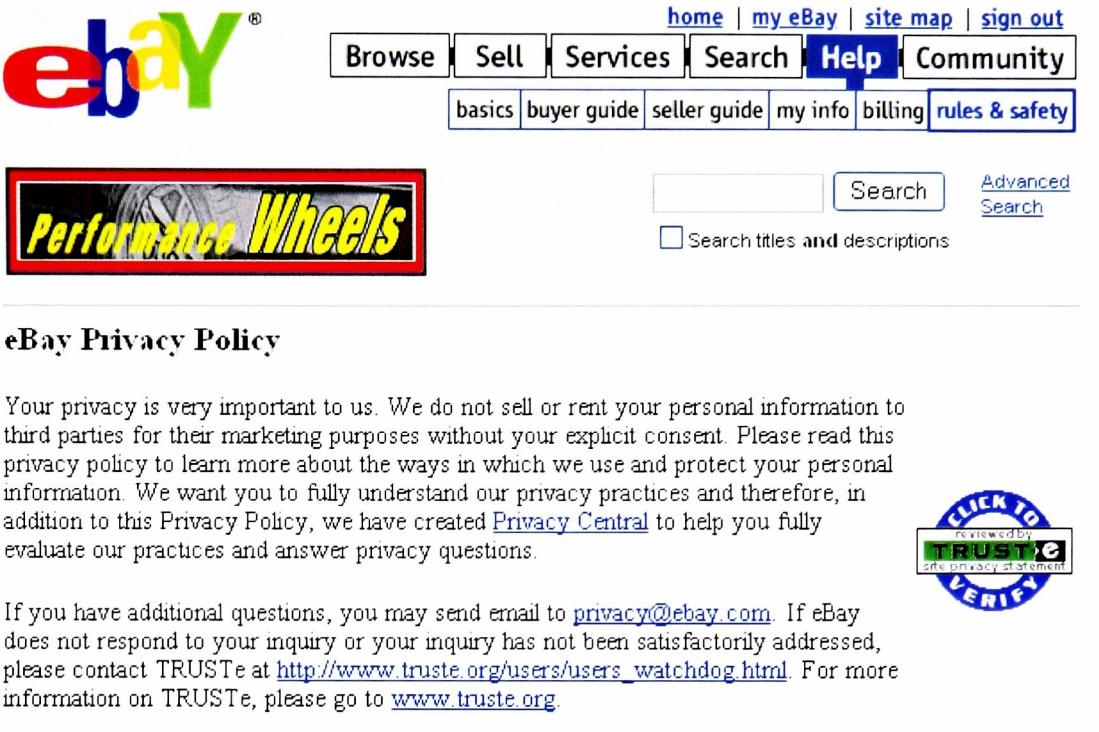

Figure 2. **An excerpt from eBay's privacy policy (http://pages.ebay.com/help/community/png-priv.html).**

of a third party? Is it any external entity or only a commercial enterprise? May the site share (as opposed to selling) personal information with third parties? Will the site disclose personal information to a governmental agency such as the FBI? Moreover, these isolated privacy statements often appear in conjunction with some product and/or service that the site offers to consumers and do not necessarily reflect the site's overall policy for handling personal information collected from users. For example, if a Web page collecting some customer data places the statement "*Your information will be kept*

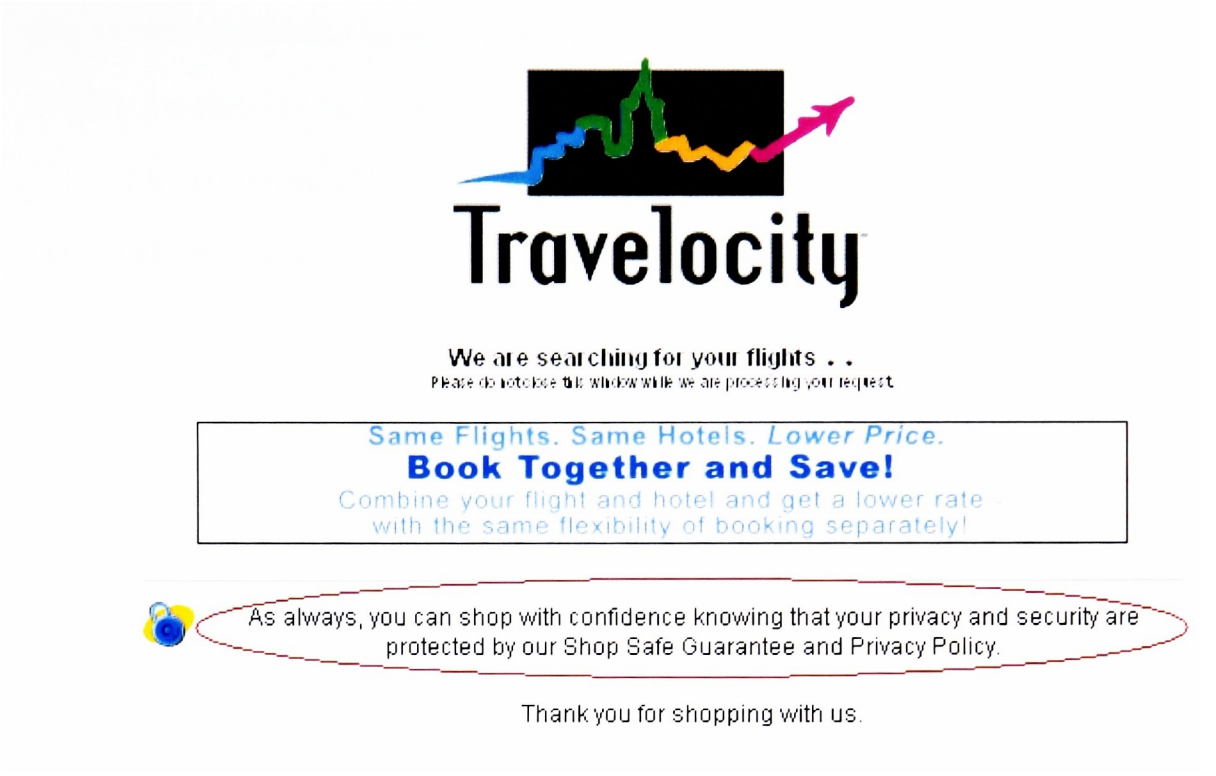

Figure 3. **A page from Travelocity.com with an informational practice statement.**

confidential," it is not yet clear if the promise refers only to the information submitted on that particular page or reflects the site's overall privacy policy.

The definition of a privacy policy also excludes University policies that discuss such matters as the proper use of computing resources, email privacy, and the sharing of personal information collected from students, faculty, and employees off-line. These notices appear on educational Web sites under different names, including Acceptable/ Appropriate Use Policy, Proper Use of Information Resources, Information Technology Policies, and University Policy Statement. Such a notice does not constitute a privacy policy as defined for the present study unless it discusses the practices of gathering electronically collected personal information via the school's Web site from users other

than University-affiliated parties (i.e., not students, faculty, staff, or donors) and the use of this information by the school.

The term "principles of fair information practice" is operationalized as the previously mentioned four core principles of the Code of Fair Information Practice (notice, choice, access, security) and the additional three issues of disclosure of personal information to third parties, use of cookies, and the posting of contact information.

The term "coverage" refers to the type of treatment individually specified, within the current study, for each fair information practice principle under analysis. A principle is "covered" if a privacy policy contains a statement(s) satisfying the operational definition for that principle. For instance, the principle of "access" is operationalized as including statements about whether a user can review, edit and delete at least some of the personal information provided to the site. If the privacy policy of a Web site contains a statement or statements indicating whether a user can review, edit and delete some personal information, the principle of "access" is considered as "covered" by that privacy policy.

The coverage of a fair information practice principle is considered partial if a privacy policy contains a statement(s) satisfying only some part of the operational definition. For example, if the privacy policy includes statements indicating whether a user can review his/her personal information but does not include statements indicating whether a user can edit or delete this information, the principle of "access" is considered "partially covered." The coverage is considered full if a privacy policy contains a statement(s) satisfying all elements of the operational definition, that is, for example, if

the policy contains statements indicating whether a user can review, edit and delete his personal information.

Thus, "notice" is defined as statements regarding what type(s) of personal information is collected, how it is collected, and how that information will be used.

"Choice" is defined as statements indicating that a Web site will ask for a user's consent and/or offer him/her a choice prior to sending him/her any communication or using his/her personal data beyond the use for which the information was provided (e.g., to complete a transaction).

"Access" is defined as including statements about whether a user can review, edit and delete at least some of the personal information provided to the site.

"Security" is defined as statements regarding the site's security measures to protect the collected personal information during transmission and subsequent storage.

"Disclosure to third parties" is defined as statements regarding whether personal information is disclosed to third parties and whether the site asks for a user's consent or offers him/her a choice prior to sharing his/her personal data with third parties.

"Cookies" is defined as statements explaining what a cookie is and indicating if the site uses cookies.

"Contact information" is defined as statements containing contact information that users may use if they have questions about their privacy and to complain in case of a suspected privacy violation.

The terms "commercial," "educational," and "governmental" combined with the expression "Web sites" also require operational definitions. For the purposes of the study

we will consider only those commercial Web sites that have a ".com" domain name extension and belong to a U.S. business.[1] The term "educational" refers only to those Web sites that have ".edu" domain name extension and belong to institutions of higher education (colleges, schools, universities) operating in the USA. The term "governmental" refers only to those Web sites that have ".gov" domain name extension and belong to U.S. governmental agencies.

Furthermore, educational Web sites are not considered in their entirety since they in many cases include a number of sites with a third-level domain name (e.g., business.harvard.edu) belonging to individual colleges, departments, libraries, health centers that make up the university. Only the major Web site, or a portal, that resides on a second level domain (e.g., www.harvard.edu), represents the entire University and usually acts as an entry point for many Web users interested in searching for University-related information is analyzed. Consequently, the privacy policies of portal sites (and not of individual colleges or departments) are considered in the research. The rationale for exclusion of individual college and department Web sites is in the fact that their privacy practice disclosures cannot be considered fully representative of the entire University policy.

Project Rationale

So far most research devoted to online privacy policies and conducted by communication, information technology and public policy scholars has focused on either the World Wide Web in general (FTC, 2000) or some specific professional categories

[1] This includes both businesses that originate in the U.S. (e.g., General Motors, PetSmart) and foreign companies that have U.S. operations (e.g., Sony USA, Hyatt Regency in Los Angeles)

such as medical (Anton & Earp, 2001) or financial (Center for Democracy & Technology [CDT], 2001) Web sites.

Another important limitation of the previous studies is the tendency to analyze primarily ".com" sites. The high interest towards ".com" domain has been quite consistent with the original FTC requirements of Fair Information Practice to be appropriated and followed by commercial Web sites (FTC, 1998). As a result, little research has been conducted on governmental Web sites (GAO, 2000), and literally no research is available regarding the privacy practices of educational sites.

Yet another limitation is the absence of comparable data on privacy policy compliance among major domains. The available research results for commercial and governmental Web sites are based on different methodologies and consequently not valid for direct comparisons. This shortage in comparable data becomes even more critical if one takes into consideration that no single study has yet tried to discover if the privacy policies are different across different categories of Web sites. In other words, no research has attempted to find out if there are any peculiarities in the way privacy practices are communicated to online audiences at commercial, educational and governmental Web sites.

One of the main reasons to suspect differences in the way the three Web site categories handle their privacy disclosures is the absence in the U.S.A. of a single regulatory institution setting standards of privacy practice disclosures for all Web domains and auditing the compliance with the standards. The FTC is the major source of recommendations and audit for commercial Web sites; however, its activity does not

cover governmental or educational Web sites. The General Accounting Office (GAO) of U.S. Congress audits governmental Web sites but does not oversee the practices of commercial or educational sites. Some sites follow the standards set by Internet privacy advocates, such as TRUSTe and BBBOnline, which have their own set of recommendations and auditing mechanisms. These inconsistencies in the content, volume and mechanisms of compliance measurement among U.S. privacy watchdogs may create favorable conditions for dissimilarities among Web site privacy policy disclosures.

The above-mentioned claim is not entirely conjectural. Two recent studies produced results that suggest possible differences in the way commercial and governmental sites cover four core principles of Fair Information Practices. A study of commercial Web sites by FTC reveals relatively close degrees of importance attached to each of the four FIP principles: 55% of the sites in the research sample comply with the category of notice, 50% comply partly with the category of choice, 43% - with the category of access, and 55% - with the category of security (FTC, 2000). A study of governmental Web sites by GAO demonstrates different attitudes the same FIP principles (GAO, 2000). The majority of federal sites (69%) meet FTC's criteria for notice, however, a smaller number of sites implement the three remaining principles of choice (45%), access (17%), and security (23%). Although the two studies have differences in their methodologies, the produced results indicate a potential for future studies to verify if the differences in the coverage of privacy practices are still discovered within a single comparative analysis.

It is also expedient to justify the necessity of considering educational and governmental Web sites together with commercial ones. Both educational and governmental sites may be (and often are) involved in collection of some personal data about their users, at least on some basic level (e.g., registering IP address, uploading cookies). Although they may or may not sell or otherwise disseminate the collected data to third parties, it does not diminish the salience of the fact that users can be profiled by these sites and therefore have the right to know the privacy practices of respective Web sites. Thus, analyzing the privacy policies of educational and governmental Web sites appears to be as important as the analysis of commercial sites.

Another argument in favor of selecting ".edu" and ".gov" Web sites as opposed to other popular domain name extensions, such as ".org" and ".net," is that all sites in ".edu" and ".gov" domains follow consistently applied eligibility criteria. The U.S. Government has reserved domain names with ".edu" and ".gov" extensions only for educational institutions and governmental agencies, respectively, and selected one managing organization for each domain.[2] Only eligible institutions can register a Web site in these two domains: ".edu" domain names are given to postsecondary institutions that are institutionally accredited by an agency in the U.S. Department of Education's list of Nationally Recognized Accrediting Agencies registered by U.S. Governmental (EDUCAUSE, n.d.), and ".gov" domain names can be entities, such as departments, programs, and agencies on the federal level, state governmental entities/programs, and

[2] EDUCAUSE manages '.edu' domain (http://www.educause.edu/edudomain/index.asp), and General Services Administration (GSA) is responsible for .gov domain (http://www.nic.gov/index.html).

cities and townships represented by an elected body of officials (General Services Administration, n.d.).

Registration for ".org" and ".net" domain names is crucially different from the procedures described above. Almost any institution or person, in or outside the U.S., can register a Web site in these domains. There are no clear-cut eligibility criteria enforced by any single federal or non-governmental organization in order to grant a domain name to an applicant. Instead, multiple commercial entities arrange for registration process for a certain fee, which has resulted in quite diverse ownership, ranging from individual amateurs to large profit institutions.

As the result of this diverse ownership, any study of privacy policies inside ".net" or ".org" domain will present difficulties in generalizing findings beyond the sample of Web sites. On the contrary, the integrity among ".edu" and ".gov" Web sites, which is the result of enforcing consistent eligibility criteria for all applicants, allows generalizing the outcomes of such research on the whole population of Web sites in the respective domains.

Given the above-mentioned concerns and considerations, the scholarly rationale behind the study is to follow up the previous privacy policy analyses by extension beyond commercial Web sites. Considering various Web site categories within a single research work will fill in a gap in the current scholarly knowledge on comparative cross-sectional Web site statistics with respect to privacy policy disclosures.

From a social perspective, the study produces valid factual data on the content of privacy policies of three important categories of Web sites, which may form the basis for

recommendations to Internet privacy policy makers involved in designing such privacy disclosures. Specifically, the research produces data on the previously insufficiently studied categories of educational and governmental Web sites.

The study will help relevant governmental agencies (e.g., FTC) and advocacy groups (e.g., TRUSTe, Online Privacy Alliance) to consider further improvement in education on online privacy issues for Web site owners as well as suggest some methodological changes in evaluation mechanisms of Web site privacy policies, specifically by shifting the focus from purely commercial to educational and governmental Web sites.

Literature Review

The first comprehensive and widely publicized study of online privacy disclosures of commercial Web sites was conducted by the FTC in 1998. One of the major objectives of the research was to determine the conformity of posted privacy statements and policies with the core principles of Fair Information Practices – notice, choice, access, and security (FTC, 1998, p. 27). Within the framework of the study, a group of FTC staff members were instructed to conduct an online content analysis of approximately 1400 commercial Web sites and analyze the sites against a set of questions posed in the questionnaire (FTC, 1998, p.19).

Six samples were evaluated: commercial U.S. sites "likely to be of interest to consumers" (group A), such sites in the health, retail, and financial sectors (groups B, C, and D, respectively), commercial U.S. sites "primarily directed to children aged fifteen or younger" (group E), and the most popular U.S. commercial sites (group F) (FTC, 1998,

Methodology section, p. 1). The sampling process was as follows. First, the researchers identified the best available listing of sites to represent each of the six target populations. The listings served as sampling frames.[3] A sampling interval was then used to randomly select sites from each sampling frame for inclusion in each group's respective sampling pool. Finally, sites in each of the six sampling pools were randomly examined until the number of qualifying sites in each group met or exceeded the target sample sizes (FTC, 1998, Methodology section, p. 4).

The surfers searched sites in the final samples to determine whether each site collected personal information from users and, if so, what kind of information was collected and whether the site disclosed its information handling practices. For the purposes of the study, "personal information" was defined to include two categories: personally identifying information – "information that can be used to identify consumers, such as name, postal address or e-mail address," and demographic and preference information, such as age, gender, income level (FTC, 1998, p. 19-20).

The study found that the majority of sites in all samples – between 87% (children's sites) and 97% (most popular sites) – collected at least one type of personal information (Fig. 4).

---

[3] The Dun & Bradstreet Corporation's Electronic Commerce Registry database served as a sampling frame for groups A through D, Yahooligans! Directory for children's sites compiled by Yahoo – for group E, and a list of most popular sites provided by several sources (Media Metrix, The PC Meter Company, etc.) – for group F (Methodology, p.3)

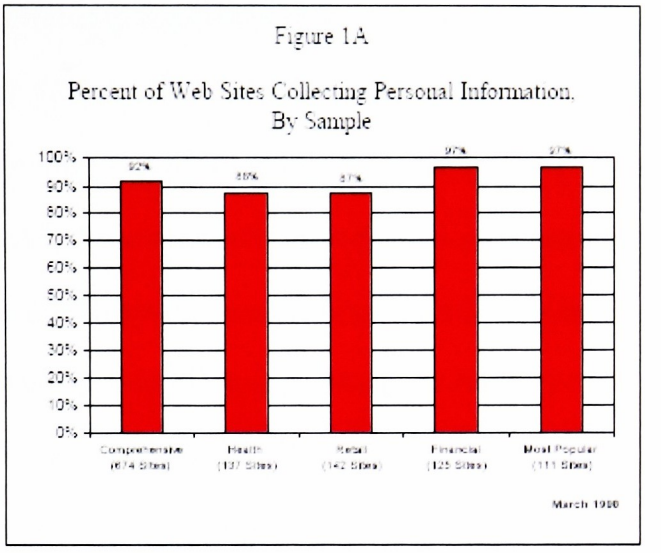

Figure 4. **Collection of personal information among Web sites by sample (from FTC 1998 Report to Congress).**

Almost all of the sites in Groups A through E that collect personal information gathered at least one type of personally identifiable information. This latter finding was very important: The presence of even one personally identifiable entry allowed Web sites owners to connect the remaining unidentifiable demographic information with a specific customer and thus opened prospects for building extensive user profiles (FTC, 1998, p. 33).

To determine if the sites gave proper notice and choice to their users related to information practices, the surfers looked for information practice disclosures. These were divided into two types: a privacy policy notice and an information practice statement. A privacy policy notice was defined as "a comprehensive description of a site's information practices that is located in one place on the site and may be reached by clicking on an icon or hyperlink." An information practice statement was defined as "a statement that

describes a particular use or practice regarding consumers' personal information, or regarding a choice offered to consumers about their personal information, that might appear in diverse locations on the site" (FTC, 1998, p. 20).

The study revealed that of the Web sites in the first four samples (comprehensive, health, retail, financial) that collect personal information, the number of sites posting any information privacy disclosure (i.e., a privacy policy notice or an information practice statement) ranged from 13% (retail) to 16% (finance). Only 2% of sites in the four samples posted privacy policy notices (FTC, 1998, p. 27).

Furthermore, 84% of the surveyed children's sites were involved in collection of personal information from children, whereas only 10% provided for any mechanism of parental control over the collection and use of such information. It is noteworthy that the latter discovery had a big impact on the Congress, which by the end of the same year passed the Children's Online Privacy Protection Act (COPPA) requiring commercial Web sites to give parents control over handling of the personal information provided by their children.

Although the 1998 FTC Report to Congress provided a comprehensive explanation of Fair Information Practice principles, it did not specify the clear-cut operational definitions for the principles of notice, choice, access, and security. However, based on the questions in the content analysis and subsequent data analysis results it is possible to conclude that the researchers gave a site credit for notice if the site posted any information practice disclosure (FTC, 1998, p. 8). "Choice" was defined as any sentence indicating that users have a choice with respect to the use of the information by the site

beyond the original purpose for which the information was provided, for example, to complete a transaction, to subscribe to a newsletter. "Access" was considered as accomplished within the site's privacy practices if there was a statement that the site allowed a user to review or/and to edit at least some personal information provided to the site (FTC, 1998, p. 9). Finally, in order to receive credit for covering the principle of security, the site had to identify in its privacy disclosure whether it provided any security measures to protect personal information after such information has been received by the site (FTC, 1998).

As noted above, the number of sites providing users with some notice about their information practices ranged from 13% to 16% in the first four samples. The number was significantly higher for the samples of children's sites (54%) and most popular sites (71%). The following figures reflecting the coverage for the remaining three FIP principles refer only to the sites with at least one privacy disclosure. Thus, approximately one-third of the sites in each of the first four samples indicated that they provided consumers with a choice for how to use their personal information. The corresponding figures for the children's and the most popular site samples were 39% and 68%, respectively. The number of sites offering access and ability to correct things was very small: from 0% health and finance to 17% in retail. Security was promised in sites ranging from 0% in health to 15% (14 sites) in the comprehensive sample. Again, the corresponding figures for the most popular sample were higher (FTC, 1998, pp. 30-31).

Thus, the first comprehensive audit of commercial Web sites revealed significant flaws in the mechanisms of information privacy disclosures. Only 14% of sites in the

comprehensive sample (i.e., a random sample of U.S. commercial Web sites drawn, irrespective of type of business, from a comprehensive electronic commerce registry) provided at least some notice about their privacy practices to users. Only one-third of the sites in the 14% provided users with some choice with respect to the use of personal information gathered by the site. A little over 8% of privacy disclosures in the sample mentioned that they provided users with access to review and/or edit at least some collected personal information. Approximately 15% of sites promised to provide security to the personal information after that information had been received by the site (FTC, 1998, p.30).

Later surveys demonstrated slow but steady progress in the online industry's compliance with the FTC-promoted four core principles of Fair Information Practices. The heavily publicized Georgetown Internet Privacy Policy Survey, which was produced in June 1999 as a progress report to FTC, found that nearly 66% of commercial Web sites posted some form of privacy disclosure as opposed to 14% in the 1998 FTC survey. Yet, only 14% of the analyzed sites have complied with the four core FIP principles (Culnan, 1999).

The method for the Georgetown study was modeled after the 1998 FTC study but not in every aspect. One of the major differences – the one that primarily accounts for differences between the study findings – is the sample selection process (Culnan, 1999, p.2). The Georgetown study analyzed a random sample of 361 commercial U.S. Web sites drawn from a list supplied by Media Metrix of the 7,500 most visited URL's. The list was compiled on the basis of unduplicated traffic of at least 32,000 unique visitors

surfing the Web from home during January 1999 (Culnan, 1999, p. 3). The FTC study sampled 1,700 Web sites from the entire ".com" domain as presented in the Dun and Bradstreet database without consideration of the number of a site's unique visitors. Apparently, the sampling based on unique user "hits" introduced a significant bias in the Georgetown study findings as the most visited sites frequently belonged to large and financially secure businesses, which had a substantial interest in disclosing their privacy practices to keep customers happy.

Another point of difference is that the Georgetown study used one comprehensive sample of commercial U.S. Web sites irrespective of business category or company size, as opposed to six distinct samples in the FTC survey, which were chosen with the above-mentioned considerations of size and category.

Finally, the Georgetown study used a larger set of questions to identify the coverage of FIP principles by commercial Web sites; the principles were also operationalized via more inclusive definitions. Thus, "notice" was defined to include statements about what information is collected, how it is collected, how it will be used, whether the information will be reused or disclosed to third parties, and whether the site said anything about its use or non-use of cookies. "Choice" was defined to include statements regarding choice offered about being contacted again by the same organization and choice about having non-aggregate personal information collected by the Web site disclosed to third parties. "Access" was defined to include allowing consumers to review or ask questions about the information the site had collected and whether the site disclosed how inaccuracies in personal information the site had collected

were handled. "Security" was defined to include protecting information both during transmission and during subsequent storage (Culnan, 1999, p. 9). Moreover, the content analysis questionnaire included two questions to identify the coverage of the fifth FIP principle – enforcement and redress. The sites providing contact information that a consumer might use to ask questions about his/her privacy or complain in case of privacy violation were considered as covering the principle of enforcement and redress (Culnan, 1999, p. 9).

As noted above, the study revealed that 66% (236 sites) of the commercial sites in the sample gathered some personal information and posted a privacy disclosure. Of the 236 Web sites, 89.8% included at least one survey element for notice, 61.9% contained at least one survey element for choice, 40.3% contained at least one survey element for access, and 45.8% contained at least one survey element for security, and 48.7% contained at least one element for contact information. Nearly 13.5% of the same 236 Web sites (or 9.5% of the 337 Web sites that collect at least one type of personal information) contained at least one survey item for notice, choice, access, security and contact information, that is, partly complied with all the five FIP principles (Culnan, 1999, p. 9-10).

The 2000 FTC survey indicated "continued improvement" in the number of Web sites posting privacy policies: 64% in the comprehensive random sample and 97% in the group of most popular sites (FTC, 2000). The number of sites posting at least one privacy disclosure (either an informational privacy statement or/and a privacy policy) was higher: 90% and 100% for the comprehensive and the most popular samples, respectively. The

detailed analysis of privacy policies against the criteria of compliance with FIP principles, however, revealed that only 20% of sites in the comprehensive sample (42% in the "most popular" sample) covered the four core FIP principles in their online privacy disclosures.

This time the Commission went beyond the mere counting of disclosures and a surface analysis of their content; it conducted a more thorough analysis of the nature and substance of privacy disclosures in light of the fair information practice principles. The methodology had been updated to match that of the Georgetown study, especially in sampling and questionnaire designing.

The operational definitions for the core variables of notice, choice, access and security had been considerably extended. Thus, "notice" was expanded to include statements about third-party disclosure, and "choice" covered statements about both internal (i.e., by the site) and external (i.e., by third parties) use of personal information beyond the purpose for which it was provided.

The reported results, however, did not reflect solely the cases of overall compliance with the definitions for fair information practice principles provided in the study; rather, the results reflected "the number of Web sites implementing the practice at least in part, but not necessarily in a complete manner" (FTC, 2000, p.30). Consequently, the site received credit for "notice" if it posted a privacy policy and identified at least one specific type of information it collected, at least one use to which such information might be put, and whether any of the information would or would not be shared with third parties. With respect to "choice," coverage was considered complete if the site offered

choice for at least one type of communication to a user and choice for the sharing of at least one type of information with third parties. With respect to "access," a site received credit if it offered the ability to review, correct or delete at least one item of personal information it had collected. And "security" was covered if the site contained at least one statement regarding security, irrespective of the actual security precautions taken by the site (FTC, 2000, p.30).

With these limitations in view, the study found that, out of the sites collecting personal information (97% in the comprehensive sample), 55% comply, at least partly, with the category of notice, 50% comply partly with the category of choice, 43% with the category of access, and 55% - with the category of security. Furthermore, 41% of sites received credit for covering both notice and choice, and 20% - for covering all four FIP principles, at least to some extent (FTC, 2000, Appendix C, p. 4).

The latest comprehensive survey of online privacy policies was conducted by a group of researchers from Ernst & Young in December 2001. In order to gain statistics comparable to the previous FTC surveys, the study, commissioned by the Progress and Freedom Foundation, precisely followed the methodology of the 2000 FTC survey. The results showed a consistent increase in Web sites' compliance with all FTC recommendations for privacy disclosure (Adkinson, Eisenach, & Lenard, 2002).

The above-mentioned studies focused solely on commercial Web sites. This can be partly explained by the limitation of FTC authority "to prohibit unfair practices... in or affecting commerce" (Federal Trade Commission Act, 1993, para. 45) and consequently inability to "cover consumer privacy breaches that occur on noncommercial Web sites,

such as non-profit or educational sites" (FTC, 2000a). On the other hand, the commercial Web is most often perceived as an immediate threat to consumer privacy and therefore is particularly interesting for privacy watchdogs.

Several studies attempted to capture the essence of privacy practices of more specific professional Web site categories including medical (Goldman, Hudson, & Smith, 2000) and financial (CDT, 2001). The results shared a common concern for the lack of notice about privacy practices on the examined Web sites and the little choice consumers had in the matter of personal information disclosure. The 2001 study by Center for Media Education examined the compliance with COPPA requirements of Web sites directed at a child audience. The analysis revealed a three-fold increase (from 24% in 1998 to 76% in 2001) in the number of Web sites posting a privacy policy to explain data collection practices (Center for Media & Education [CME], 2001). However, only slightly more than 12% of examined Web sites met the crucial requirement of parental notice.

Several studies were undertaken to examine privacy practices of governmental Web sites. In a report released September 15, 2000, Brown's Taubman Center for Public Policy and American Institutions examined 1,813 Web sites including 1,716 state government sites, 36 federal legislative or executive sites, and 61 federal court sites. One of the key findings of the report states that "only 5 percent of government websites [sic] show some form of security policy and 7 percent have a privacy policy" (West, 2000).

The National Electronic Commerce Coordinating Council (NECCC) undertook two successive studies with the focus on the main Web pages or portals of the 50 states and U.S. territories, and the 25 largest U.S. cities and counties based on population. The

first review, made in March of 2000, demonstrated that only 10 states (or 20%) had privacy policies accessible from their home page. In the second follow-up survey, completed on December of 2000, the corresponding number rose to 24 (National Electronic Commerce Coordinating Council [NECCC], 2000).

In September 2000, the General Accounting Office (GAO), an investigative arm of U.S. Congress, published a report titled "Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles" (GAO, 2000). The researchers examined 65 Web sites of various federal agencies collecting users' personal data online. The analysis showed that 85% of the sites posted a privacy notice. The majority of federal sites (69%) met FTC's criteria for notice. However, a smaller number of sites implemented the three remaining principles of choice (45%), access (17%), and security (23%).

With respect to analysis of fair information practices of Web sites, it is also important to consider the experience of privacy seal programs, such as TRUSTe and BBBOnline. TRUSTe bases its evaluation mechanism on the four core elements of the Fair Information Practices – notice, choice, access, and security – and expands the reach of the assessment through such additional categories as *registration process*, *special features* (related to the handling of personal information provided for such services as email, chat, discussion groups and newsletters), *co-branding* (related to the disclosure of the privacy practices of a site's partners who may have access to users' personal data), and *links to other sites* (related to the privacy practices of the Web sites that can be reached from the current site). Besides, TRUSTe uses some categories present in other

evaluation instruments such as *cookies*, *contact information*, and *parental review of information* (http://www.truste.org).

BBBOnline's requirements are identical to those of FTC in that they demand that Web site owners cover major principles of Fair Information Practices. Unlike FTC, however, BBBOnline makes a special emphasis on the fifth element of FIP, that is, disclosure of enforcement and redress mechanisms available in case of a suspected privacy breach (BBBOnline, n.d.).

Thus, the above-mentioned studies reveal steady and slow advancement of the commercial Web towards implementing core FIP principles. The surveys also demonstrated the most vulnerable points in online privacy practices, which sometimes required a legislative rather than voluntary compliance.

With respect to governmental Web sites, the studies seem to go against the assumption that the government must, or at least is supposed to, advocate the use of privacy disclosures on all of its online outlets. The survey results indicate that most governmental sites still provide insufficient coverage of basic FIP principles.

It is also important to mention that some surveys have demonstrated the importance of elements in a privacy disclosure that are not the part of core FIP principles, such as contact information, use of cookies, and opt-in /opt-out procedures of obtaining users' consent for personal information disclosure. This carries an important methodological implication for both the current and future studies as it drives researchers to a more advanced and thorough examination and subsequent evaluation of Web site privacy policies.

From a methodological perspective, the majority of the previous research on privacy policy evaluation has been conducted in the form of an online survey of compliance with certain requirements, be it FTC-recommended FIP principles (FTC, 2000; see also Adkinson et al., 2002) or Congress-enacted COPPA regulations (CME, 2001). However, sampling procedures and survey questions often varied from one study to another, which has rendered impossible a straightforward comparison of the collected data across the surveys. In spite of these difficulties one longitudinal study compared the results of four major surveys restricting the analysis to "comparable samples" and examining the "variables that measure the same phenomena across surveys" (Adkinson et al., 2002). The overall results of the comparative analysis reflected a statistically significant increase in the number of sites posting privacy notices. As to individual elements of Fair Information Practices, the study revealed continuous progress in compliance with the categories of notice and security and a significant decrease in coverage of the category of access.

Most studies use random sampling from a relatively large base population of Web sites to achieve a high degree of representativeness of the sample and allow for generalizations beyond the given sampling frame (Culnan, 1999; FTC 2000). Furthermore, all evaluations are fundamentally based upon the test of compliance with the core principles of the Code of Fair Information Practices – notice, choice, security, and access. Some assessment mechanisms also incorporate a separate bloc to evaluate the fifth FIP principle of redress and enforcement (BBBOnline), sometimes through the category of contact information (TRUSTe). Several evaluation schemes test compliance

with regulations applicable to a limited group of sites, such as in the case of checking children's Web sites for COPPA compliance (CME, 2001; FTC 1998). However, the category of parental control, or parental review of information, may be an element of a more comprehensive assessment (FTC, 1998; TRUSTe, n.d.) if the sites in the sample are targeted to a large audience of mixed age composition. Finally, items of an actual content analysis sheet often represent multiple narrow-focused questions checking the degree of compliance with each of the analyzed principles of privacy practices disclosure (FTC, 2000).

Methods

Sample Selection

The study was based on three target populations: a random sample of commercial Web sites, a random sample of educational sites, and a random sample of governmental sites. The three samples were drawn from three lists of Web sites retrieved by the Google™ search engine in response to a single search query (the word "help") but each time with advanced search options modified so that to retrieve only commercial, only educational, or only governmental sites. The resulting three lists of Web sites served as sampling frames, from which three sampling pools were created using a systematic sampling procedure described below. Finally, three samples – one for each of the three Web site categories – were drawn from the respective sampling pools using a procedure described below.

The Google Search Engine

Google is one of the most comprehensive search engines on the Internet; it has indexed approximately three billion Web pages by August 2003 ("Extreme Searcher's Web Page – News & Updates, The," n.d.). The heart of Google's proprietary search software is PageRank™, a system for ranking Web pages that uses the vast link structure of the World Wide Web as an indicator of the value of an individual page. In essence, Google interprets a link from page A to page B as a vote cast by page A in favor of page B. PageRank, however, does not merely count the number of "votes," or links, a page receives on the Web; it also analyzes the page that casts the vote. Votes cast by pages that themselves receive many links count more heavily than votes from Web sites with few links (Google, n.d.).

The importance of a given Web page in terms of the number of links it receives from other Web sites is not the only factor in the search engine's decision to retrieve it as a matching result. Google combines PageRank with the data from a "hit list," a list of occurrences of a particular word on a particular Web page including position, font size, and capitalization. To be more specific, for every Web page that contains a given search query, Google identifies: (a) whether a hit (the occurrence of a search query in a document) occurs in a "fancy" area (URL, page title, or metatag) or "plain" area (everything except the fancy area); (b) the font size of the word; (c) whether the word is capitalized; and (d) the position of the word in the document (Brin & Page, n.d.).

It is expedient to consider an example in order to better illustrate Google's capabilities. Suppose we are running a search for the query "research." First off, the

search engine will retrieve all the pages in its index that contain the word "research." Further, it identifies all the pages where the match is in the "fancy" area," that is, URL, page title, and metatag. These pages are in the top retrieved results and placed one after another in a hierarchy based on their PageRank: documents with a higher PageRank are placed first, followed by pages with lower PageRank (Fig. 5).

Figure 5. **A Google page with the first 10 matches for the "research" search query.**

Further, Google analyzes the pages that contain the word "research" in the "plain" area, that is, any part of a document except URL, page title, and metatag. These pages are placed after the results from "fancy" matches. The hierarchy is defined by the PageRank, the font size (the larger the font, the more weight is attached to that particular occurrence of the word), the capitalization (capitalized words have more weight than non-capitalized

ones), and the position in the document (the earlier the word is located in the document, the more important the occurrence is).

Unlike other search engines, Google does not sell placement within retrieved results themselves, which increases the objectivity of the matching procedure since no page can buy a "higher" rank in the database. Google has a number of advanced features including retrieval of pages based on the language of a Web site and domain name extension – two options extremely useful for the current research (Google, n.d.).

Despite its immense index covering almost three billion Web pages, Google returns only up to 1,000 top results for any search query. According to a Google team representative, this approach is quite common in the entire Internet search engine industry, with figures ranging from 500 to 3,000 results per query. Such a policy allows keeping the business low-cost and enables free public access. Moreover, search results for any query "tend to tail off long before" result number 1,000, while users rarely go past number 100 (email communication with a Google team member, October 4, 2003).

In view of the above-mentioned limitation, the samples selected for the present study are representative only of the population of Web sites retrieved by Google for a given search query. Consequently, the results of this study cannot be generalized to the entire universe of commercial, educational, and governmental Web sites.

The Creation of Sampling Frames

Three sampling frames were created, one for each of the three analyzed Web site categories: commercial, educational, and governmental. Each frame was determined by entering the keyword "help" in the Google search engine at http://www.google.com,

checking "only" in the drop-down menu in the "Domain" section on the Advanced Search page, accessible from the site's home page, entering the corresponding domain name extension (".com," ".edu" or ".gov") in the appropriate window to the right of the "Domain" section, and checking "English" in the drop-down menu in the "Language" section (Fig. 6).

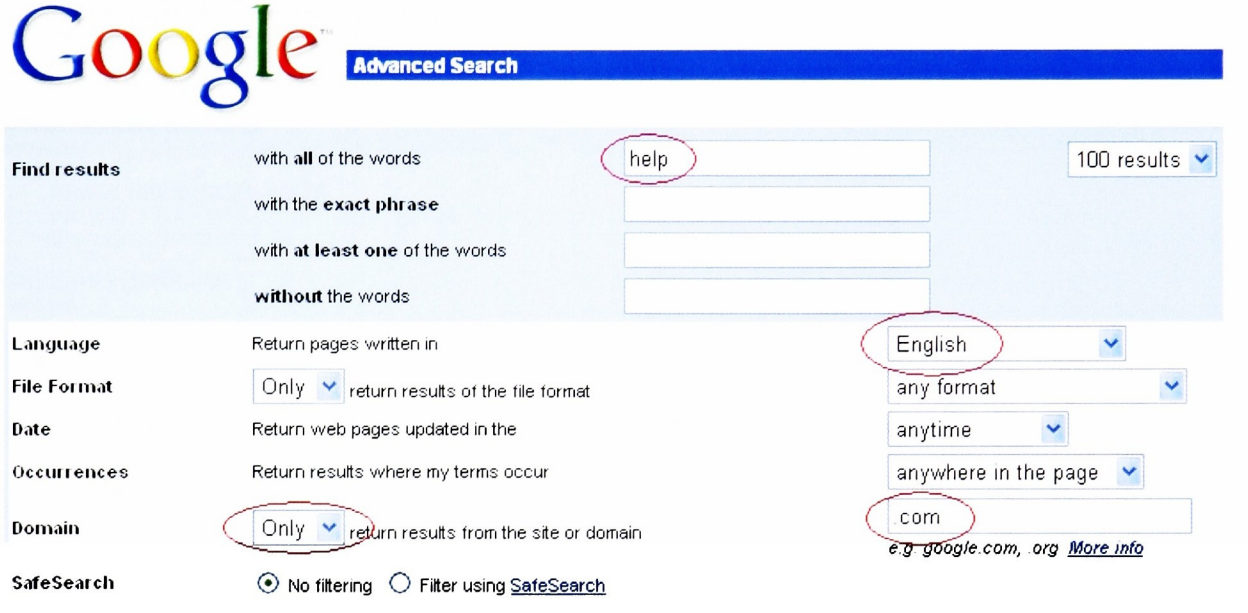

Figure 6. **Setting search parameters for sampling.**

The totality of Web pages (approximately 1,000) returned in response for the keyword "help" (with the exception of sponsored links that appear on the right side of the page and indented results that reflect similar matches from the same Web site – see Fig. 7) for each of the three domains was considered to be a sampling frame for the corresponding Web site category.

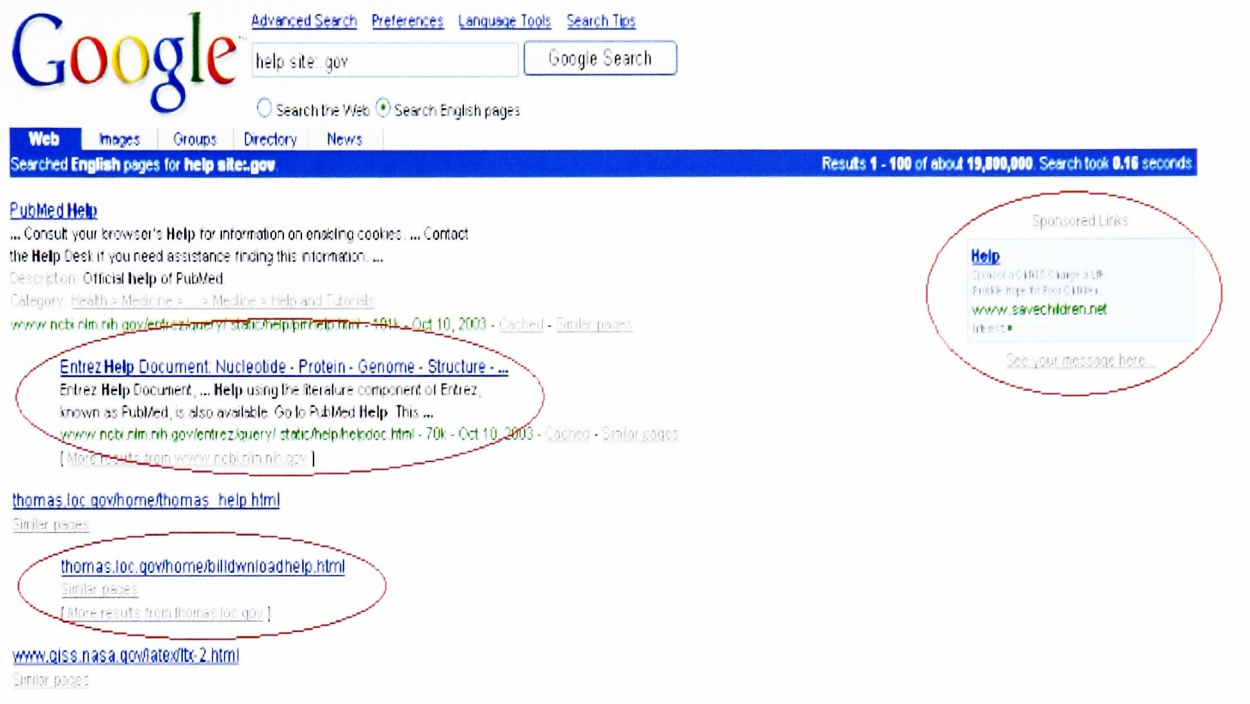

Figure 7. **Indented results and sponsored links are not included in the sampling frames.**

The Creation of Sampling Pools

The following sampling procedure was used to create three pools of sites from the corresponding sampling frames drawn from Google's index of Web sites. First, a target sample size of 100 sites was established for each of the three final samples. It was estimated[4] that up to 200 sites in the ".com" and ".gov" domains and up to 300 Web sites in the ".edu" domain might need to be examined to ensure a final sample size of 100 eligible sites. After the target size for sampling pools had been determined, a sampling interval was determined by dividing the total number of sites in each sampling frame by 200 (the desired size of a sampling pool for commercial and governmental Web sites) or

[4] The estimates are based partly on the results of the previous studies, including FTC 2000 and GAO 2000, and partly on the preliminary investigations of the author.

300 (the desired size of a sampling pool for educational Web sites). The sampling interval of 4 was then used to randomly select sites from a sampling frame for inclusion in the corresponding sampling pool by the following methodology. A random one-digit number (six) was generated by drawing 1 item from a bowl with 9 items numbered from one through nine, and the site appearing in the random number's slot on the sampling frame list was selected for inclusion, as was each site appearing on the list at the interval of one sampling interval. The sampling procedure continued until the desired size for each sampling pool was achieved or until the end of the sampling frame, whichever came first. The same procedure was repeated for each of the three domains.

Since Google retrieves multiple matches for the same domain name, an additional procedure was followed in the process of creation of sampling pools. Only one match belonging to a certain domain name was included in a sampling pool. All other matches belonging to the same domain were not included in a sampling pool once this domain name had been sampled.

In the present study, a "domain" stands for the totality of all Web pages, sites, and servers using a particular domain name, defined as the word or letters immediately preceding the domain name extension (".com", ".edu" or ".gov") (FTC, 2000, Methodology section, p.1). For example, the site "my.rit.edu," the page "rit.edu /academics.html," and the server "www2.rit.edu" would all be included in the domain "rit.edu." In this study, we define a Web site as a domain, which serves as the unit of analysis for the survey. The exception from this rule is made for ".gov" Web sites if a governmental Web site has a two-letter extension preceding the major domain name

extension and representing the state that put up the site, for instance, www.courtinfo.ca.gov. In this case, the entire third-level domain (www.courtinfo.ca.gov), and not the second level domain (www.ca.gov), is included in a sampling pool.

If the sampling interval ended on a domain that was ineligible for inclusion in a sampling pool, that domain was substituted for by a domain at the interval of three from the ineligible site. If the substitute was also ineligible, the same procedure was repeated until an eligible site was found. The sampling procedure for the rest of the sampling pool continued from the ineligible site for which a substitute was selected.

Final Samples: Site Eligibility Survey

Three surfers were assigned URLs from the three sampling pools based on the following procedure. The URLs included in each sampling pool were numbered in the order of their inclusion in the corresponding sampling pool. Then all the sites appearing in the ".com" sampling pool were assigned to one surfer, the sites in the ".edu" sampling pool were assigned to another surfer, and the sites in the ".gov" sampling pool, to the third surfer.

The surfers were further instructed to visit the Web sites they had been assigned in the order of appearance on the sampling pool list and to spend no more than 20 minutes per site. The surfers received a half-day training in using the Web Site Eligibility Check Form and were supplied with detailed written instructions (see Appendix C, part II). The surfers were then required to fill in a Web Site Eligibility Check Form for each site they visited in the assigned sampling pool in order to determine if the site qualified

for inclusion in the content analysis phase. The surfers had to discover if the site was not inaccessible (question #1 on the Check Form), belonged to a unique Web site (question #2), was in the English language (question #3) or had an English version (question #4), gathered at least some personal information (question #8), and posted a unique privacy policy (question #10 and #11). Commercial sites (those with a ".com" extension) had to go through additional qualification, and namely, the site had to belong to an American business (questions #5 and #6). Educational sites (those with an ".edu" extension) also underwent an additional eligibility check to ascertain that they belonged to institutes of higher education (question #7).

Additionally, each surfer noted if the site had attempted to install a cookie on his/her computer's hard drive. For this purpose, the privacy preferences on all computers were modified to prompt a user every time a Web site attempted to upload a cookie.

The surfers were required to print out the privacy policy of each eligible Web site. The Web site eligibility check process within each sampling pool continued until the first 100 eligible Web sites were identified. These 100 eligible sites constituted the final sample for the corresponding domain.

Data Collection

The process of collecting data represented a content analysis of the privacy policy notices of the Web sites in the three final samples. Three content coders were assigned Web sites from three final samples based on the following procedure. The URLs included in each sample were numbered from one to 100 in the order of their inclusion in the corresponding samples. Then one coder received sites from one through 35 from the

".com" sample, sites from one through 35 from the ".edu" sample, and sites from one through 30 from the ".gov" sample. Another coder received sites one through 35 from the ".com" sample, sites from one through 30 from the ".edu" sample, and sites from one through 35 from the ".gov" sample. The third coder received sites one through 30 from the ".com" sample, sites from one through 35 from the ".edu" sample, and sites from one through 35 from the ".gov" sample. The content coders underwent two-day (4 hours + 4 hours) training in the use of the content analysis form and were supplied with detailed written instructions (see Appendix C, part III).

The content coders then analyzed the privacy policies of all the sites that had been included in the three final samples. Each privacy policy was carefully read with the goal of determining its compliance with a number of principles of personal data privacy including the four core principles the Code of Fair Information Practice – notice, choice, access, security – and three additional principles of disclosure to third parties, cookies, and contact information.

The content analysis form incorporated 15 items starting with #13 and ending with #27. Items #13, 14 and 15 were designed to identify the compliance with the principle of Notice. These questions helped determine if the site notified its users about the site's data collection practices in general (#13), about the type(s) of data gathered (#14), and about the way(s) the data might be used (#15). Item #16 on the content analysis form identified the compliance with the principle of Choice, that is, whether a user's consent was solicited before using his/her personal information. Items 17 through 19 were designed to measure the compliance with the principle of Access as they

identified if a user was enabled to review (#17), edit (#18) and delete (#19) at least some of the personal information collected by the site. The set of items from #20 through #23 served to identify the compliance with the principle of Security, and namely, whether a Web site provided any security for users' personal information (#20), whether it protected data during its transfer from user to site (#21) and during subsequent storage (#22), and whether a site informed users of the tools used to protect personal data (#23). Item #24 was designed to identify if a site informed users of its practices of information disclosure to third parties. Item #25 asked about the use of cookies by a Web site, and item #26 inquired if the site explained what a cookie was. Finally, item #27 identified if a site published contact information, which customers could use to ask questions about the site's privacy practices.

Every item on the content analysis form was designed in one of the following two ways. It was either a question requiring "yes" or "no" answer or a question with multiple-choice answers. Each item required a thorough analysis of the content of a privacy policy to determine if the text contained specific information, most often in the form of a complete sentence, sought out in the question. For instance, item #14 asked if the privacy policy contained at least one complete sentence informing the user of the types of personal information the site collected. This means that a content analyst might give the positive answer to the question only if s/he found at least one sentence containing information on at least one type of personal data collected by the site. If there was no sentence containing such information, the answer to the question would be "no."

Data Analysis

Once all of the sites were content analyzed, data were entered by two data-entry people. One data-entry team member read off answers to the second member of the pair who inputted the data. These numbers were then manually checked for accuracy by both team members separately. A set of queries were then run on the data to ensure that the data were internally consistent (i.e., all conditional answers were answered or left blank, as appropriate). All errors were corrected prior to the actual data analysis.

Finally, the data were analyzed using Minitab® for Windows®. The analysis focused on the performance of Web sites and sought to estimate the proportion of sites whose privacy policies fell into various categories. In particular, the analysis revealed the percentage of sites in each of the three studied samples that fully or partially complied with each of the seven principles of fair information practice, as defined for the present study. The data analysis also demonstrated the percentage of sites in each sample covering various combinations of fair information practice principles (e.g., notice and choice only; notice, choice, access and contact information only; etc.) as well as the percentage of sites covering only a certain portion of a given principle (e.g., for the principle of access the analysis uncovers the percentage of sites allowing only to review personal information; review and edit personal information; and review, edit and delete personal information).

The data analysis results were provided in individual and summary tables for all three samples to allow comparisons (see Appendix D).

Inter- and Intracoder Reliability

In order to measure the amount of agreement among the content coders, intercoder reliability tests were run on a set of research results. Fifteen units of analysis (i.e., analyzed privacy policies) were selected, five out of each of the three final samples, using the following random sampling technique. The number of units in each sample (100) was divided by 5 (the desired number of units required for reliability tests), which produced the figure of 20. Then, every 20^{th} unit in a sample, counting from the 1^{st} unit, was selected to be included in the reliability test sample. The same procedure was repeated with each of the final samples. The resulting sample of 15 units was used to measure both the intercoder and intracoder reliability.

Each coder was asked to code the privacy policies in the reliability sample twice, with a time lag of one week between the two coding sessions. The coding results recorded by all three coders from the first coding session were used to assess intercoder reliability. The reliability was calculated applying Cohen's *kappa* coefficient for each pair of coders and for all three coders together. The average intercoder reliability among the three coders reached approximately 0.83. The reliability between coders in pairs was as follows: 0.837 for Coders 1 and 2, 0.824 for Coders 1 and 3, and 0.847 for Coders 2 and 3.

The coding results recorded by each coder from both the first and the second coding sessions were used to assess intracoder reliability. The reliability was calculated applying Cohen's *kappa* coefficient for each set of results (test and post-test) for every

coder. The intracoder reliability coefficients were as follows: 0.82 for Coder 1, 0.97 for Coder 2, and 0.92 for Coder 3.

Research results

Web Site Eligibility Check

In order to obtain the desired number (100) of Web sites for each of the final samples, the Web surfers performed eligibility checks on 163 ".com" Web sites, 298 ".edu" Web sites, and 130 ".gov" Web sites.

In the sampling pool for commercial Web sites, 63 out of the 163 analyzed sites were considered ineligible for various reasons: 21 because they did not belong to a business enterprise, 9 sites did not belong to a U.S. business, 15 sites did not post a privacy policy, 12 sites were ineligible because their privacy policy was identical with that of their parent company, which had already been considered prior in the survey, and 6 sites were ineligible for other reasons (Fig. 8).

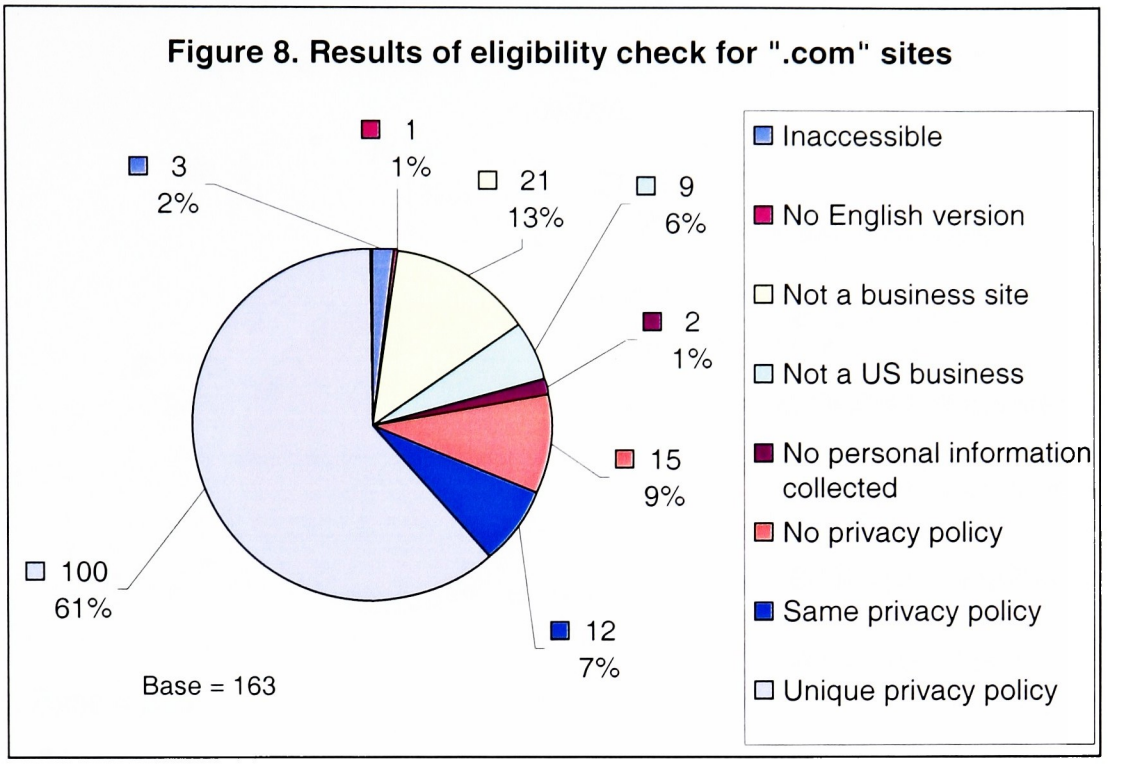

Figure 8. **Results of the Web site eligibility check for the ".com" sampling pool (base=163). (Source: Appendix D, Table 1)**

In the sampling pool for educational Web sites, 198 out of the 298 analyzed Web sites were considered ineligible for the following reasons: 14 sites were ineligible because they did not belong to an institute of higher education, 174 sites did not post a privacy policy, and 10 sites for other reasons (Fig. 9).

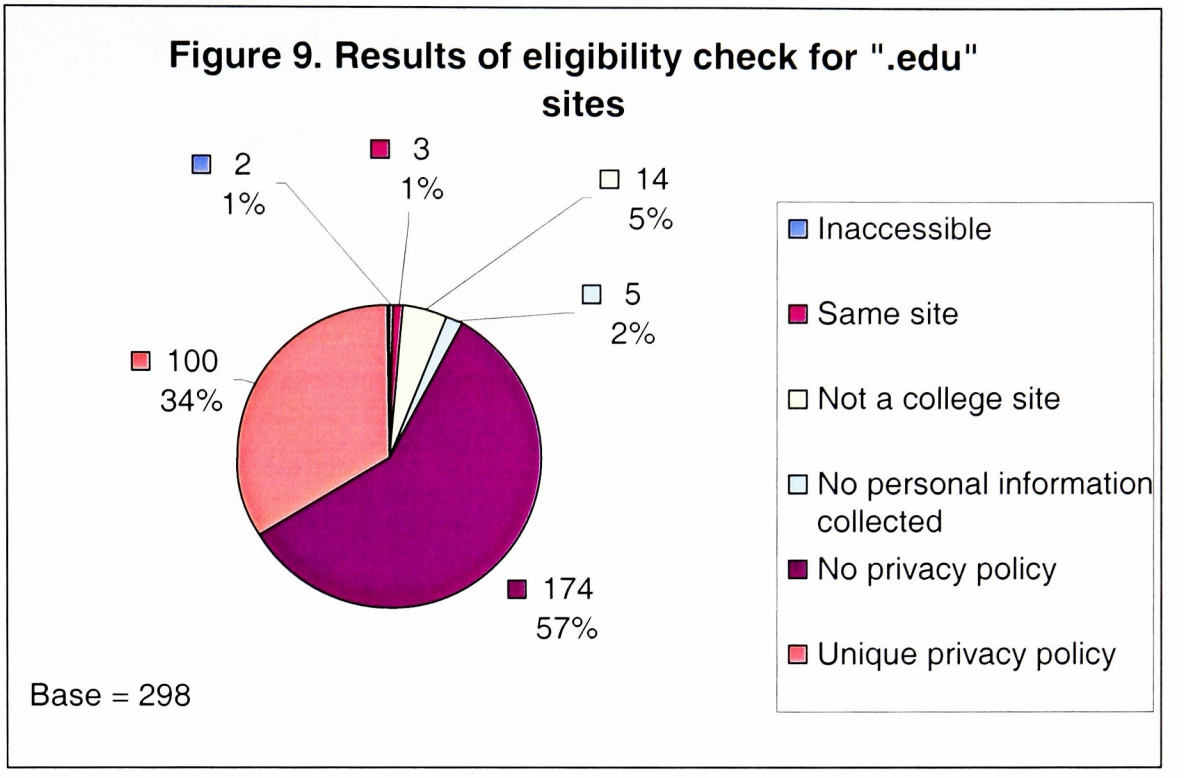

Figure 9. **Results of the Web site eligibility check for the ".edu" sampling pool (base=298). (Source: Appendix D, Table 1)**

In the sampling pool for governmental Web sites, 30 out of the 130 analyzed Web sites were found ineligible for the following reasons: 4 sites were inaccessible, 5 sites did not post a privacy policy, and 21 sites were ineligible because their privacy policy was identical with that of their parent institution, which had already been considered prior in the survey (Fig. 10).

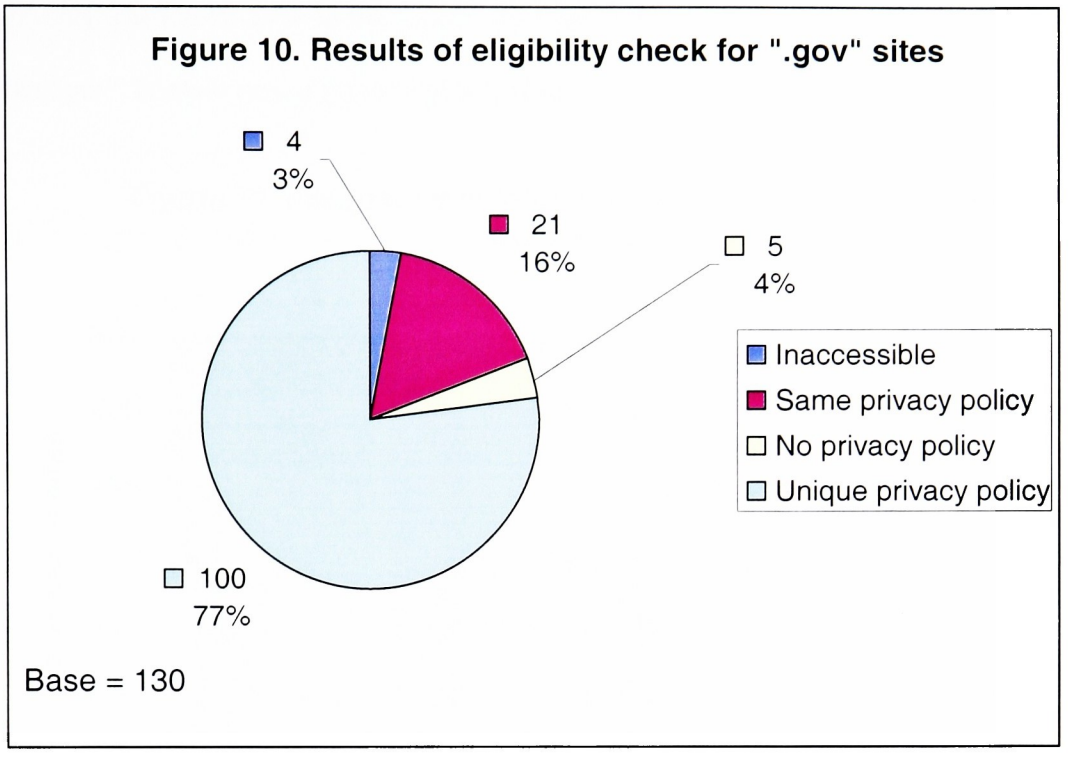

Figure 10. **Results of the Web site eligibility check for the ".gov" sampling pool (base=130) (Source: Appendix D, Table 1)**

The eligibility check revealed that the overwhelming majority of the analyzed sites collected at least one type of personal information, most often an email address. Thus, 98% (127 sites) of the analyzed ".com" Web sites belonging to U.S. business enterprises (129 sites), 98% (274 sites) of the analyzed ".edu" sites belonging to U.S. institutions of higher education (279 sites), and 100% of ".gov" sites belonging to U.S. governmental agencies (126 sites) collected at least one type of personal information from Web users. However, the percentage of the pre-qualifying sites[5] posting privacy

[5] Pre-qualifying sites in the ".com" sample are the unique Web sites that belong to U.S. businesses. Pre-qualifying sites in the ".edu" sample are the unique Web sites belonging to U.S. institutions of higher education. Pre-qualifying in the ".gov" sample are the unique Web sites belonging to U.S. governmental agencies

policies was lower: 87% in the ".com" domain, 36% in the ".edu" domain, and 96% in the ".gov" domain post a privacy policy (Fig. 11).

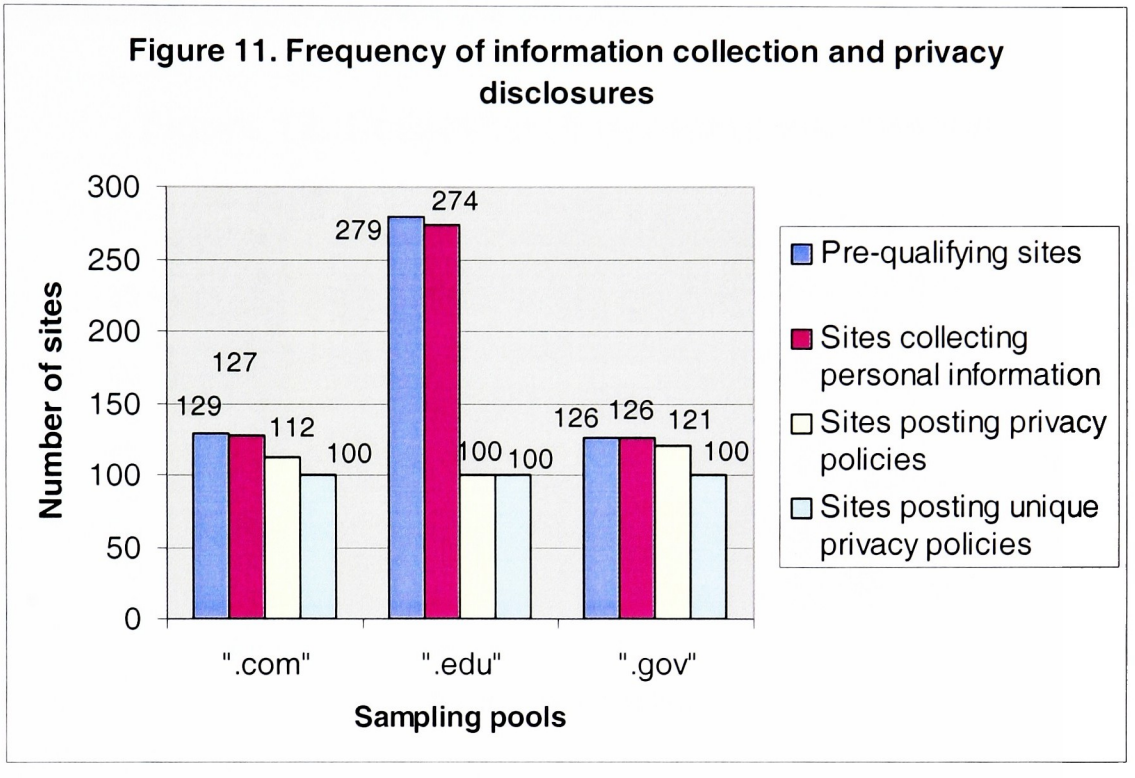

Figure 11. **Of the pre-qualifying sites in each sampling pool, the number of sites collecting personal information and the number of sites posting privacy policies.**

(Source: Appendix D, Table 2)

With respect to the collection of personally identifiable information, the figures were as follows. A user's email address was collected by 98% of U.S. commercial Web sites, 98% of educational Web sites belonging to the institutes of higher education, and 100% of governmental sites. A user's name was collected by 85% of U.S. commercial Web sites, 49% of educational Web sites belonging to the institutes of higher education, and 45% of governmental sites. Further, 64% of U.S. commercial Web sites, 29 % of educational Web sites belonging to the institutes of higher education, and 37% of

governmental sites collected users' postal addresses. Finally, users' phone numbers were gathered by 53% of U.S. commercial Web sites, 24% of educational Web sites belonging to the institutes of higher education, and 24% of governmental sites (Fig. 13).

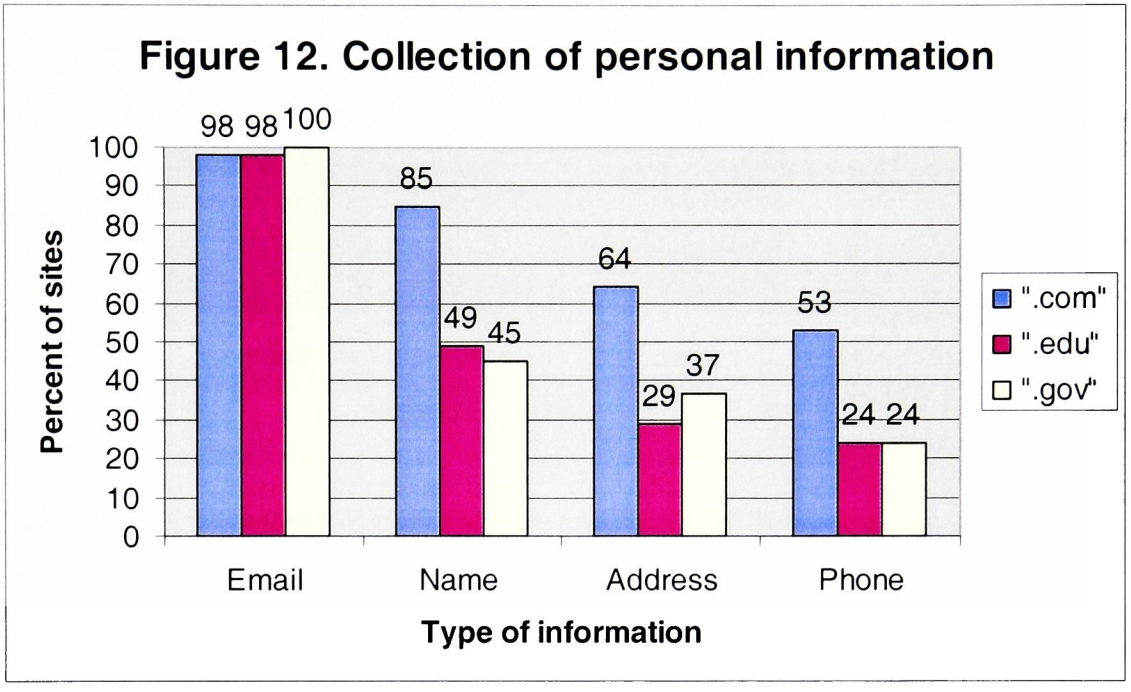

Figure 12. **Of the pre-qualifying sites in each sampling pool, the percentage of sites collecting email address, name, postal address, or phone number.**

(Source: Appendix D, Table 3)

The eligibility check also produced results for the sites that attempted to set cookies on the user's computer: 84% of U.S. commercial Web sites, 53% of educational sites belonging to the institutes of higher education, and 60% of U.S. governmental Web sites (Fig. 13).

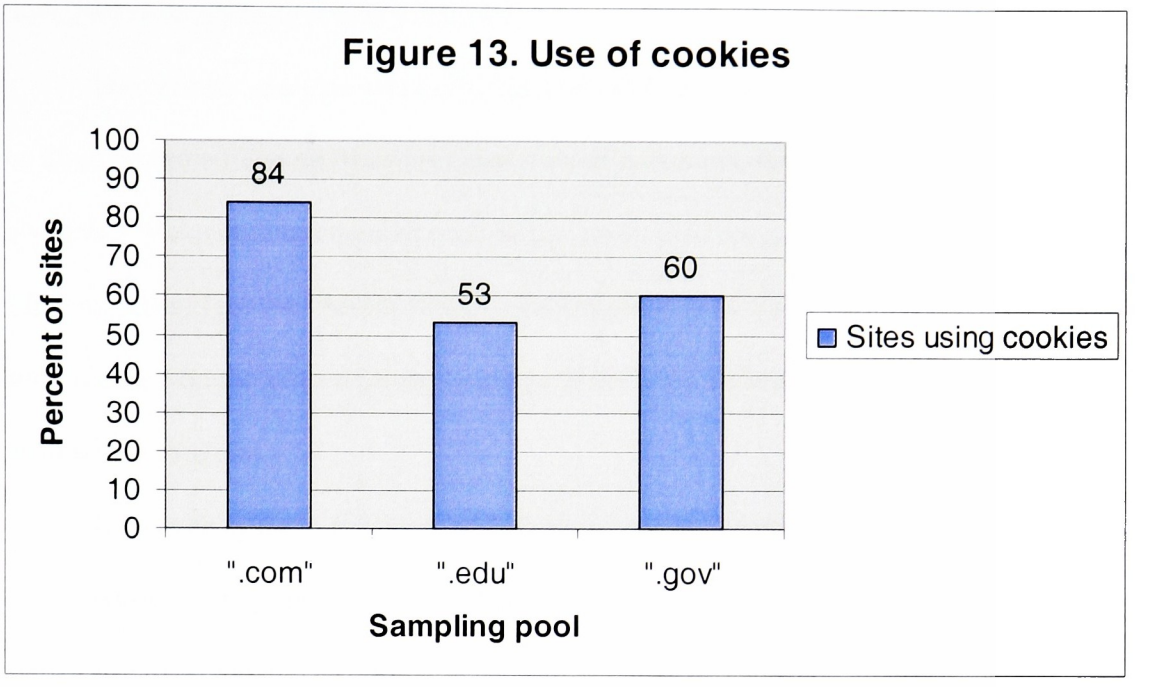

Figure 13. **Of the pre-qualifying sites in each sampling pool, the percentage of sites using cookies.**

(Source: Appendix D, Table 3)

However, there is a certain limit to the value of these latter findings. Every Web site may potentially count from several dozens to several thousands of pages, some of which may attempt to send a cookie when accessed by a Web user. The surfers, on the other hand, were instructed to browse every site for a limited amount of time and were not expected to cover every single Web page within a site. Consequently, the produced figures demonstrate the number of Web sites where surfers came across a page (pages) that tried to send a cookie to the user's hard drive but do not necessarily reflect the actual number of sites that use cookies, which may be substantially higher.

The Content Analysis of Privacy Policies

The content analysis was performed on the final samples of Web sites in each of the three domains. The analysis included a set of questions designed to find out the extent to which a Web site implemented each of the seven principles of fair information practice (FIP), as defined for the present study. Analyzing the compliance with FIP principles the study focused on the posted privacy polices of the Web sites that collected at least some personal information.

Coverage of Each Principle of Fair Information Practice

Notice. The principle of Notice is undoubtedly the most basic of FIP principles since it is a pre-requisite to the implementation of other principles. The content analysis form asked three questions to ascertain the site's coverage of the Notice principle in its privacy policy: **(1)** *Does the Privacy Policy contain at least one complete sentence indicating that the site does not collect any electronically collected personal information from its users?* **(2)** *Does the Privacy Policy contain at least one complete sentence informing the user of the type(s) of electronically collected personal information the site gathers?* and **(3)** *Does the Privacy Policy contain at least one complete sentence informing the user of the ways the website does or may use the collected personal information?*

The answers to the first question indicated that all the privacy policies in each sample informed users of the fact of gathering at least some kind of electronically collected personal information. Further, 93% of commercial Web sites, 84% of educational Web sites, and 97% of governmental Web sites informed users of the type(s)

of electronically collected personal information the site gathers. Finally, 98% of commercial Web sites, 88% of educational Web sites, and 99% of governmental Web sites informed users of the way(s) the Web site uses the collected personal information (Fig. 14).

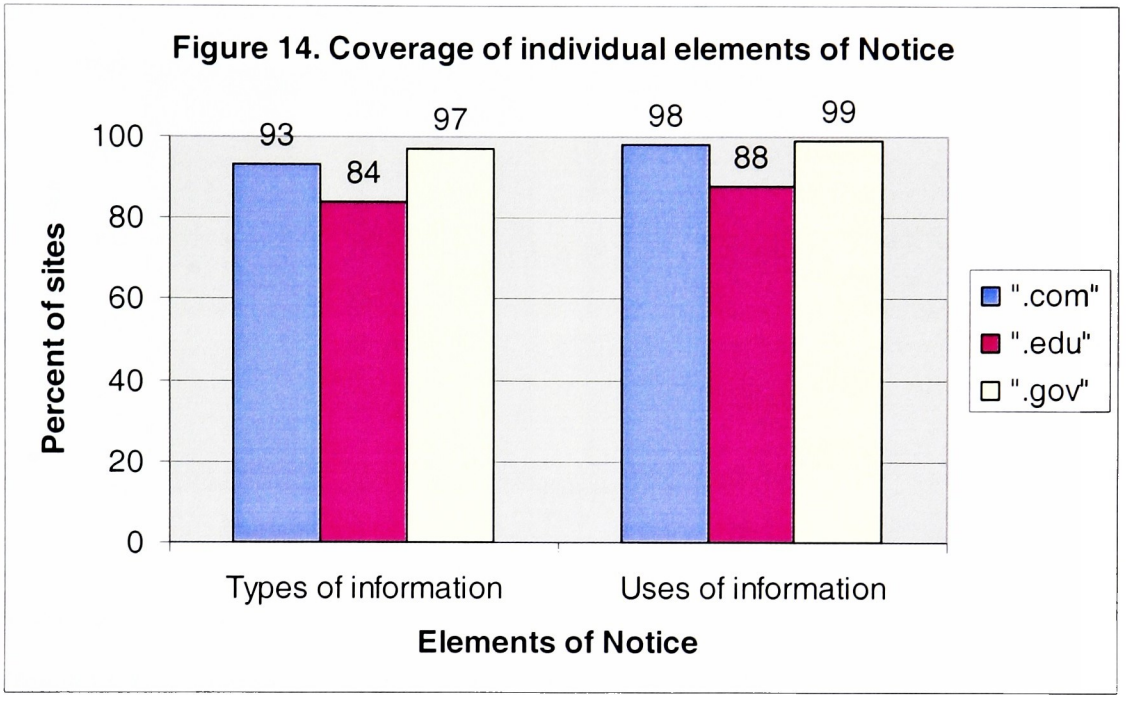

Figure 14. **The number/percentage[6] of sites in the final samples providing individual elements of the principle of Notice in their privacy policies.**

(Source: Appendix D, Table 4)

As a result, 99% of commercial Web sites, 90% of educational Web sites, and 99% of governmental Web sites at least partly covered the principle of Notice in their privacy policies (i.e., they informed the users of either the types of collected personal information or the ways the collected information was used). Finally, 92% of commercial

[6] From hereon, all the numbers in the tables, unless otherwise noted, represent both an actual number of sites and a percentage since the final samples consist of 100 Web sites

Web sites, 82% of educational Web sites, and 97% of governmental Web sites fully covered the principle of Notice (i.e., they informed the users of both the types of collected personal information and the ways this information was used) (Fig. 15).

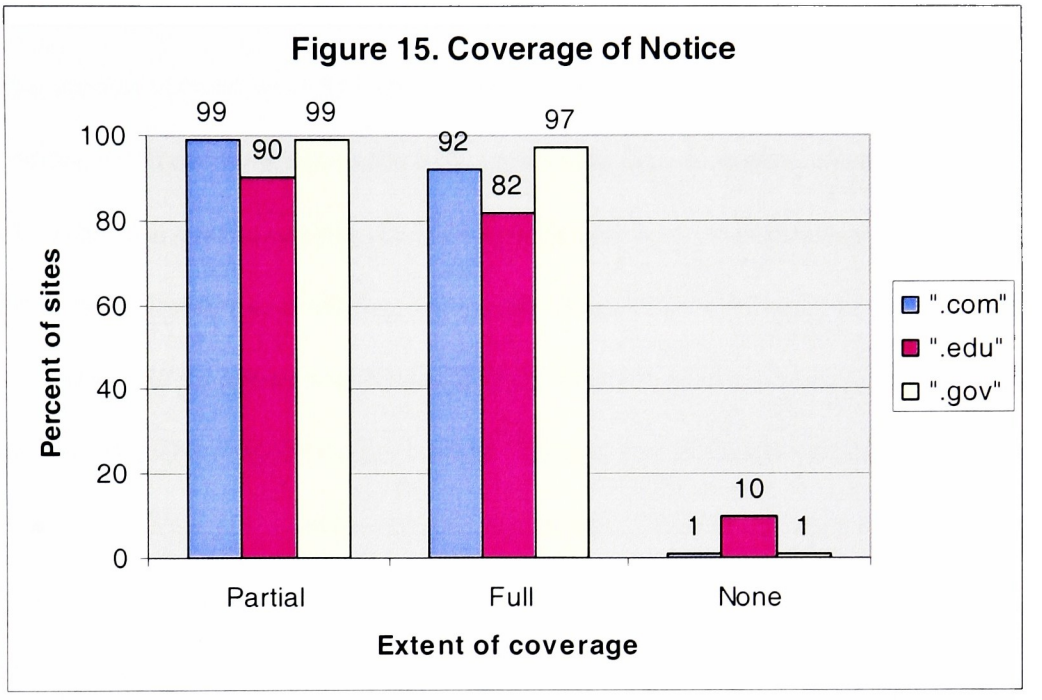

Figure 15. **The number/percentage of sites in the final samples providing partial,[7] full or no coverage of the principle of Notice in their privacy policies.**

(Source: Appendix D, Table 4)

Choice. The principle of Choice related to providing Web users with options regarding the use of the collected personally identifiable information by the Web site beyond the purposes for which the information was originally provided to the site. Under

[7] From hereon, partial coverage, unless otherwise noted, refers to the coverage of at least one individual element of a given FIP principle

this principle, a Web site has to provide a user with the choice to allow or prohibit any secondary use of the information collected about him/her by the site.[8]

The content coders were presented with multiple-choice answers in order to assess the extent of coverage of the principle of Choice in each analyzed privacy policy. The answer options were as follows: **(A)** *The Privacy Policy contains at least one complete sentence informing the user that he/she has an option, via an* ***opt-out*** *procedure, of preventing the site from sending the user any communication*, **(B)** *The Privacy Policy contains at least one complete sentence informing the user that he/she has an option, via an* ***opt-in*** *procedure, of indicating the wish to receive communication from the site*, **(C)** *The Privacy Policy contains at least one complete sentence saying that the Web site will ask for a user's consent and/or offer him/her a choice prior to sending him/her any communication but does not make clear if the consent will be acquired via an opt-in or an opt-out procedure*, **(D)** *The Privacy Policy contains at least one statement indicating that the user does not have a choice with regard to sending him/her communication from the site*, **(E)** *The Privacy Policy contains one or more statements indicating that the site requires a user's consent prior to using at least some of his/her personal information and one or more statements indicating that the user does not have a choice with regard to the use of at least some of his/her personal information*, **(F)** *The Privacy Policy contains at least one complete statement indicating that the site will never use a user's personal information beyond the purpose for which the information was*

[8] In the present study, the principle of Choice relates to the secondary uses of personally identifiable information only by the Web site itself and does not include the choice with respect to the sharing of personal information with third parties. The latter constitutes a separate principle, Disclosure to Third Parties.

originally provided or if the Privacy Policy contains a statement that the site will use the collected personal information only (a) to improve the site, (b) in aggregate form, (c) to analyze trends and/or (d) as necessary to process the user's request/order, and **(G)** *The Privacy Policy does not contain any statement indicating whether a user has any choice with regard to sending him/her communication from the site.*

As a result, the coverage of the Choice principle in the ".com" sample was as follows: 58% of sites provided users with the choice described in option A, 4% of sites provided the choice on the level of option B, 5% of sites – on the level of option C, 7% option D, 12% - option E, 5% - option F, and 9% - option G (Fig. 16).

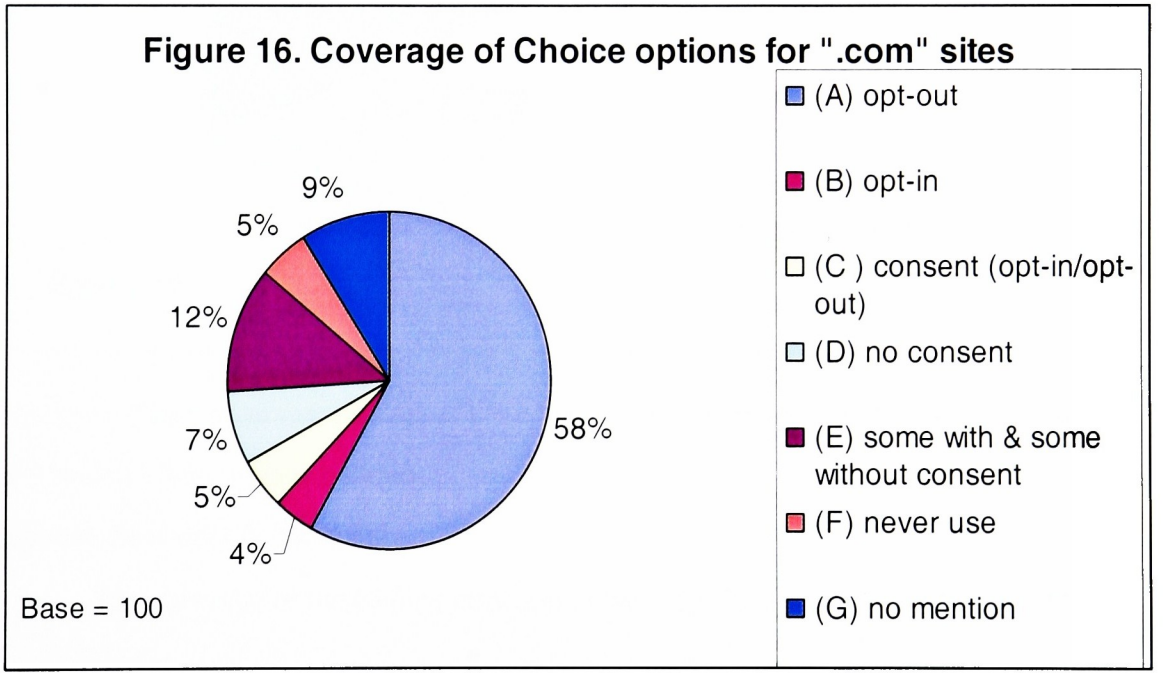

Figure 16. **The number/percentage of sites in the ".com" sample providing various options of Choice in their privacy policies.**

(Source: Appendix D, Table 5a)

The coverage of the principle of Choice in the ".edu" sample was as follows: 16% of sites provided users with the choice described in option A, 2% of sites provided choice on the level of option C, and 9% of sites provided the choice on the level of option D. The choice provided on the level of options F and G was 42% and 31%, respectively (Fig. 17).

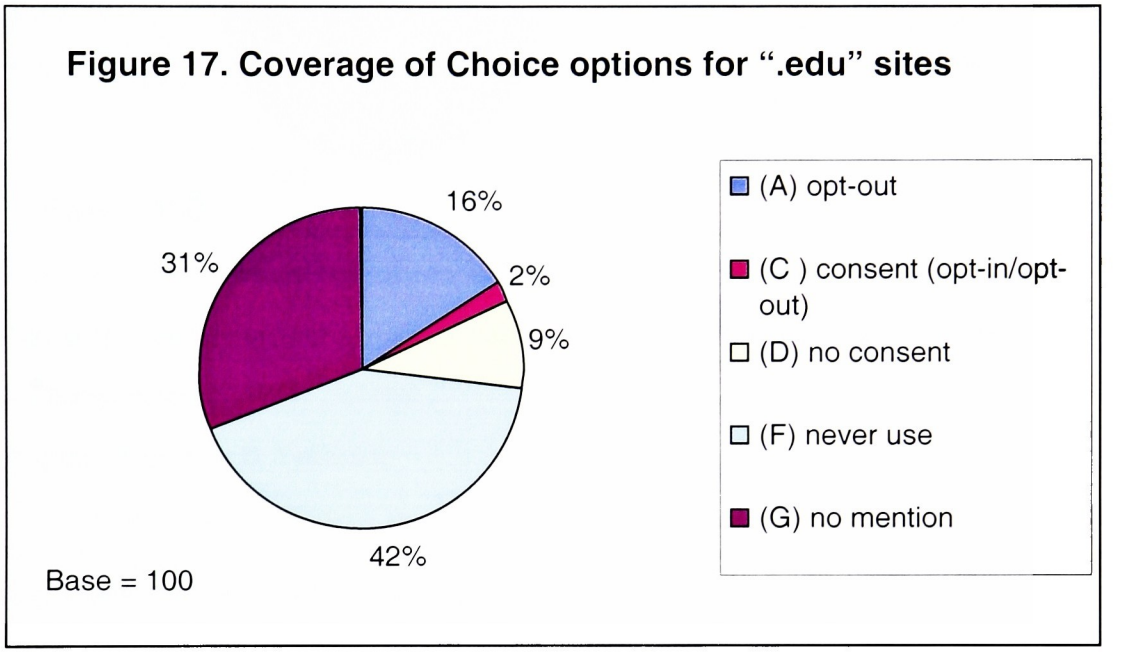

Figure 17. **The number/percentage of sites in the ".edu" sample providing various options of Choice in their privacy policies.**

(Source: Appendix D, Table 5a)

The coverage of the Choice principle in the ".gov" sample was as follows: 6% of sites provided users with the choice described in option A, 2% of sites provided the choice on the level of option B, and 10% of sites provided the choice on the level of option D. The choice provided on the level of options E, F and G was 1%, 75% and 6%, respectively (Fig. 18).

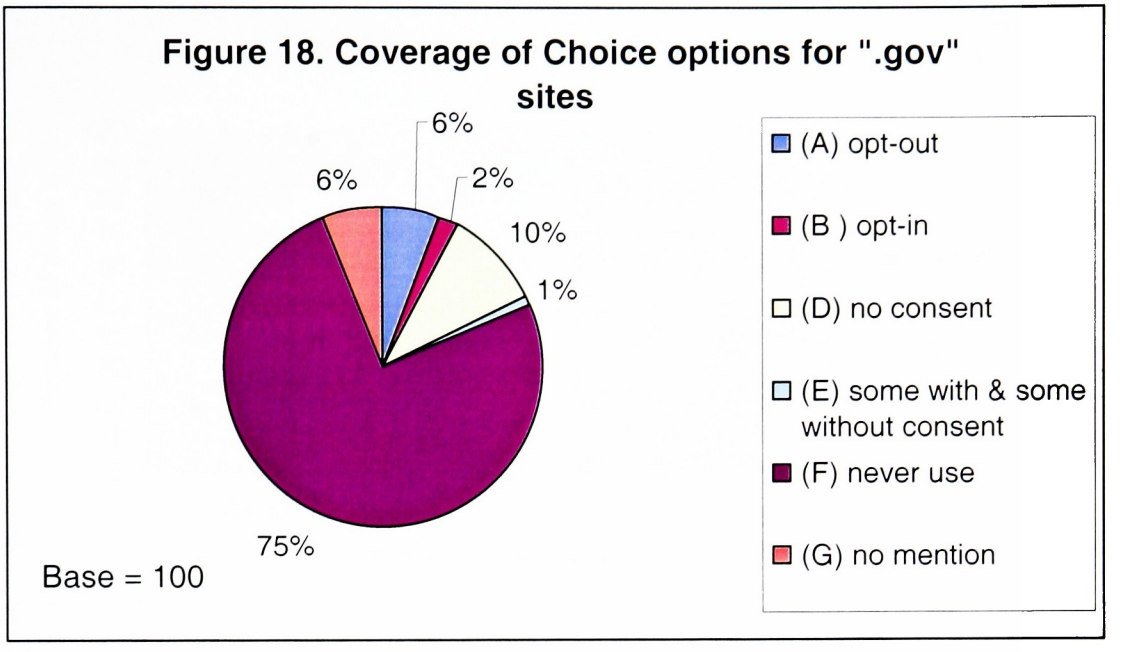

Figure 18. **The number/percentage of sites in the ".gov" sample providing various options of Choice in their privacy policies.**

(Source: Appendix D, Table 5a)

Consequently, 84% of commercial Web sites, 60% of educational sites, and 84% of governmental sites at least partly provided users with choice related to the secondary use of the collected personally identifiable information. Further, 72% of commercial Web sites, 60% of educational Web sites, and 83% of governmental Web sites provided full choice to the user. Finally, 16% of commercial, 40% of educational and 16% of governmental sites did not provide users with any choice relating to the secondary use of the collected personally identifiable information (Fig. 19).

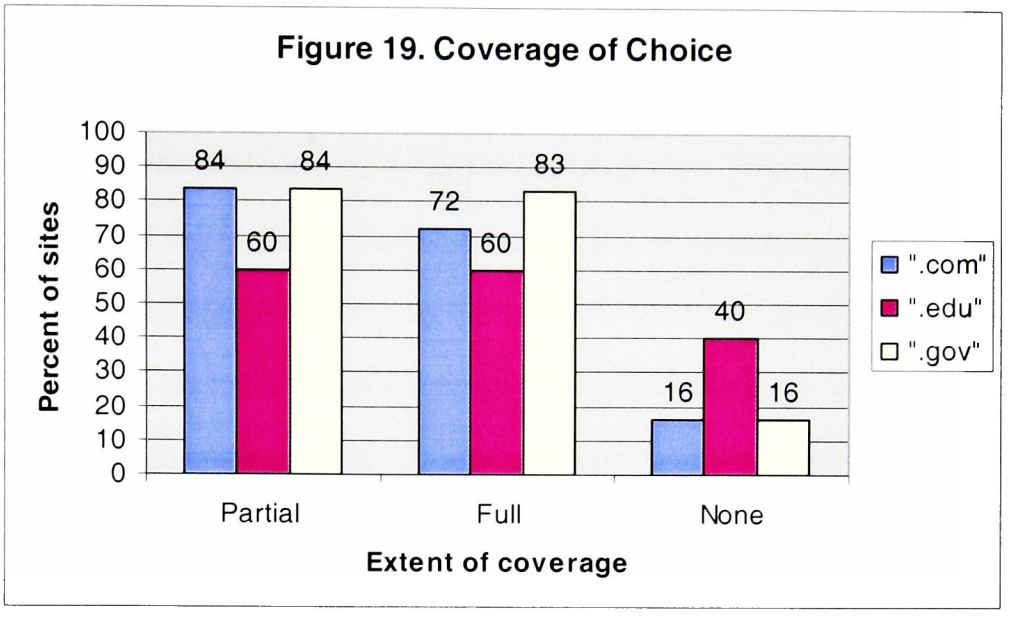

Figure 19. **The number/percentage of sites in the final samples providing partial, full or no coverage of the principle of Choice in their privacy policies.**

(Source: Appendix D, Table 5b)

Access. The principle of Access is the third major FIP principle which refers to a person's ability to access data about him/her, correct any inaccuracies and demand the removal of any objectionable data. The content analysis form incorporated three questions to determine if the privacy policy covered the principle of Access: **(1)** *Does the Privacy Policy contain at least one complete sentence indicating that the user can review the personal information collected by the Web site?* **(2)** *Does the Privacy Policy contain at least one complete sentence indicating that the user can edit the personal information collected by the Web site?* and **(3)** *Does the Privacy Policy contain at least one complete sentence indicating that the user can delete at least some of the personal information collected by the Web site?*

The analysis of the answers to the first question demonstrates that 64% of commercial Web sites, 19% of educational Web sites and 8% of governmental Web sites provided some mechanism allowing a user to review the personal information collected by the site. Furthermore, 64% of commercial, 22% of educational and 8% of governmental sites provided a way for the user to update or correct the information that had been collected about him/her. Finally, 39% of commercial, 8% of educational and 8% of governmental sites allowed users to have at least some collected personal information removed from the site's databases (Fig. 20).

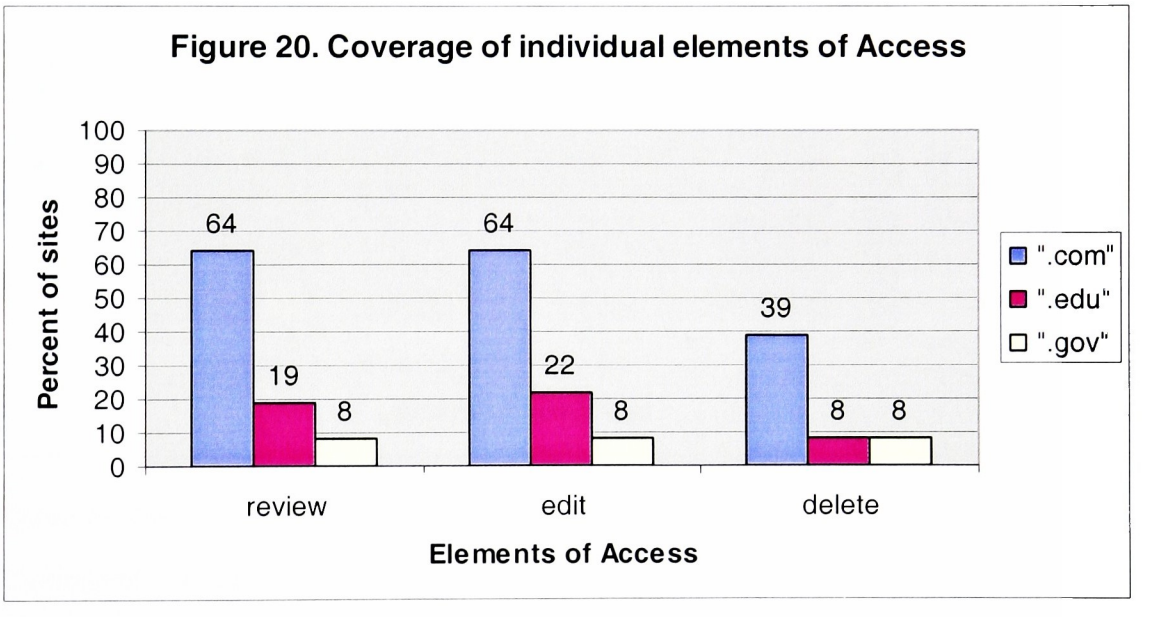

Figure 20. **The number/percentage of sites in the final samples providing coverage for individual elements of Access in their privacy policies.**

(Source: Appendix D, Table 6)

Consequently, 68% of commercial Web sites, 24% of educational Web sites, and 13% of governmental Web sites at least partly covered the category of Access in their privacy policies (i.e., they allowed users to review, to edit or to delete some personal

information collected by the site). Further, 63% of commercial sites, 18% of educational sites, and 7% of governmental sites covered the category of Access by allowing both to review and to edit at least some personal information collected by the site. Finally, 36% of commercial, 5% of educational and 3% of governmental sites fully covered the Access principle in their privacy policies (i.e., they allowed users to review, to edit and to delete some personal information collected by the site) (Fig. 21).

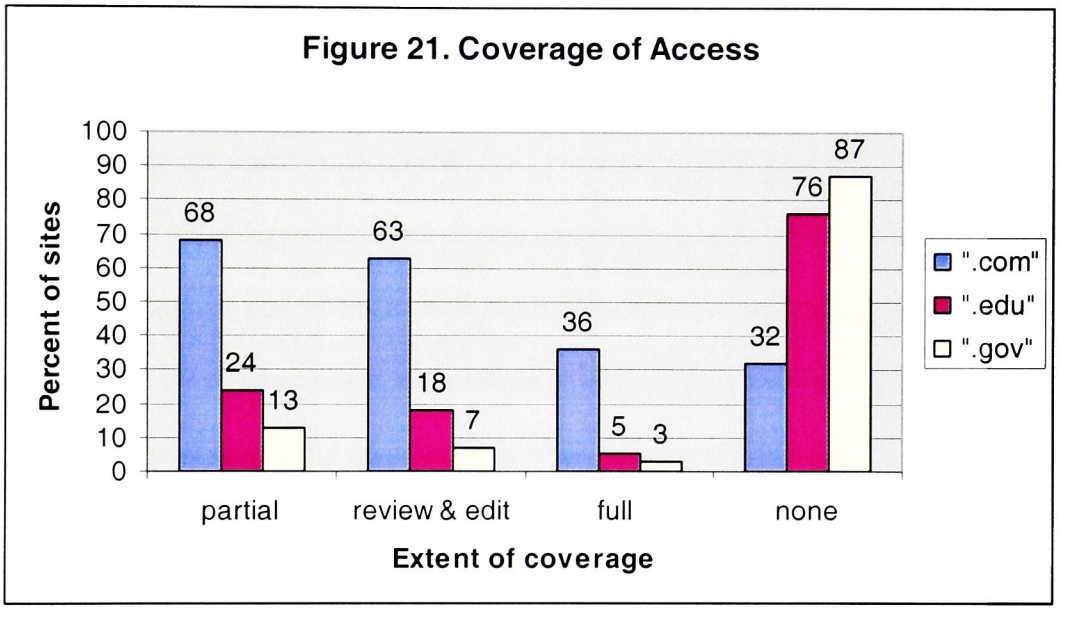

Figure 21. **The number/percentage of sites in the final samples providing partial, full or no coverage of Access in their privacy policies.**

(Source: Appendix D, Table 6)

Security. The principle of security refers to site's obligation to protect electronically collected personal information from unauthorized access, use, disclosure or loss. The study assessed the extent to which Web site privacy polices disclose security measures undertaken to safeguard users' personal data from unauthorized access and use. The following three questions were asked to determine the essence of disclosures about

security: **(1)** *Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security for the information it collects from users?* **(2)** *Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security during transmission of personal information to the site?* **(3)** *Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security during the storage of personal information collected from users?* and **(4)** *Does the Privacy Policy contain at least one complete sentence indicating what specific tools or measures the site uses to protect the user's personal information from being intercepted by unauthorized third parties both during transmission and/or subsequent storage?*

The analysis of the answers to the first question reveals that 69% of commercial Web sites, 42% of educational Web sites and 24% of governmental Web sites provided at least basic some disclosure about the use of security mechanisms by the Web site to protect the electronically collected personal information. Furthermore, 47% of commercial, 22% of educational and 16% of governmental sites specifically mentioned the use of security measures during transmission of personal information to the site. Additionally, 55% of commercial, 23% of educational and 10% of governmental sites mentioned the use of security mechanism to protect personal information during its storage. Finally, 58% of commercial, 27% of educational and 18% of governmental sites named specific security mechanisms that were used by the site to safeguard the collected personal information (Fig. 22).

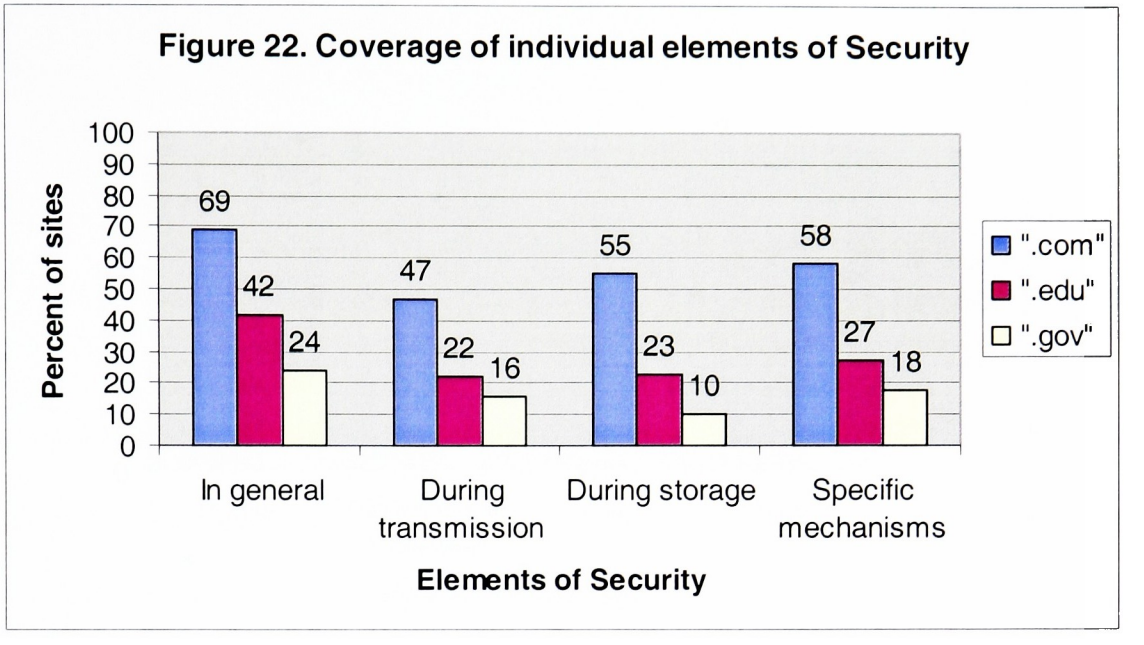

Figure 22. **The number/percentage of sites in the final samples providing individual elements of Security in their privacy policies.**

(Source: Appendix D, Table 7)

Consequently, 69% of commercial Web sites, 42% of educational Web sites, and 24% of governmental Web sites at least partly covered the category of Security in their privacy policies (i.e., they provided at least some information about security measures to protect the personal information collected by the site). Further, 40% of commercial sites, 13% of educational sites, and 9% of governmental sites covered the category of Security by informing the user of security measures during both transmission and storage of personal information. Finally, 39% of commercial, 12% of educational and 8% of governmental sites fully covered the Security principle in their privacy policies (i.e., they informed the user of security measures during both transmission and storage of personal information and name specific mechanism employed in this process) (Fig. 23).

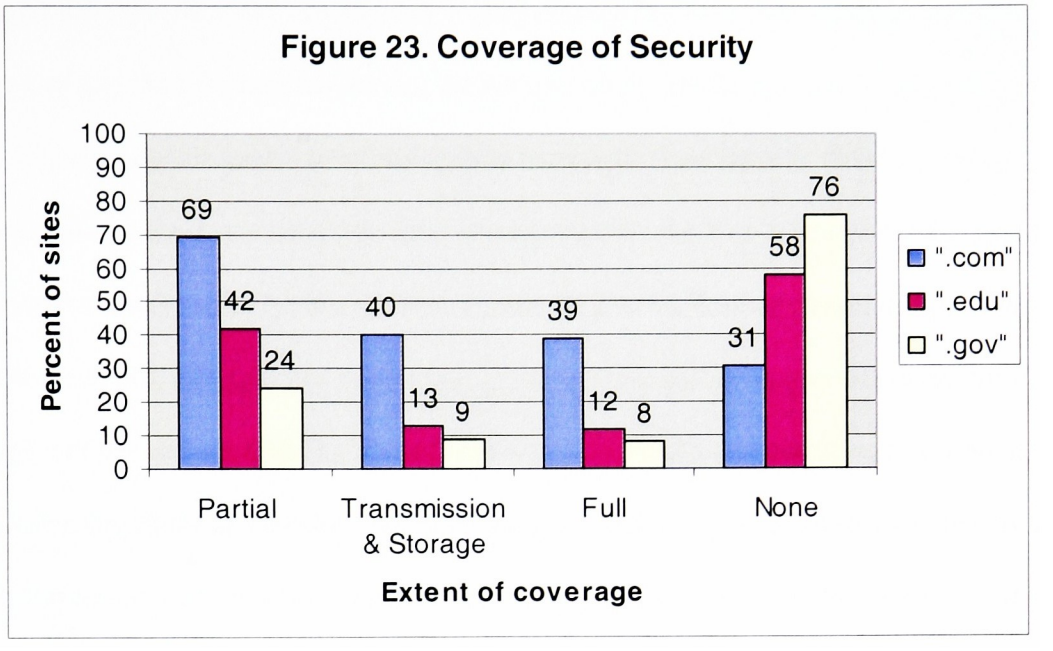

Figure 23. **The number/percentage of sites in the final samples providing partial, full or no coverage of the principle of Security in their privacy policies.**

(Source: Appendix D, Table 7)

Disclosure to Third Parties. The principle of Disclosure to Third Parties requires that a Web site provide users with options regarding the disclosure of the collected personally identifiable information to third parties beyond the purposes for which the information was originally provided to the site. Under this principle, a Web site has to provide a user with the choice to allow or prohibit any secondary use by third parties of the information collected about him/her.

The content coders were presented with multiple-choice answers in order to assess the extent of coverage of the principle of Disclosure to Third Parties in each analyzed privacy policy. The answer options were as follows: **(A)** *The Privacy Policy contains at least one complete sentence informing the user that he/she has an option, via an* ***opt-out*** *procedure, of preventing the site from sharing the user's personal information*

with third parties, **(B)** *The Privacy Policy contains at least one complete sentence informing the user that he/she has an option, via an* ***opt-in*** *procedure, of indicating the wish to share the user's personal information with third parties*, **(C)** *The Privacy Policy contains at least one complete sentence saying that the Web site will ask for a user's consent and/or offer him/her a choice prior to sharing his/her personal information with third parties, but does not make clear if the consent will be acquired via an opt-in or an opt-out procedure*, **(D)** *The Privacy Policy contains at least one complete statement indicating that the user does not have a choice with regard to sharing his/her personal information with third parties*, **(E)** *The Privacy Policy contains one or more statements indicating that the site requires a user's consent prior to sharing at least some of his/her personal information with a third party and one or more statements indicating that the user does not have a choice with regard to the sharing of at least some of his/her personal information with third parties*, **(F)** *The Privacy Policy contains one or more statements indicating that the site will never share personal information with third parties, or if the Policy contains a statement that the site will share personal information only (a) if required to do so by law, (b) in aggregate form, (c) as necessary to process the user's order, (d) to protect the security of other users, (e) to protect the integrity of the site, and (f) if the user's actions are in violation of the Web site's terms of use*, and **(G)** *The Privacy Policy does not contain any sentence offering users a choice and/or requiring their consent with regard to sharing their personal information with third parties.*

As a result, the coverage of the Disclosure to Third Parties principle in the ".com" sample was as follows: 34% of sites provided users with the choice described in option A, 2% of sites provided the choice on the level of option B, and 23% of sites provided the choice on the level of option C. The choice provided on the level of options D, E, F, and G was 2%, 10%, 28%, and 1%, respectively (Fig. 24).

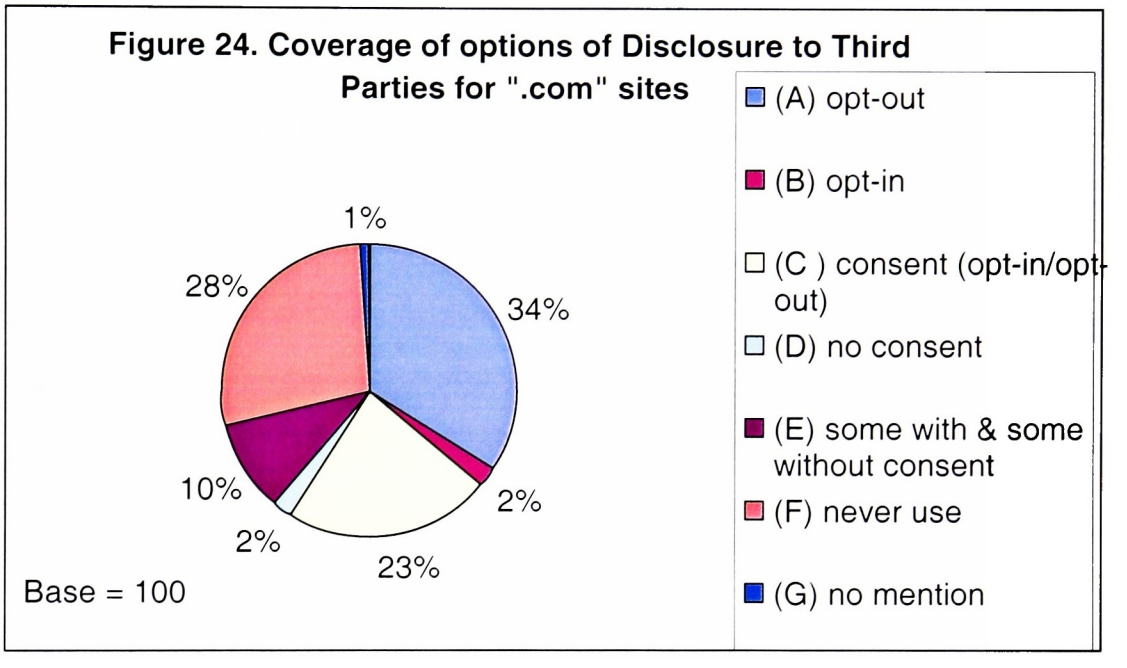

Figure 24. **The number/percentage of sites in the ".com" sample providing various options of Disclosure to Third Parties in their privacy policies.**

(Source: Appendix D, Table 8a)

The coverage of the principle of the Disclosure to Third Parties in the ".edu" sample was as follows: 2% of sites provided users with the choice described in option A, 3% of sites provided the choice on the level of option B, and 16% of sites provided the choice on the level of option C. The choice provided on the level of options D, F, and G was 8%, 53%, and 18%, respectively (Fig. 25).

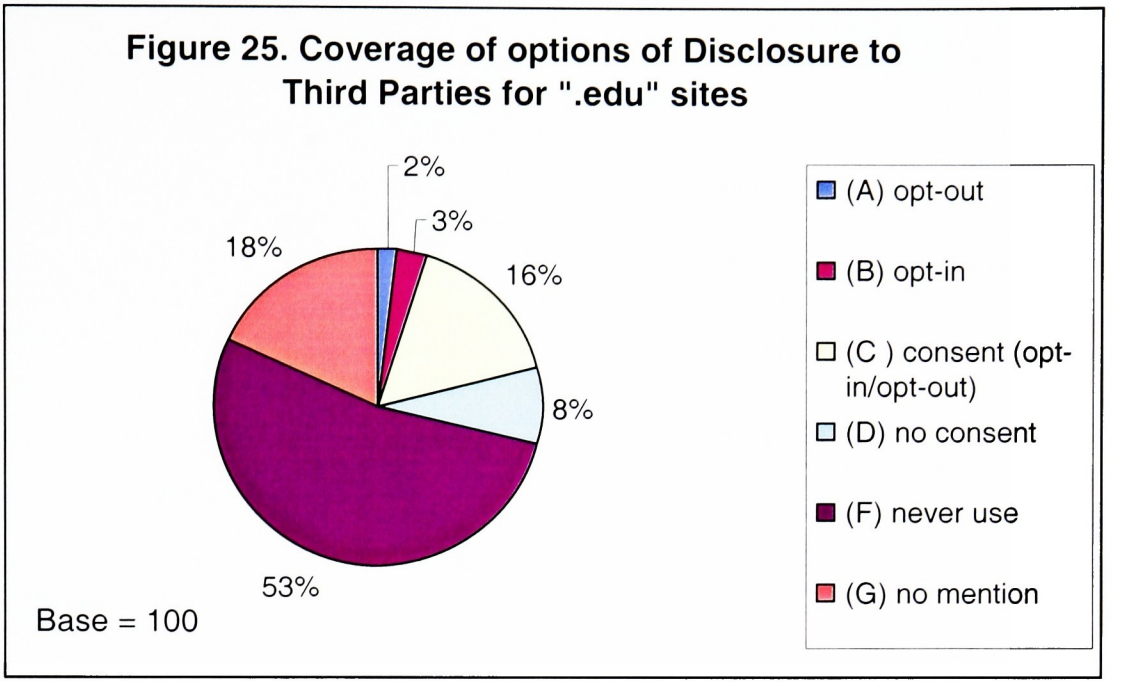

Figure 25. **The number/percentage of sites in the ".edu" sample providing various options of Disclosure to Third Parties in their privacy policies.**

(Source: Appendix D, Table 8a)

The coverage of the Disclosure to Third Parties principle in the ".gov" sample was as follows: 1% of sites provided users with the choice described in option A, 6% of sites provided the choice on the level of option C, and 33% of sites provided the choice on the level of option D. The choice provided on the level of options E, F, and G was 2%, 50%, and 8%, respectively (Fig. 26).

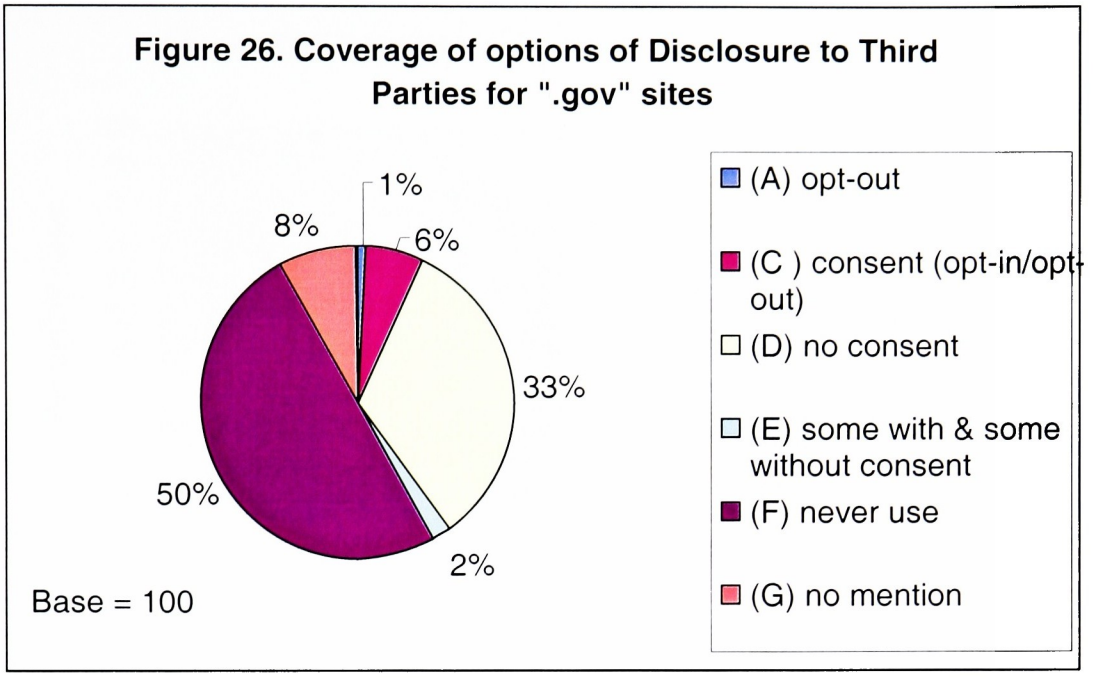

Figure 26. **The number/percentage of sites in the ".gov" sample providing various options of Disclosure to Third Parties in their privacy policies.**

(Source: Appendix D, Table 8a)

Consequently, 97% of commercial Web sites, 74% of educational Web sites, and 59% of governmental Web sites provided users with some choice related to the disclosure of their personally identifiable information to third parties beyond the original purpose for which the data were collected. Further, 87% of commercial sites and 74% of educational sites, and 57% of governmental sites provided full choice to the user. Finally, 3% of commercial, 26% of educational and 41% of governmental sites did not provide users with any choice relating to the disclosure of the collected personally identifiable information to third parties (Fig. 27).

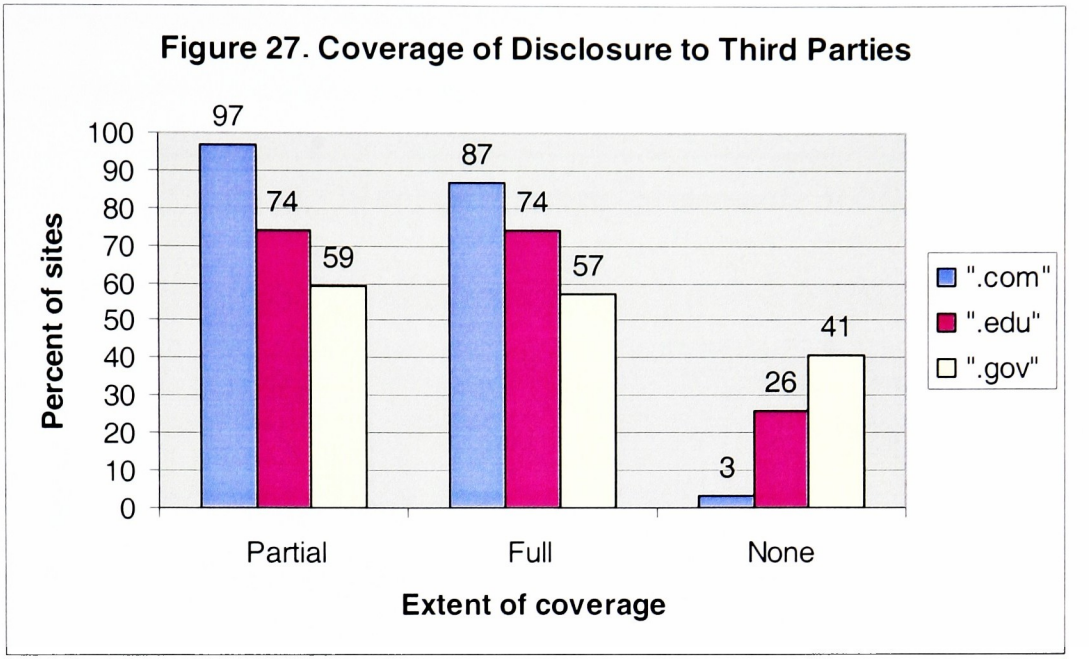

Figure 27. **The number/percentage of sites in the final samples providing partial, full or no coverage of the principle of Disclosure to Third Parties in their privacy policies. (Source: Appendix D, Table 8b)**

Cookies. The principle of Cookies requires that a Web site's privacy policy disclose whether the site uses or may use cookies and explain what a cookie is. Two items were incorporated into the content analysis form in order to assess the compliance with this principle. The questions were as follows: **(1)** *Does the Privacy Policy contain at least one complete sentence saying anything about whether the site does or may use cookies?* and **(2)** *Does the Privacy Policy contain at least one complete sentence indicating what a cookie is and/or explaining the purpose of its use?*

The answers to the first question indicated that 87% of commercial Web sites, 57% of educational Web sites, and 62% of governmental Web sites informed users in their privacy policies whether a site might or did use cookies. Further, 84% of

commercial Web sites, 53% of educational Web sites, and 55% of governmental Web sites explained to users what a cookie was (Fig. 28).

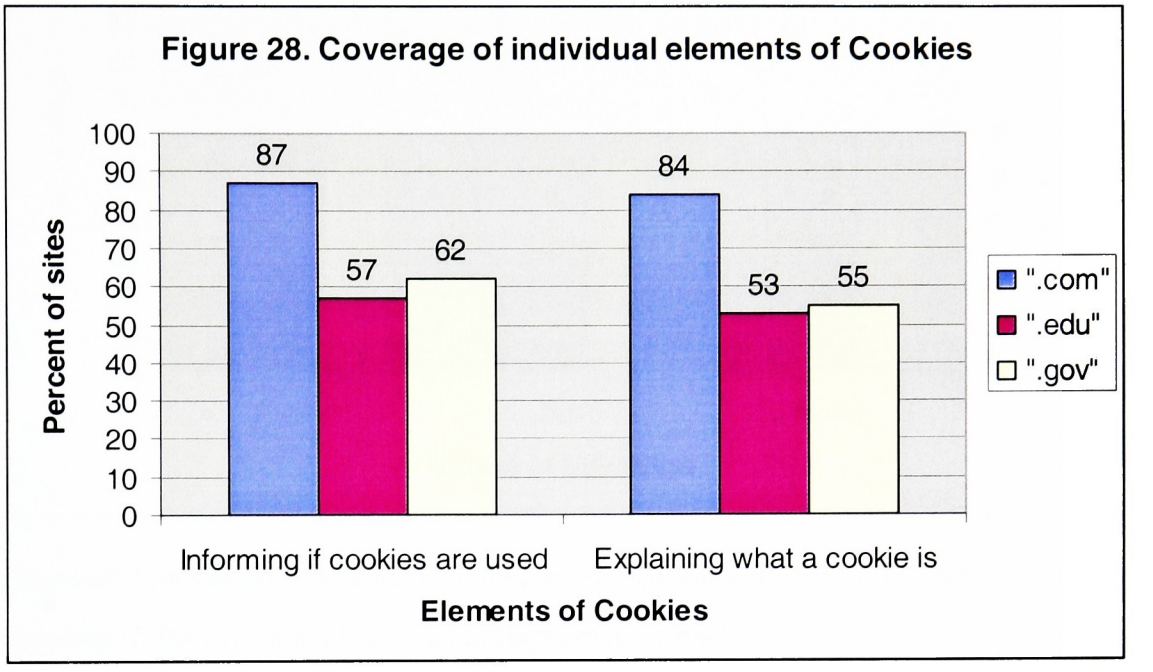

Figure 28. **The number/percentage of sites in the final samples providing individual elements of Cookies in their privacy policies.**

(Source: Appendix D, Table 9)

As a result, 87% of commercial Web sites, 57% of educational Web sites, and 62% of governmental Web sites at least partly covered the principle of Cookies in their privacy policies (i.e., they informed the users whether the site did or might collect information via cookies). Finally, 84% of commercial Web sites, 53% of educational Web sites, and 54% of governmental Web sites fully covered the principle of Cookies (i.e., they informed the users whether the site did or might use cookies and explained what a cookie was) (Fig. 29).

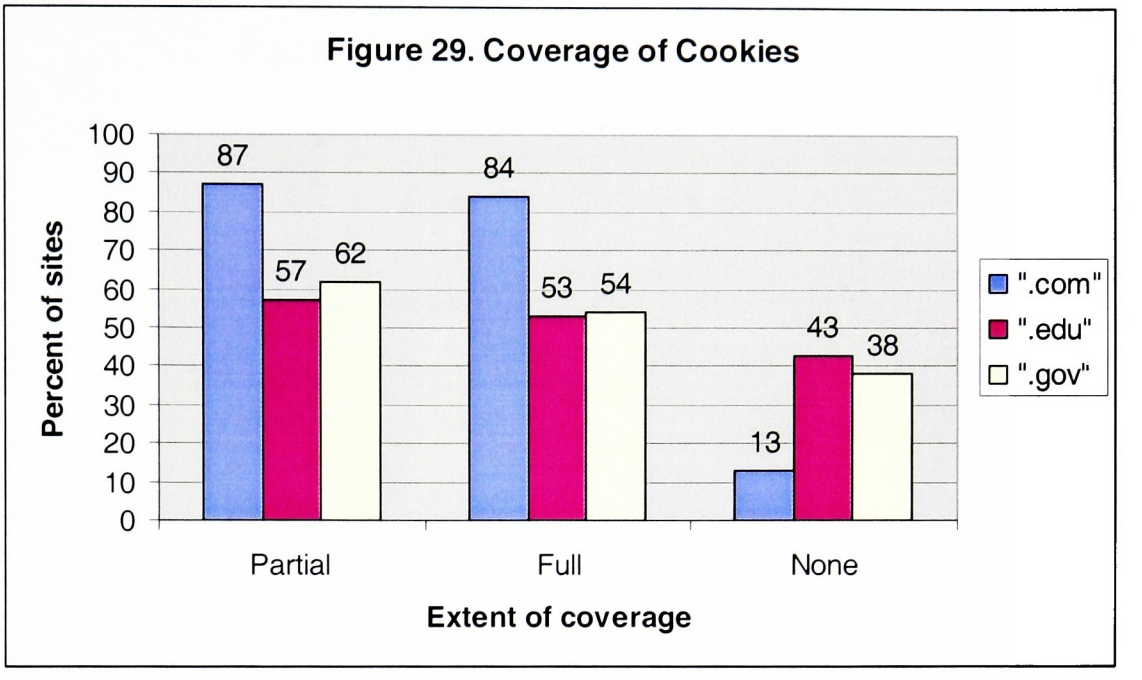

Figure 29. **The number/percentage of sites in the final samples providing partial, full or no coverage of the principle of Cookies in their privacy policies.**

(Source: Appendix D, Table 9)

Contact Information. The principle of Contact Information demands that a privacy policy include contact information that Web site visitors could utilize if they had any questions or concerns related to the site's privacy policy. The content analysis form included one question directly asking if the privacy policy posted such contact information.

As a result, 92% of commercial Web sites, 68% of educational Web sites, and 48% of governmental Web sites covered the principle of Contact Information within their privacy policies (Fig. 30).

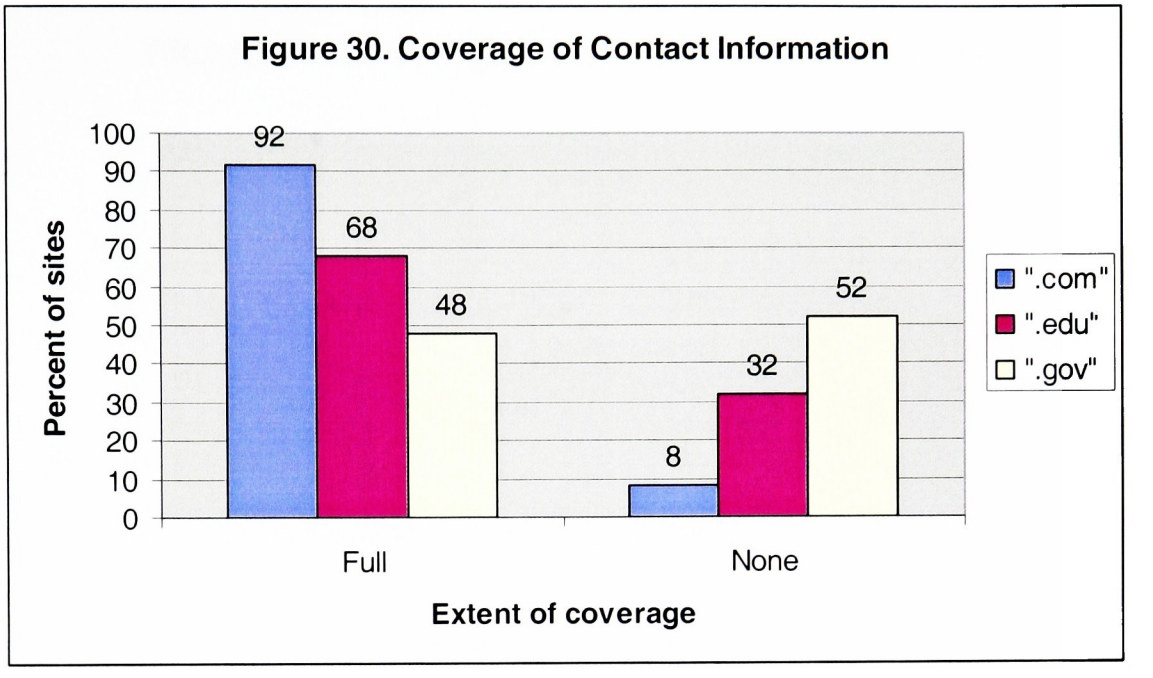

Figure 30. **The number/percentage of sites in the final samples providing full or no coverage of the principle of Contact Information in their privacy policies.**

(Source: Appendix D, Table 10)

Coverage of Various Combinations of Fair Information Practice Principles

The data analysis results showed that 55% of commercial, 9% of educational and 4% of governmental Web sites at least partly covered in their privacy policies all seven principles of fair information practice: Notice, Choice, Access, Security, Disclosure to Third Parties, Cookies, and Contact Information. However, only 13% of commercial, 1% of educational and 2% of governmental Web sites fully complied with all the seven principles of fair information practice (Fig. 31).

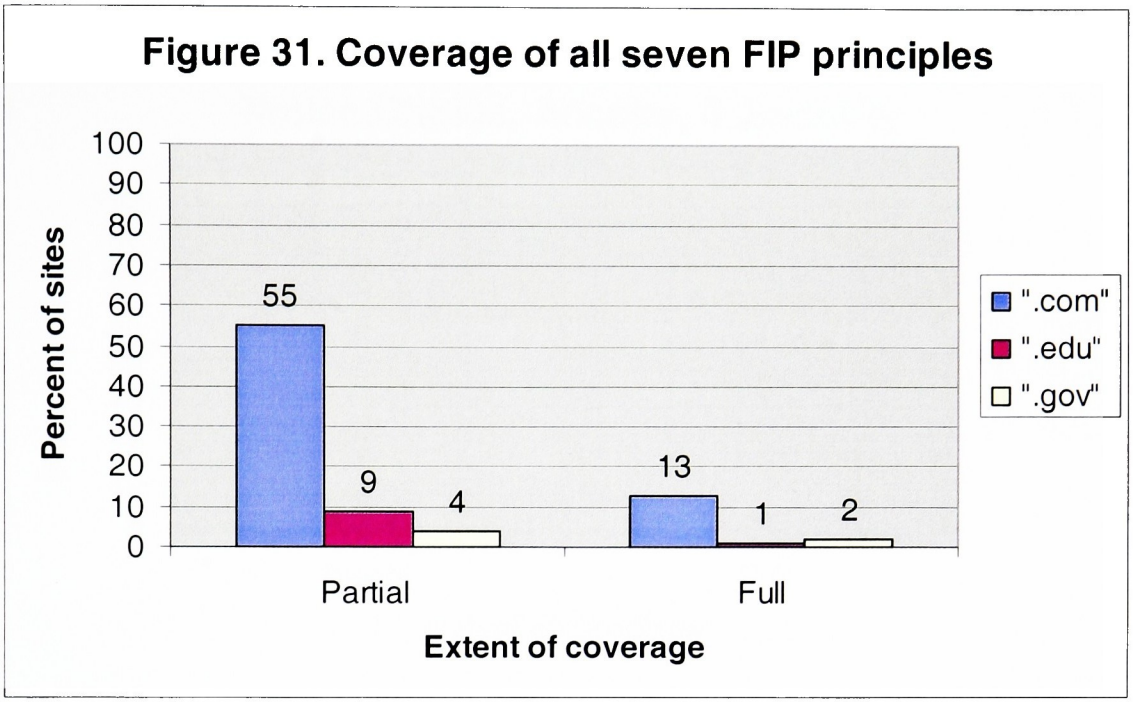

Figure 31. **The number/percentage of sites in the final samples providing full and partial coverage of all seven FIP principles: Notice, Choice, Access, Security, Disclosure to Third Parties, Cookies, and Contact Information.**

(Source: Appendix D, Table 12)

The percentage of Web sites at least partly covering four major FIP principles – Notice, Choice, Access, and Security – in their privacy policies was higher in each of the three domains: 57% of ".com" Web sites, 14% of ".edu" sites, and 11% of ".gov" sites. As for the full coverage of the four FIP principles, it was provided in 17% of commercial Web sites, 1% of educational Web sites, and 2% of governmental Web sites (Fig. 32).

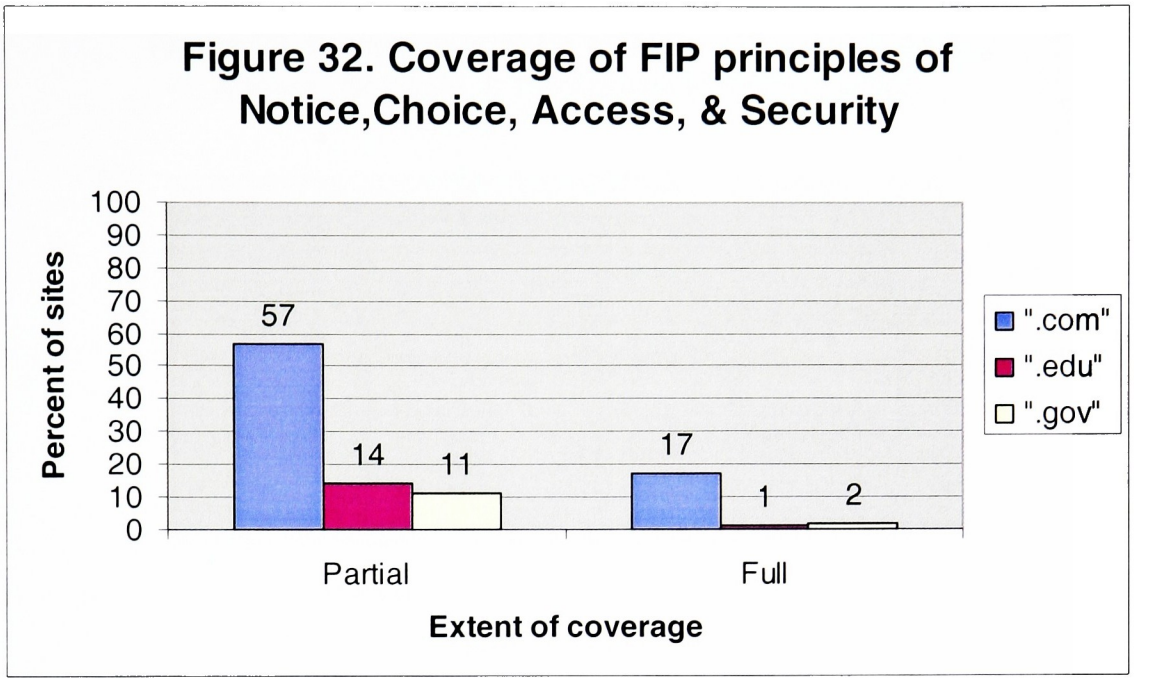

Figure 32. **The number/percentage of sites in the final samples providing full and partial coverage of four major FIP principles: Notice, Choice, Access, and Security. (Source: Appendix D, Table 12)**

The percentage of Web sites covering the four major FIP principles of Notice, Choice, Access, Security and a fifth principle of Disclosure to Third Parties was a little lower (most noticeably in the ".gov" sample) than the coverage of the four FIP principles. Thus, 57% of commercial, 12% of educational, and 5% of governmental sites provided at least partial coverage of the five principles. Full coverage was implemented by 14% of commercial, 1% of educational, and 2% of governmental Web sites (Fig. 33).

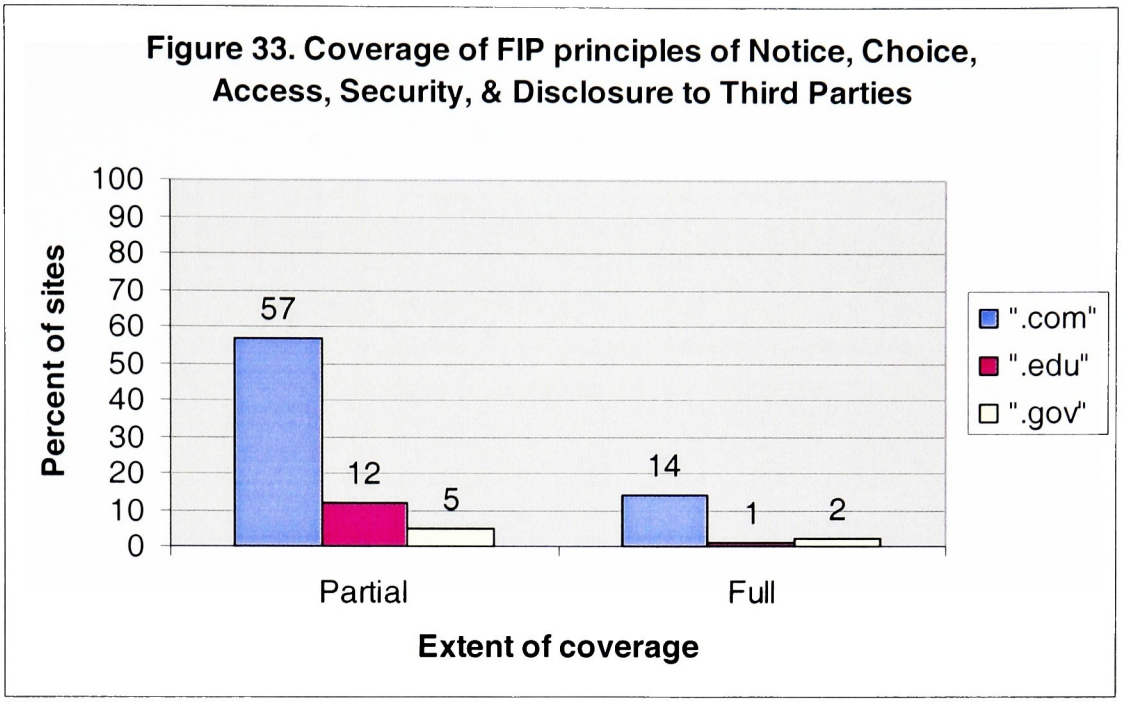

Figure 33. **The number/percentage of sites in the final samples providing full and partial coverage of five FIP principles: Notice, Choice, Access, Security, and Disclosure to Third Parties.**

(Source: Appendix D, Table 12)

The percentage of sites covering six FIP principles – Notice, Choice, Access, Security, Disclosure to Third Parties, and Contact Information – was very close to the corresponding figures for all threes samples in the coverage of the five FIP principles of Notice, Choice, Access, Security, and Disclosure to Third Parties: 56% (partial coverage) and 14% (full coverage) of ".com" sites, 11% (partial) and 1% (full) of ".edu" sites, and 4% (partial) and 2% (full) of ".gov" sites (Fig. 34).

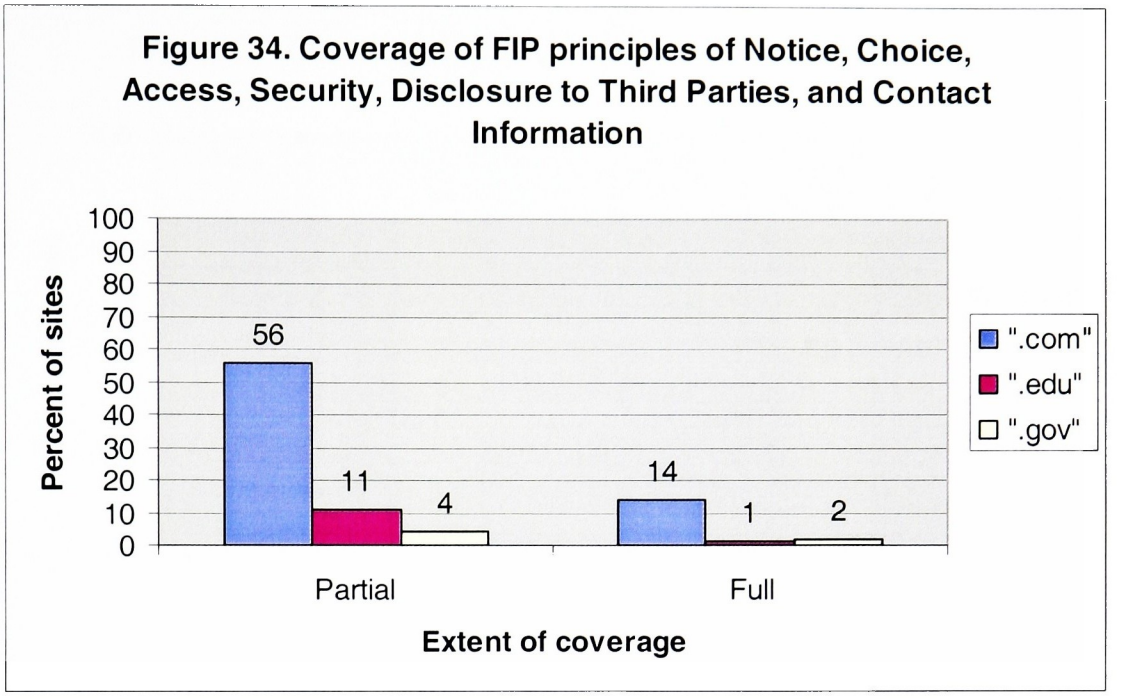

Figure 34. **The number/percentage of sites in the final samples providing full and partial coverage of five FIP principles: Notice, Choice, Access, Security, Disclosure to Third Parties, and Contact Information.**

(Source: Appendix D, Table 12)

The percentage of sites covering the two fundamental FIP principles – Notice and Choice – in the privacy policies was as follows: 84% (partial coverage) and 68% (full coverage) of commercial Web sites, 56% (partial) and 55% (full) of educational sites, and 84% (partial) and 82% (full) of governmental Web sites (Fig. 35).

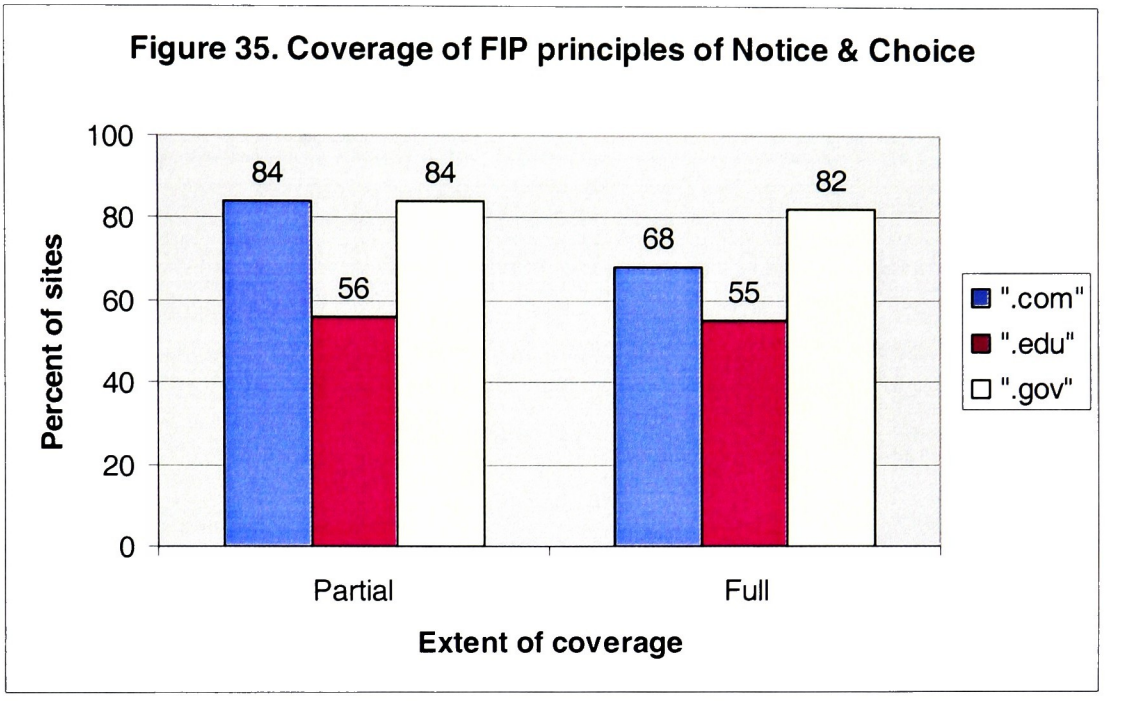

Figure 35. **The number/percentage of sites in the final samples providing full and partial coverage of two fundamental FIP principles: Notice and Choice.**

(Source: Appendix D, Table 12)

The percentage of Web sites covering the two mentioned fundamental FIP principles of Notice and Choice, and a third principle of Disclosure to Third Parties was a little lower than the coverage of the two FIP principles of Notice and Choice for ".com" sites and substantially lower than the coverage of the two principles in the ".gov" and ".edu" samples. Thus, 84% of commercial, 48% of educational, and 53% of governmental sites provided at least partial coverage of the three principles. Full coverage was implemented by 62% of commercial, 48% of educational, and 51% of governmental Web sites (Fig. 36).

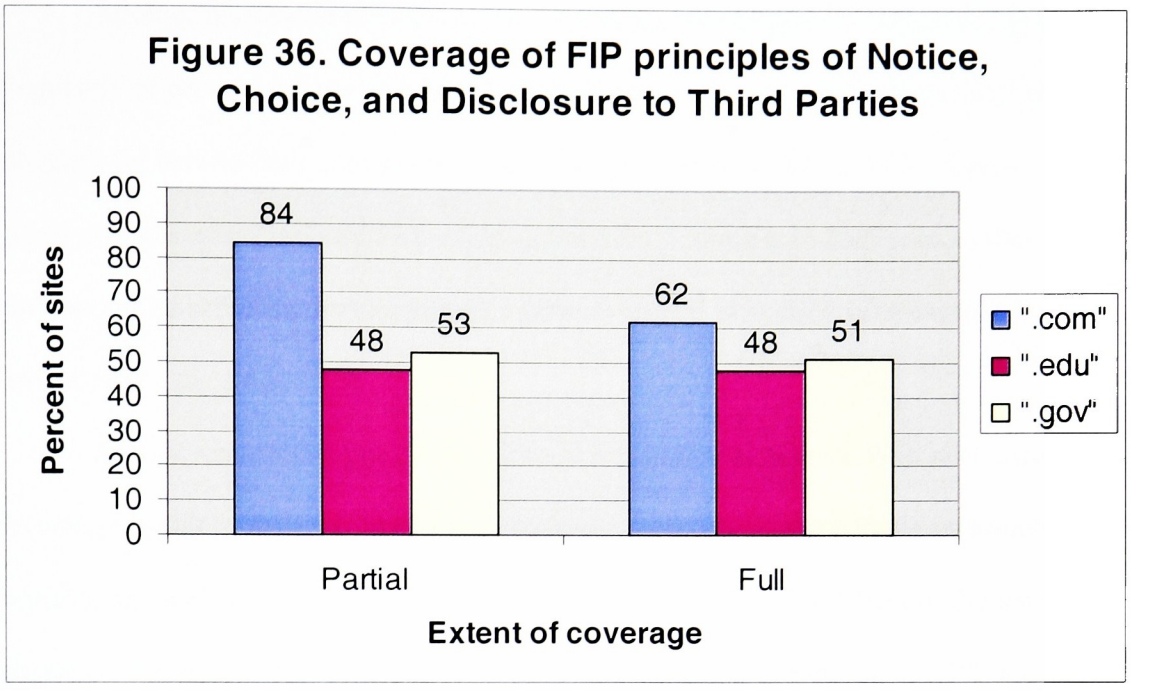

Figure 36. **The number/percentage of sites in the final samples providing full and partial coverage of three FIP principles: Notice, Choice, and Disclosure to Third Parties. (Source: Appendix D, Table 12)**

Summary of Research Findings

The study revealed a number of differences among the privacy policies of commercial, educational, and governmental Web sites.

The Web site eligibility survey demonstrated that the overwhelming majority of pre-qualifying sites in all three sampling pools collected email addresses from Web users. However, the figures reflecting the collection of the remaining three types of personally identifiable information – name, postal address and phone number – for commercial Web sites were almost twice as high as the corresponding results for governmental and educational sites (Fig. 12).

Another noticeable difference revealed by the site eligibility check was in the frequency of privacy policies for the three Web site categories, with educational sites standing far behind both commercial and governmental sites. While 96% of pre-qualifying governmental and 87% of pre-qualifying commercial Web sites in the corresponding sampling frames posted a privacy policy, only 36% of pre-qualifying educational sites did so (Fig.11).

A third remarkable point of difference was in the number of Web sites using cookies. Similar to their performance in gathering personally identifiable information, commercial Web sites outnumbered educational and governmental sites in the use of cookies: 84% of eligible sites in the ".com" sampling pool as opposed to 53% and 60% in the educational and governmental sampling pools, respectively (Fig. 13).

The content analysis of the Web privacy policies in three final samples revealed numerous differences in the way commercial, educational, and governmental Web sites implemented the principles of fair information practice. The performance in the coverage of the individual elements[9] of the most fundamental FIP principle, Notice, was slightly lower in the ".edu" sample than in the two others. The same holds true for the partial and full coverage of the Notice principle: 90% of educational sites provided partial and 82% - full coverage of Notice in their privacy policies, as opposed to 99% (partial coverage) and 92% (full coverage) of commercial and 99% (partial) and 97% (full) of governmental Web sites.

---

[9] The principle of Notice is made up of two individual elements: (1) informing the user of the type(s) of electronically collected personal information the site gathers, and (2) informing the user of the uses the electronically collected personal information can be put to.

The differences in the coverage of the principle of Choice were more substantial than in the coverage of Notice. Thus, commercial sites greatly outnumbered educational and governmental sites in the use of an opt-out procedure to provide Web users with choice regarding any secondary use of their personal information by the site: 58% of commercial sites as opposed to 16% of educational and 6% of governmental sites. In other words, over a half of commercial privacy policies were telling to their users that, unless a user specifically told the site not to send him/her any email communication, the site would do so.

Governmental sites, in turn, appeared to champion the practice of never putting the collected personal information to secondary uses. Thus, 75% of governmental privacy policies specifically mentioned that they would not contact a user unless it was necessary to process his/her order or request. The corresponding number for educational sites was at a lower but still a remarkable level of 42%. However, only 5% of commercial sites used their privacy policies to communicate the promise of not using personal information for secondary purposes.

Another point of noticeable difference was in the number of sites completely ignoring the principle of Choice. Thus, 31% of educational Web privacy policies did not say anything about the user's choice with regard to sending him/her any future communication from the site, while the corresponding figures for commercial and governmental sites were 9% and 6%, respectively. As a result, only 60% of privacy policies in the ".edu" sample provided full coverage of the Choice principle, as opposed to 72% of policies in the ".com" and 83% in the ".gov" samples (Fig. 19).

The principle of Access appeared to be one of the weakest points for both governmental and educational Web sites. Thus, 87% of ".gov" and 76% of ".edu" privacy policies did not have a single statement informing the user of his/her rights to review, update or delete the personal information collected by the site. Commercial privacy policies, on the contrary, attached substantial importance to this principle of fair information practice: 63% of Web policies in the ".com" sample informed users of the ways to both review and update their personal information, and 36% additionally allowed having at least some information to be removed from the site's database (i.e., provided the full coverage of Access) (Fig. 21).

Similar to the principle of Access, the performance of governmental and educational sites in the coverage of the principle of Security was lower than that of commercial Web sites. While 69% of ".com" sites provided at least some information about the existence of security measures on the site to protect consumer's personal information (i.e., partially covered the principle of Security), only 42% of educational and 24% of governmental sites did so. Furthermore, 47% of commercial Web privacy policies specifically mentioned the use of security measures to protect consumers' information during transmission, and 55% indicated that they stored collected personal information in a secure environment. The corresponding numbers for educational and governmental sites were 22% and 16% (security during transmission) and 23% and 10% (security during storage), respectively. As a result, the full coverage of the Security principle was provided by 39% of commercial Web sites, as opposed to 12% of educational and 8% governmental sites (Fig. 23).

One possible explanation for the sharp differences in the coverage of Access and Security among the three samples is in the fact that commercial sites collect more personally identifiable information than educational or governmental Web sites. Consequently, they may experience a greater need to communicate to users the options for accessing the collected personal information and explain the security measures taken to protect sensitive information from unauthorized interception. The graph below demonstrates a relationship between the collection of one type of personally identifiable information (name) and the extent of coverage for the principles of Access among three domains: the higher is the level of information collection, the higher is the coverage of Access (Fig. 37).

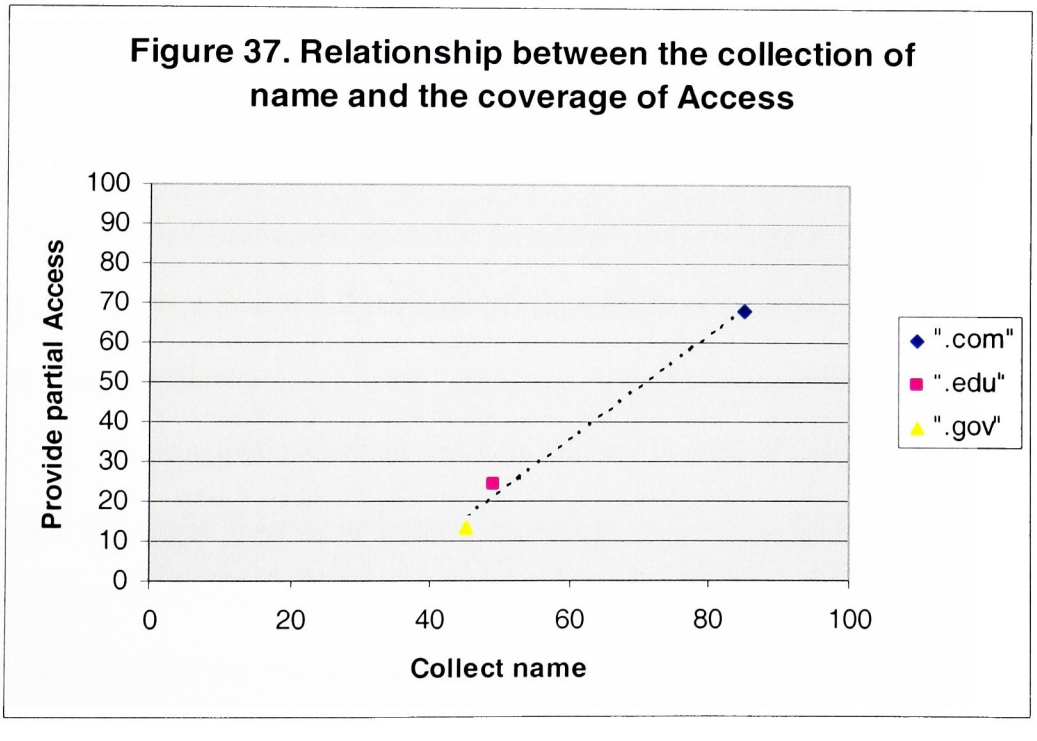

Figure 37. **The relationship between the collection of information (name) and the coverage of Access (partial). (Source: Appendix D, Tables 2 and 6)**

The pattern of differences in the coverage of the principle of Disclosure to Third Parties was very similar to the one found in the coverage of Choice. Again, commercial sites championed the concept of opting-out with 34% of privacy policies specifically mentioning that the site would share personal information with third parties unless otherwise instructed by the user. The corresponding figures for educational and governmental sites were 2% and 1%, respectively. In addition, over 50% of both governmental and educational privacy policies, as opposed to 28% of commercial ones, clearly indicated that they would never share the collected personal information with third parties unless required to do so by law.

A difference among the three samples was also noticeable in the sharing of information without consent. While only 2% of commercial and 8% of educational sites mentioned the possibility of non-consensual sharing of personal information with third parties, 33% of governmental sites indicated that they would share collected personal information with other state agencies. As a result, only 57% of privacy policies in the ".gov" sample provided full coverage of the principle of Disclosure to Third Parties, as opposed to 87% of policies in the ".com" and 74% of policies in the ".gov" sample.

The principle of Cookies was fully covered by 84% of commercial Web sites, which was higher than the corresponding 53% in the ".edu" and 54% in the ".gov" samples. The comparison of these figures with the data on the actual use of cookies collected during the Web site eligibility survey did not reveal substantial discrepancies. In other words, the number of sites informing users about the use of cookies in the privacy polices was almost equivalent to the number of sites using cookies.

The performance in the coverage of the final principle of Contact Information was similar to the one in the coverage of Cookies. Commercial Web privacy policies in 92% of cases contained information on how to contact the site for any questions or concerns related to informational privacy. The corresponding figures for educational and governmental sites were 68% and 48%, respectively.

Summarizing the performance of each sample across the entire spectrum of FIP principles, one can notice that major weaknesses were similar in all three samples. Thus, commercial privacy policies had the least coverage in the categories of Access, specifically with respect to allowing users to remove some personal information from the site's database (39%) and the principle of Security, specifically in regards with informing users of security measures during transmission of information to the site (47%) (Fig. 38).

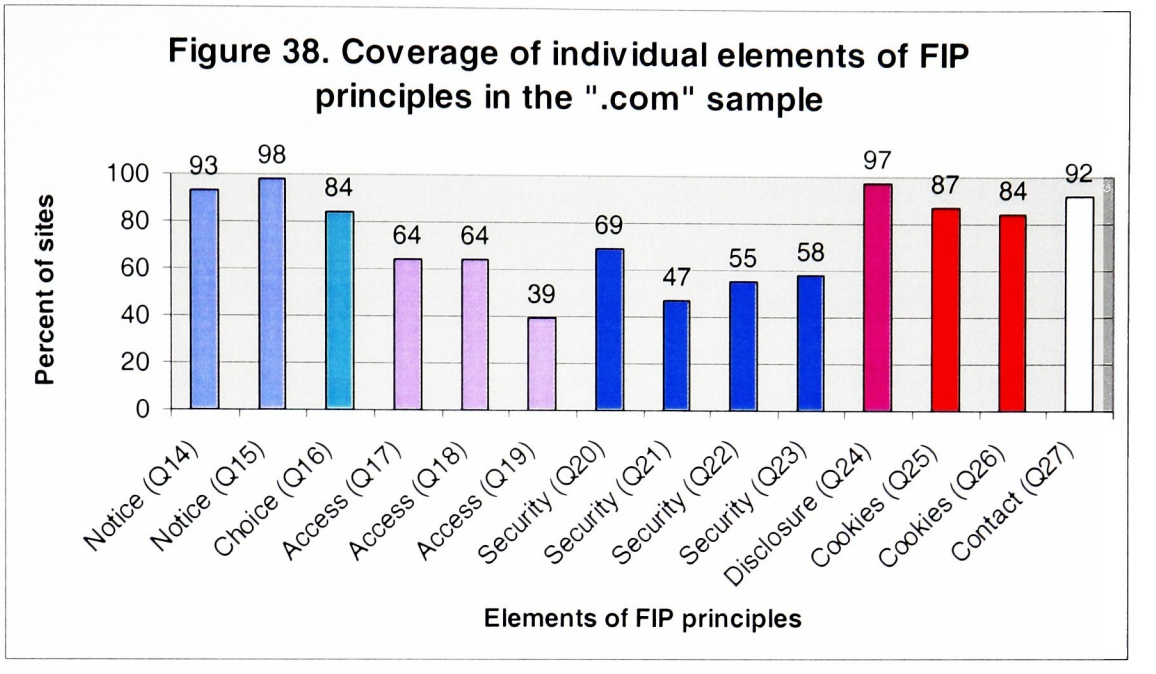

Figure 38. **The number/percentage of sites in the ".com" sample implementing the individual elements[10] of each analyzed FIP principle.**

(Source: Appendix D, Table 11)

Educational sites also had a most noticeable gap in the coverage of Access and Security although the numbers were much lower than the corresponding figures in the ".com" sample. Moreover, the performance was almost equally low for all three elements of Access and three of the four elements of Security (Fig. 39).

[10] The extent of coverage of each individual element of an FIP principle is determined by a separate question in the content analysis form. For example, Question 17 determines whether a site provides a user with an opportunity to review his/her personal information (an element of the principle of Access), and Question 21 checks if a Web site takes certain steps to provide security during transmission of personal information (an element of the Security principle). Consequently, each column in the graph reflects the coverage of one element (or the whole principle if it consists of only one element). The columns of the same color represent the elements of one and the same FIP principle.

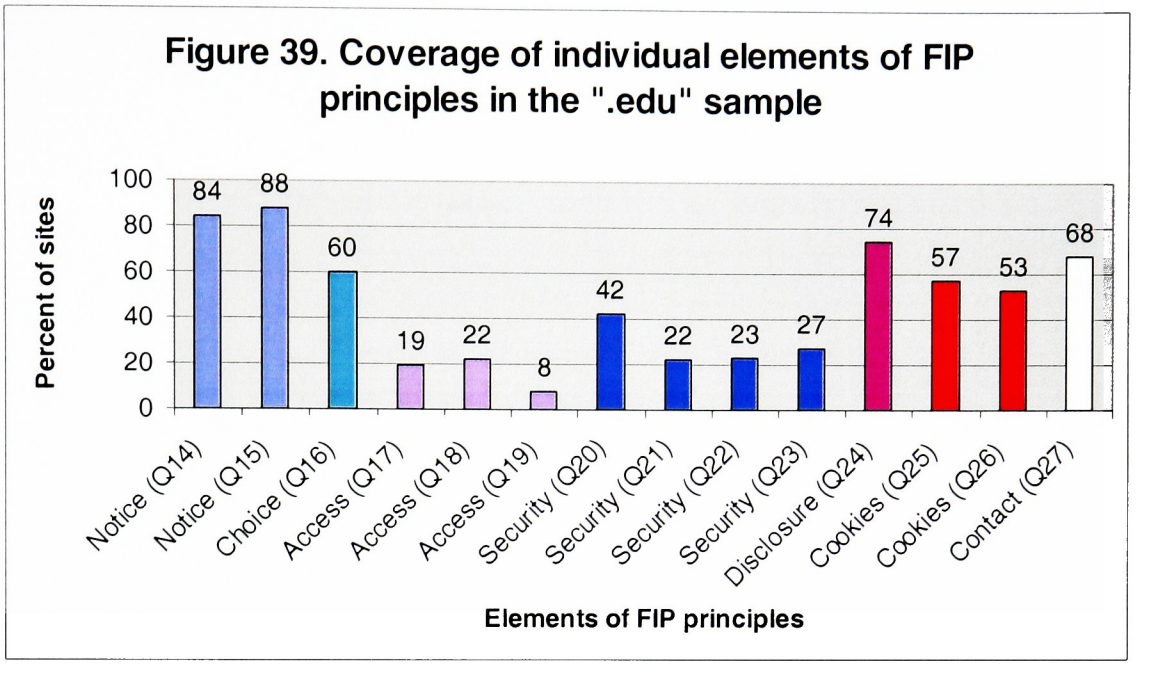

Figure 39. **The number/percentage of sites in the ".edu" sample implementing the individual elements of each analyzed FIP principle.**

(Source: Appendix D, Table 11)

Finally, governmental sites, similar to the two other samples, had a very low coverage for the principles of Access and Security, with the figures being lowest of all the three samples and remaining almost equally low for all individual elements of the mentioned two principles (Fig. 40).

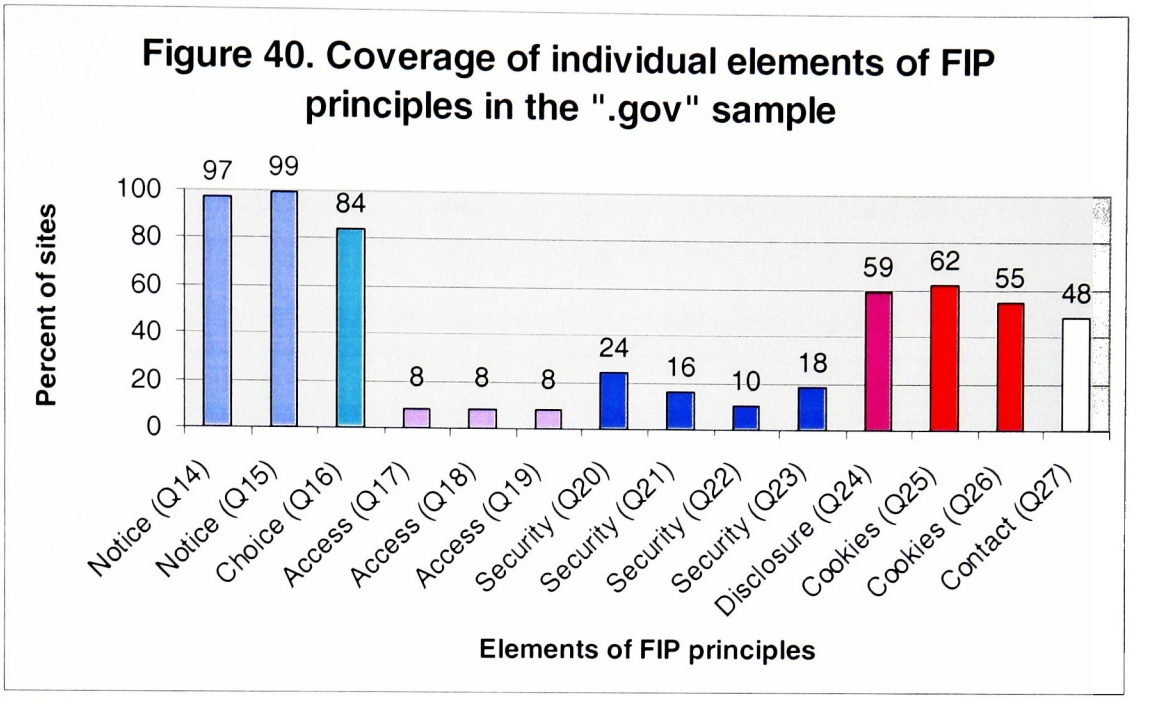

Figure 40. **The number/percentage of sites in the ".gov" sample implementing the individual elements of each analyzed FIP principle.**

(Source: Appendix D, Table 11)

Because of the differences in the coverage of individual FIP principles, all three research samples demonstrated various degrees of coverage for combinations of FIP principles. In general, commercial privacy policies had the widest coverage of most combinations of principles, with educational and governmental sites trailing far behind. However, as the number of constituent elements within each combination decreased, the performance of educational and governmental sites improved. For example, 55% of sites in the ".com" sample provided partial coverage for a combination of all seven FIP principles, whereas the corresponding numbers for educational and governmental sites were 9% and 4%, respectively. As the number of elements within a combination dropped to three major ones – Notice, Choice, and Disclosure to Third Parties – the performance

of educational and governmental sites improved dramatically reaching 48% and 53%, respectively (Fig. 41).

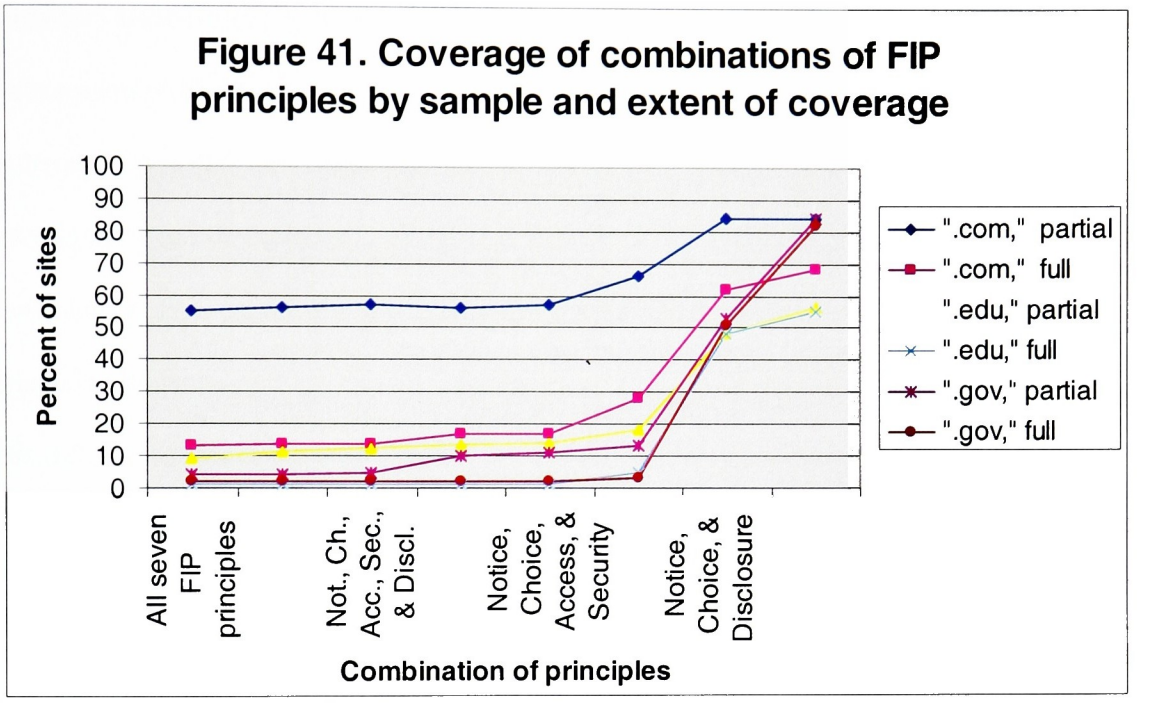

Figure 41. **The number/percentage of sites in the final samples providing full and partial coverage of various combinations of FIP principles.**

(Source: Appendix D, Table 12)

Conclusion

Results

Overall, the research findings suggest a number of differences among the privacy policies of commercial, educational, and governmental Web sites. The differences are in the way the Web site categories communicate the implementation of fair information practice principles in their privacy policy notices posted on the Web. Some of the dissimilarities are substantial, and some can be ignored.

The study suggests that the sharpest dissimilarity exists in the coverage of the principles of Access (allowing a Web user to review and update the data collected about him/her) and Security (protecting a user's personal information during transmission and subsequent storage). For these two principles, commercial privacy policies provide substantially wider coverage than educational and governmental policies. However, the discrepancy in the extent of coverage of the Access and Security principles by commercial sites on the one hand, and educational and governmental sites, on the other, may also be explained by the fact that commercial sites gather more personally identifiable information from users than educational and governmental Web sites.

Furthermore, governmental and educational sites provide a user-friendly option of never putting the user's personal information to a secondary use (Choice) and never sharing collected personal information with third parties unless required by law (Disclosure to Third Parties) much more frequently than commercial sites.

The study also reveals that the commercial privacy policies, in general, have the widest coverage of most combinations of FIP principles among the three samples. However, as the number of constituent elements within each combination decreases down to two or three fundamental principles, the performance of educational and governmental sites improves.

Heuristics

The study produced data on the content of privacy policies of three important categories of Web sites, which may form the basis for recommendations to Internet privacy policy makers involved in designing such privacy disclosures. The findings act as

a signal to Web site owners to pay more attention to a number of specific areas of concern within a privacy disclosure, such as, for example, the coverage of security issues in governmental privacy policies. Most importantly, the research produced data on the privacy policies of educational Web sites, a category that had not been studied before.

The research design incorporates an instrument for the content analysis of Web privacy policies that represents an expansion of the content analytical instrument used by FTC in the previous studies. The updated version used in the present research may be conducive in expanding the methodological potential of the future studies.

Finally, the study findings may help relevant governmental agencies (e.g., FTC) and advocacy groups (e.g., TRUSTe, Online Privacy Alliance) to consider further improvement in education on online privacy issues for Web site owners as well as suggest some methodological changes in evaluation mechanisms of Web site privacy policies, specifically by shifting the focus from purely commercial to educational and governmental Web sites.

Limitations

The study analyzes samples of ".com," ".edu," and ".gov" Web sites that were selected from the totality of matching results retrieved by the Google search engine in response to the "help" search query. Consequently, the study findings cannot be generalized beyond the list of sites retrieved by Google.

The design of the present research benefited greatly from the methods used by previous studies, such as FTC (2000) and Culnan (1999), especially in the sample selection and the questionnaire development. However, the present research methodology

incorporates a number of unique features, and therefore caution should be taken before drawing any comparisons between the findings of the present and the previous studies.

The study measures the coverage of fair information practice principles as provided in the Web privacy policies of analyzed Web sites. By so doing, the study assesses only the extent of disclosure of any given principle in a privacy policy, not the extent of actual implementation of fair information practices by the site. Although privacy policies indeed describe the general intentions of a Web site owner with respect to handling users' personal information, they cannot serve as a testimony to whether the site actually follows its own promises.

Recommendations for future research

This study focuses only on ".com," ".edu" and ".gov" domains. As ".net," ".biz," ".org" and other domain names become more popular, Web sites with these extensions should be included in future research samples. Further studies may also greatly benefit from more representative samples that will allow the generalization of research findings beyond the analyzed samples.

The study findings suggest a number of differences in the coverage of fair information practice principles in the three analyzed samples. Future studies may look for relationships between any given difference (such as, for example, in the coverage of Choice with respect to the secondary use of collected personal information) and another variable (such as, for example, the size of a company / institution or its area of expertise).

Another potential area of research is the comparison of the coverage of FIP principles in privacy policies with the extent of actual implementation of FIP principles

by Web sites. Such comparative study may be designed for each domain in separate (e.g., only ".edu" domain) and several domains together.

Appendices

Appendix A. Web Site Eligibility Check Form

Web Site Eligibility Check Form

Surveyor's name.....

Assigned URL .....

Questions:

Q1 Can you access the Web site?

IF NO, STOP THE SURVEY and WRITE "U" in the box to your right.
THEN GO to the next assigned URL.
IF YES, GO TO Q2

Q2 Does the URL lead to a Web site that has been surveyed under a different web address?

IF YES, STOP THE SURVEY and WRITE "S" in the box to your right.
THEN GO to the next assigned URL.
IF NO, GO TO Q3

Q3 Is the Web site in the English language?

IF YES, SKIP TO Q5 for ".com" sites, TO Q7 for ".edu" sites, or TO Q8 for ".gov" sites.
IF NO, GO TO Q4

Q4 Does the Web site have an English version?

IF NO, STOP THE SURVEY and WRITE "F" in the box to your right
THEN GO to the next assigned URL
IF YES, ENTER the English version and continue the survey only within that version.

Questions 5 and 6 refer ONLY to .com Web sites. If you survey a ".edu" Web site, SKIP to Q7. If you survey a ".gov" Web site, SKIP to Q8

Q5 Does the Web site belong to a business enterprise?

IF NO, STOP THE SURVEY and WRITE "P" in the box to your right.

THEN GO TO the next assigned URL

IF YES, GO TO Q6

Q6 Does the Web site belong to a non-US business?

IF YES, STOP THE SURVEY and WRITE "O" in the box to your right.

THEN GO TO the next assigned URL

IF NO, GO TO Q8

Questions 7 refers ONLY to ".edu" Web sites

Q7 Does the Web site belong to an institute of higher education?

IF NO, STOP THE SURVEY and WRITE "I" in the box to your right.

THEN GO TO the next assigned URL

IF YES, GO TO Q8

Q8 Does the Web site gather any personal information?
Examples:

Name
Email address
Postal address
Telephone number
Fax number
Credit card number
Social Security Number
Age/ Date of Birth
Gender
Education
Occupation

IF NO, WRITE "P" in the box to your right.

THEN SKIP TO the Q12

IF YES, GO TO Q9

Q9 Which of the following types of personally identifiable information does the Web site collect? (Circle all that apply.)

(a) email address
(b) name
(c) postal address
(d) phone number
(e) none of the above

Q10 Does the Web site have a Privacy Policy?

IF NO, WRITE "R" in the box to your right.

THEN SKIP TO Q12

IF YES, GO TO Q11

Q11 Has this Privacy Policy been considered before?

IF YES, WRITE "L" in the box to your right.

THEN GO TO Q12

IF NO, PRINT the entire privacy policy, WRITE the assigned URL on top of the first page, and PLACE the print-out in the folder.
THEN GO TO Q12

Q12 Has the Web site attempted to send a cookie to your hard drive at least once during your visit?

YES NO

STOP THE SURVEY. GO TO the next assigned URL.

Appendix B. Content Analysis Form

Content Analysis Form

Analyst's name.....

Assigned URL.....

Instructions: Circle YES or NO for each question below unless otherwise directed

SECTION 1 - THE CATEGORY OF NOTICE

Q13 Does the Privacy Policy contain at least one complete sentence indicating that the site does NOT collect any electronically collected personal information from its users?

YES NO

If NO, GO to Q14
If YES, STOP THE SURVEY, WRITE "N/A" and GO to the next assigned URL

Q14 Does the Privacy Policy contain at least one complete sentence informing the user of the type(s) of electronically collected personal information the site gathers?

Examples of electronically collected personal information include, but are not limited to, name, postal address, telephone number, email address, social security number, credit card number, financial matters medical or employment history, zip code, age, gender, income level, occupation, education, hobby, password, domain name, Internet Protocol address, and statistical information about which Web pages a user visits.

YES NO

Q15 Does the Privacy Policy contain at least one complete sentence informing the user of the ways the Web site does or may use the collected personal information?

Examples of ways to use collected personal information include, but are not limited to, processing the order, improving the user's experience with the site, targeting specific messages to the user within the site, sending out email communication to the user, sharing the information with partners, engaging the user in various activities on the site.

YES NO

SECTION 2 – THE CATEGORY OF CHOICE

Q16 Which of the following statements is true? (Circle One Letter)

A. The Privacy Policy contains at least one complete sentence informing the user that he/she has an option, via an **opt-out** procedure, of preventing the site from sending the user any communication.
B. The Privacy Policy contains at least one complete sentence informing the user that he/she has an option, via an **opt-in** procedure, of indicating the wish to receive communication from the site.
C. The Privacy Policy contains at least one complete sentence saying that the Web site will ask for a user's consent and/or offer him/her a choice prior to sending him/her any communication but does not make clear if the consent will be acquired via an opt-in or an opt-out procedure.
D. The Privacy Policy contains at least one statement indicating that the user does not have a choice with regard to sending him/her communication from the site.
E. The Privacy Policy contains one or more statements indicating that the site requires a user's consent prior to using AT LEAST SOME of his/her personal information AND one or more statements indicating that the user does not have a choice with regard to the use of AT LEAST SOME of his/her personal information.
F. The Privacy Policy contains at least one complete statement indicating that the site will never use a user's personal information beyond the purpose for which the information was originally provided or if the Privacy Policy contains a statement that the site will use the collected personal information only (a) to improve the site, (b) in aggregate form, (c) to analyze trends and/or (d) as necessary to process the user's request/order.
G. The Privacy Policy does not contain any statement indicating whether a user has any choice with regard to sending him/her communication from the site.

SECTION 3 – THE CATEGORY OF ACCESS

Q17 Does the Privacy Policy contain at least one complete sentence indicating that the user can review the personal information collected by the Web site?

YES NO

Q18 Does the Privacy Policy contain at least one complete sentence indicating that the user can edit the personal information collected by the Web site?

YES NO

Q19 Does the Privacy Policy contain at least one complete sentence indicating that the user can delete at least some of the personal information collected by the Web site?

YES NO

SECTION 4 – THE CATEGORY OF SECURITY

Q20 Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security for the information it collects from users?

IF NO, SKIP to Q19
IF YES, GO to Q24

Q21 Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security during transmission of personal information to the site?

YES NO

Q22 Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security during the storage of personal information collected from users?

YES NO

Q23 Does the Privacy Policy contain at least one complete sentence indicating what specific tools or measures the site uses to protect the user's personal information from being intercepted by unauthorized third parties both during transmission and/or subsequent storage?

Examples of security measures and tools include, but are not limited to, a secure server, SSL (Secure Socket Layer technology), encrypting the messages, using password authentication.

YES NO

SECTION 5 – THE CATEGORY OF DISCLOSURE TO THIRD PARTIES

Q24 Which of the following statements is true? (Circle One Letter)

A. The Privacy Policy contains at least one complete sentence informing the user that he/she has an option, via an **opt-out** procedure, of preventing the site from sharing the user's personal information with third parties.
B. The Privacy Policy contains at least one complete sentence informing the user that he/she has an option, via an **opt-in** procedure, of indicating the wish to share the user's personal information with third parties.
C. The Privacy Policy contains at least one complete sentence saying that the Web site will ask for a user's consent and/or offer him/her a choice prior to sharing

his/her personal information with third parties, but does not make clear if the consent will be acquired via an opt-in or an opt-out procedure.

D. The Privacy Policy contains at least one complete statement indicating that the user does not have a choice with regard to sharing his/her personal information with third parties.
E. The Privacy Policy contains one or more statements indicating that the site requires a user's consent prior to sharing AT LEAST SOME of his/her personal information with a third party AND one or more statements indicating that the user does not have a choice with regard to the sharing of AT LEAST SOME of his/her personal information with third parties.
F. The Privacy Policy contains one or more statements indicating that the site will never share personal information with third parties, or if the Policy contains a statement that the site will share personal information only (a) if required to do so by law, (b) in aggregate form, (c) as necessary to process the user's order, (d) to protect the security of other users, (e) to protect the integrity of the site, and (f) if the user's actions are in violation of the Web site's terms of use.
G. The Privacy Policy does not contain any sentence offering users a choice and/or requiring their consent with regard to sharing their personal information with third parties.

SECTION 6 – THE CATEGORY OF USE OF COOKIES

Q25 Does the Privacy Policy contain at least one complete sentence saying anything about whether the site does or may use cookies?

YES NO

IF NO, SKIP to Q27
IF YES, GO to Q26

Q26 Does the Privacy Policy contain at least one complete sentence indicating what a cookie is and/or explaining the purpose of its use?

YES NO

SECTION 7 – THE CATEGORY OF CONTACT INFORMATION

Q27 Does the Privacy Policy contain at least one complete sentence explaining how the user can contact the Web site if he/she has questions related to the site's privacy practices?

YES NO

Appendix C. Instructions for Surveyors and Analysts

Instructions for Surveyors and Analysts

PART 1. IMPORTANT TERMS

Privacy Policy is an electronic document, located on a Web site and accessible through a hyperlink, that explains the Web site owner's practices of collecting data about Web users and using this information.

Personal information is information about a natural person that includes, but is not limited to, his/her name, social security number, postal address, telephone number, education, financial matters, medical or employment history, electronic mail address, gender, age, and date of birth.

Electronically collected personal information means any information about an individual user that is collected by electronic means and maintained by an institution, including, but not limited to, his/her name, social security number, home address, telephone number, education, financial matters, medical or employment history, electronic mail address, gender, age, date of birth, AND **information that reveals any network location, hardware/software properties, and Web browsing patterns** such as user's Internet Service Provider (ISP), Internet Protocol (IP) address, Web browser version, and statistical information about which Web pages the user visits.

Personal information (electronically or otherwise collected) can be subdivided into two large categories: personally identifiable information and personally non-identifiable information. **Personally identifiable information** is information that can be used to identify a person. Such information includes, but is not limited to, name, postal address, telephone number, fax number, email address, credit card number, and social security number, and IP address. **Personally non-identifiable information** is information that, if taken alone, cannot be used to identify a person. Personally non-identifiable information includes, but is not limited to, age, date of birth, gender, education, occupation, hobby, Zip code, Web browser version, and browsing patterns.

Within the current survey "personal information" refers to both personally identifiable AND personally non-identifiable information. In other words, if you are asked, for example, to find out if the Web site gathers personal information, the answer will be YES if the site collects at least one type of EITHER personally identifiable AND/OR personally non-identifiable information. Questions asking about the collection of personal information do not include the cases of gathering electronically collected personal information unless otherwise noted.

Gathering/collecting personal information stands for the process of collecting personally identifiable and/or personally non-identifiable information from users via some mechanisms, either with or without the user's knowledge.

Opt-in procedure stands for an affirmative act by the user, such as checking a click-box or sending an email, before the information can be used in a particular manner. In other words, unless the user provides his/her consent, the personal information will not be used by the site.

Opt-out procedure stands for an action by the user, such as checking a click-box or sending an email, to prevent the site from using the personal information about him/her. In other words, unless the user requests the information not to be used, the information may or will be used by the site.

Third party stands for any company/organization other than the owner of the assigned Web site.

PART 2. WEB SITE ELIGIBILITY CHECK

Search a Web site for no more than 20 minutes to determine its eligibility for the content analysis. Be sure to surf through the whole site while looking for answers to the questions stated. However, since many Web sites contain links leading off the site, pay attention not to leave the pages of the assigned URL as you move from page to page using hyperlinks. If in doubt, check the Web address reflected in the Internet Explorer's address bar to make sure it belongs to the same domain as the assigned URL.

Your computer privacy preferences have been modified to prompt you every time a Web site attempts to install a cookie on your hard drive. If during your visit to a site, a message pops up asking you to accept or block a cookie, ACCEPT it. Make a note of it (or simply keep it in mind) since, at the end of the Web Site Eligibility Check form, you will be asked if the site has tried to send a cookie to your machine.

Start with the first Web site on your list, write the URL in the assigned blank space on the Web Site Eligibility Check Form. Be sure to include your name in the specified area on the Form.

Q1 Can you access the Web site?

The Web site is considered inaccessible if the page retrieved immediately after typing in the assigned URL contains one of the following messages:

Under construction
No DNS entry
Unavailable

Inactive
Server is down

OR

any other message which, based on your judgment, shows that one cannot access the site.

Note: If after typing in an assigned URL, you are automatically redirected to another URL, consider it to be the same domain as you have been assigned. Simply write the new URL below the original entry in the Web Site Eligibility Check Form and continue with your assessment.

Q2 Does the URL lead to a Web site that has been considered under a different Web address?

Some companies/organizations register several domain names for their Web site. Whenever a user enters one of the registered URLs in his/her browser window, he/she is automatically re-directed to the main location where the Web site resides. For example, if you type www.windows.com in your browser's window, you will be redirected to www.microsoft.com domain. This means that Microsoft registered both URLs and they lead to one and the same site.

Answer YES to the question only if during your survey you come across a URL that leads to the Web site you have previously considered under a different domain name, e.g. if you type in www.uic.edu and it leads you to www.uillinois.edu – a URL you have already analyzed.

Q3 Is the Web site in the English language?

English is considered the main language of the site if it is used for the written content of the first page retrieved after typing in the assigned URL.

Q4 Does the Web site have an English version?

The site is considered to have an English version if the latter can be accessed via a hyperlink placed on the home page and represents a full or partial mirror of the main language version.

Q5 Does the Web site belong to a business enterprise?

Not all the .com Web sites are commercial in nature. Some of them belong to individuals who use them as their personal home pages. Others also belong to non-commerce, non-profit institutions.

A Web site is considered to belong to a business enterprise if the site contains some information clearly indicating that the owner is a firm, a company, a corporation, or any other entity that produces and sells its end products or services to consumers.

Moreover, a site does not have to be the company's main page on the Web: It may be exclusively devoted to one of its products. For example, www.real.com belongs to Real Networks, Inc. and is entirely devoted to one of the company's products – RealOne player.
A site is also considered to belong to a business enterprise if it offers completely free services to its end users but gains profit by placing advertising on its pages.

A personal site is, as a rule, not considered commercial if the owner uses the site merely to promote his/her ideas, products, or services. However, a personal site is considered to be a business enterprise if it incorporates a platform to complete financial transactions between the site's owner and buyers via the Internet.

The following sections of the site may contain information that will help identify whether the site belongs to a commercial entity:

About Us / About this site
Advertising / Advertise with us
Contact Information / Contact Us
Company Profile
Help
Legal Notice
Terms of Service/ Terms of Use

Any site that does not belong to a commercial entity, does not gain profit from advertising, and does not sell any product or service cannot be considered, for the purposes of the present study, as belonging to a business enterprise.

If the site does not contain any specific information revealing whether it is owned by a business enterprise, it must NOT be included in the final sample.

Q6 Does the Web site belong to a non-US business?

Search the site for any piece of written information that identifies the company's country of origin and/or operation. The following sections of the site may contain information that will help identify the country of origin and/or operation:

About Us / About this site
Advertising / Advertise with us
Contact Information / Contact Us
Company Profile

Help
Legal Notice
Terms of Service/ Terms of Use

Additionally, look for any place on the main pages of the site for a telephone number and a postal address as these can easily reveal if the company operates in the USA.

If you are unable to identify the country of origin/operation, the site is considered to belong to an American business.

Q7 Does the Web site belong to an institute of higher education?

Not all the ".edu" Web sites belong to schools of higher education. Some of them belong to state organizations involved in educational matters. Others belong to scientific research institutes, medical centers, or professional college associations.

A Web site is considered to belong to an institute of higher education if the site contains some information clearly indicating that the owner is a university, a college, an institute or another entity whose main area of service is the provision of academic programs to students who study to receive undergraduate, graduate, post-graduate or another degree that is higher than a certificate for completing a high school.

The following sections of the site may contain information that will help identify whether the site belongs to an institute of higher education:

About Us / About this site
Contact Information / Contact Us
Help
Legal Notice
Terms of Service/ Terms of Use

If the site does not contain any specific information revealing whether it is owned by an institute of higher education, it must NOT be included in the final sample.

Q8 Does the Web site gather any personal information?

As mentioned above, the term "gathering personal information" stands for the process of collecting personally identifiable and/or personally non-identifiable information from users via some mechanisms, either with or without the user's knowledge. For the definitions of personally identifiable and personally non-identifiable information please review Part 1 of this document.

In order to identify if the site gathers personal information try to view as many pages as possible. Make sure you first visit the pages where collection of information is most

likely to take place. Below is a list of expressions that will prompt you in the right direction while searching for the answer to the question.

Login (here)
Registration
FAQs
Membership
My/Your Account
Order (here)
Feedback
Subscribe (here)
Survey
Guest book
Tell/Email to a friend

As soon as you find a proof of the fact that the site gathers at least ONE type of personal information, answer YES to the question and continue according to further instructions.

If you cannot find a single fact indicating that the site collects some personal information, answer NO and continue according to further instructions.

Q9 Which of the following types of personally identifiable information does the Web site collect?

Spend some time browsing the site's pages in order to find out if the site collects one or more of the four types of personally identifiable information, and namely, email, name, postal address, and phone number.

Make sure you visit the pages where collection of information is most likely to take place. Below is a list of expressions that will prompt you in the right direction while searching for the answer to the question.

Login (here)
Registration
FAQs
Membership
My/Your Account
Order (here)
Feedback
Subscribe (here)
Survey
Guest book
Tell/Email to a friend

Note. The collection of email addresses also includes the cases of provision of an active hyperlink with an email address to the site's webmaster or any other contact person (e.g. *If you have any questions about the site, contact the webmaster at* webmaster@ohsu.edu)

Q10 Does the Web site have a Privacy Policy?

In order to identify if the site has a Privacy Policy (see Part 1 for definition) try to view as many pages as possible. Most often the link to Privacy Policy is at the home page. However, some sites may place the document elsewhere. Furthermore, the Web site may present its Privacy Policy under a different title such as Privacy, Privacy Statement, Legal Notice, Legal Page, Disclaimer, Terms of Use, Terms of Service, Policy/Policies and Help. Please check as many potential hyperlinks as possible prior to arriving at a final conclusion about the presence of a Privacy Policy on the site.

Note 1. Quite often on educational Web sites, one can meet a privacy policy notice (or notices) that is related to the policy of a given school with respect to the sharing of personal information collected from the students off-line and/or discussing the acceptable use of computing resources on campus. These notices appear on educational Web sites under different names including Acceptable/ Appropriate Use Policy, Proper Use of Information Resources, Information Technology Policies, and University Policy Statement.

Such a notice does NOT CONSTITUTE a privacy policy as defined for the present study unless it discusses the practices of collection of personal information via the school's Web site and use of this information by the school.

Note 2. Some governmental Web sites, especially those belonging to a state government, have two privacy policy notices, one describing the state's privacy-related regulations and the other speaking about the site's privacy practices. The state's regulations usually appear under the heading "Privacy Policy", and the site's practices, under "Conditions of Use" or other. If you encounter such a site, analyze ONLY the site's privacy practices (i.e. Conditions of Use).

Q11 Has this Privacy Policy been considered before?

Certain commercial and governmental entities have a corporate structure where one institution (a parent company or a governmental department) plays the leading role in determining policy decisions for its branches/divisions. Quite often the branches of a big parent institution have their own Web presences with content different from the Web site of the leader. However, when it comes to policies and strategies, the Web site of a subordinate entity simply provides a link to the parent institution's Web site.

If clicking on a Web site's hyperlink to Privacy Policy leads you to a parent company's Web site, which you have considered before, DO NOT analyze the same privacy policy again. **Answer YES** to the survey question and follow further instructions.

If, however, the hyperlink leads you to a different Web site's Privacy Policy but you have not analyzed that policy before, **Answer NO** to the survey question and follow further instructions.

Q12 Has the Web site attempted to send a cookie to your hard drive at least once during your visit?

Your computer privacy preferences have been modified to prompt you every time a Web site attempts to install a cookie on your hard drive.

If during the entire visit to a site you have received at least one pop-up message asking you to accept or block a cookie, **Answer YES** to the survey question and follow further instructions.

If during the entire visit to a site you have not received any message asking you to accept or block a cookie, **Answer NO** to the survey question and follow further instructions.

PART 3. CONTENT ANALYSIS

In completing the content analysis you should base your answers on the printed version of the Web site's Privacy Policy available in your folder, NOT the electronic version accessible via the Internet.

You should start answering the questions in the Content Analysis Form after at least one careful reading of the entire document. Furthermore, each question requires reading the Policy and searching for clues to an answer. Do NOT ASSUME anything. Answer the question ONLY on the basis of the factual data available in the document unless otherwise instructed. Use your judgment and common sense while encountering situations not described in the Instructions.

Q13 Does the Privacy Policy contain at least one complete sentence indicating that the site does NOT collect any electronically collected personal information from its users?

Answer YES to the question only if you find a clear statement that the site does not gather ANY information from its users.

Example: We do not collect any information about you when you visit our site.

Note. Before answering YES to the question, read the entire Privacy Policy and make sure that the document does not contain any statement indicating that the site gathers at

least some kind of electronically collected personal information. Consider the following example: *We do not collect any information about our users... Send us an email if you have any questions about the site.* Although the Policy contains an explicit statement claiming the site does not gather any information, the same document also incorporates a sentence offering users to contact the site for further questions, and thus provide the site with the user's email address.

Answer NO to the question if you do not find a clear statement that the site does not gather any information, or if you find any statement indicating that the site collects at least one type of electronically collected personal information.

Example: We collect only your email address which is used to send you important messages about our service.

We don't collect any data about you except the information you knowingly provide to us.

Q14 Does the Privacy Policy contain at least one complete sentence informing the user of the type(s) of electronically collected personal information the site gathers?

Answer YES to the question if you find at least one statement indicating a type/types of personal information the site collects from its users.

Example: We collect you name and email address when you register for this site.

We may require your credit card information to prove your age.

Answer NO to the question if you do not find a statement indicating at least one type of personal information the site does or may gather from its users.

Q15 Does the Privacy Policy contain at least one complete sentence informing the user of the ways the website does or may use the collected personal information?

Answer YES to the question if the Privacy Policy contains a statement indicating at least one way the site uses the information collected from its users. Such a statement may describe how the information will be used by the site, or how the information will not be used by the site.

Example: We use the information collected from you to provide you better experience on our site.

We only use your information to process your order.

We may use your email to send you occasional messages from our site.

We will not share your personal information with third parties without your express consent.

Answer NO to the question if you do not find a statement indicating at least one way the personal information about users may be or is used by the site.

Q16 This item requires you to identify if the Web site provides users a choice on the use of the personal information collected by the site.

Circle A if the Privacy Policy contains at least one statement indicating that the site does or may use the personal information provided by the user (beyond the use for which the information was originally provided) unless the user instructs the site not to do so, e.g. by sending an email or clicking a check-box. (Consult Part 1 of these Instructions for the definition of Opt-out Procedure)

Circle B if the Privacy Policy contains at least one statement indicating that the site will not use the personal information provided by the user (beyond the use for which the information was originally provided) unless the user provides his/her express consent, e.g. by sending an email or checking a click-box. (Consult Part 1 of these Instructions for the definition of Opt-in Procedure)

Keep in mind that "B" is the right answer only if there is no other statement in the entire Privacy Policy indicating that the site may or does use AT LEAST SOME of the user's personal information without his/her prior consent.

Circle C if the Privacy Policy contains at least one statement indicating that the site requires the user's consent prior to using his/her personal information (beyond the use for which the information was originally provided) but does not specify if such a consent is acquired via an opt-in or opt-out procedure.

Keep in mind that "C" is the right answer only if there is no other statement in the entire Privacy Policy indicating that the site will seek a user's consent via an opt-in or opt-out procedure prior to using AT LEAST SOME of his/her personal information.

Circle D if the Privacy Policy contains a statement indicating that the user does not have a choice with regard to sending him/her communication from the site.

Example: We will use your email to send you occasional communication about our products and services.

Keep in mind that "D" is the correct answer only if there is no other statement in the entire Privacy Policy indicating that a user may opt-out from receiving communication from the site or put a stop to the use of his/her personal information.

Circle E if the Privacy Policy contains one or more statements indicating that the site requires a user's consent (via an opt-in/ opt-out procedure) prior to using AT LEAST SOME of his/her personal information AND one or more statements indicating that the user does not have a choice with regard to the use of AT LEAST SOME of his/her personal information.

Circle F if the Privacy Policy contains at least one statement indicating that the site will never use a user's personal information beyond the purpose for which the information was originally provided or if you find a statement that the site will use the collected personal information only (a) to improve the site, (b) in aggregate form, (c) to analyze trends and/or (d) as necessary to process the user's request/order.

Circle G if the Privacy Policy does not contain any statement indicating whether a user has any choice with regard to sending him/her communication from the site.

Q17 Does the Privacy Policy contain at least one complete sentence indicating that the user can review the personal information collected by the Web site?

Answer YES if you find a statement indicating that the site allows the user to review at least some of the collected personal information.

Example: Click on "My Account" to review your information.

Answer NO if you cannot find any statement indicating whether the site allows the user to review at least some of the collected personal information.

Q18 Does the Privacy Policy contain at least one complete sentence indicating that the user can edit the personal information collected by the Web site?

Answer YES if you find a statement indicating that the site allows the user to edit at least some of the collected personal information.

Example: You can edit your personal information by clicking on My Account on the Home page.

Please send us email to update the information on your personal account.

Answer NO if you cannot find any statement indicating whether the site allows the user to edit at least some of the collected personal information.

Q19 Does the Privacy Policy contain at least one complete sentence indicating that the user can delete at least some of the personal information collected by the Web site?

Answer YES if you find a statement indicating that the site allows the user to delete at least some of the collected personal information.

Example: Please send us an email if you want your account to be removed from our Web site.

You can delete any information you deem unnecessary by logging in Your Account on the Home page

Answer NO if you cannot find any statement indicating whether the site allows the user to delete at least some of the collected personal information.

Q20 Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security for the information it collects from users?

Answer YES if you find any statement indicating that the site takes steps to ensure security of the personal information irrespective of whether the statement concerns the security of data transmission, the security of data storage, or security in general.

Examples: We take steps to ensure the security of your personal information

We use secure servers to process your order.

This is a secure site.

We use encryption to protect your personal information from being intercepted by unauthorized parties.

We store your information on a secure server.

Answer NO if you cannot find any statement indicating whether the site takes any steps to ensure the security of the collected personal information, or if you find a statement saying that the site does not take any steps to provide security.

Q21 Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security during transmission of personal information to the site?

Answer YES if you find any statement indicating that the site takes steps to ensure security of the personal information during data transmission from the user to the Web site.

Answer NO if you cannot find any statement indicating whether the site takes any steps to ensure the security of the personal information during data transmission, or if you find a statement saying that the site does not take any steps to provide security during data transmission.

Q22 Does the Privacy Policy contain at least one complete sentence indicating that the Web site takes certain steps to provide security during the storage of personal information collected from users?

Answer YES if you find any statement indicating that the site takes steps to ensure security of the personal information during its during its storage.

Answer NO if you cannot find any statement indicating whether the site takes any steps to ensure the security of the personal information during its storage, or if you find a statement saying that the site does not take any steps to provide security during storage of personal information.

Q23 Does the Privacy Policy contain at least one complete sentence indicating what specific tools or measures the site uses to protect the user's personal information from being intercepted by unauthorized third parties?

Answer YES if you find any statement specifying what tools/mechanisms/software applications the site utilizes to ensure security of the personal information irrespective of whether the statement concerns the security of data transmission, the security of data storage, or security in general.

Examples: We use SSL (Secure Socket Layer) to protect your information.

We encrypt the messages from you to protect it from interception by unauthorized third parties.

Answer NO if you cannot find any statement specifying what tools/mechanisms/software applications the site utilizes to ensure security of the personal information.

Q24 This question requires you to identify if the Web site provides users a choice on the disclosure of the personal information collected by the site to third parties.

Circle A if you find at least one statement informing the user that the site does or may disclose the personal information provided by the user to third parties unless the user instructs the site not to do so, e.g. by sending an email or clicking a check-box. (Consult Part 1 of these Instructions for the definition of Opt-out Procedure)

Examples: Click here if you don't want your email address to be shared with our partners.

Please send us an email if you do not wish to receive promotional offers from our partners.

Circle B if you find at least one statement indicating that the site will not disclose the personal information provided by the user to third parties unless the user provides his/her express consent, e.g. by sending an email or checking a click-box. (Consult Part 1 of these Instructions for the definition of Opt-in Procedure)

Examples: We will not share your personal information with third parties unless you express your consent in your email.

You should click here if you want to receive email offers from our business partners.

Keep in mind that "B" is the right answer only if there is no other statement in the entire Privacy Policy indicating that the site may or does disclose AT LEAST SOME of the user's personal information to third parties without his/her prior consent.

Circle C if you find at least one statement indicating that the site requires the user's consent or offer him/her a choice prior to sharing his/her personal information with third parties, but does not specify if such a consent is acquired via an opt-in or opt-out procedure.

Examples: We will not share your personal information with third parties without your express consent.

We will disclose information about you to our trusted partners only after obtaining your express permission.

Keep in mind that "C" is the right answer only if there is no other statement in the entire Privacy Policy indicating that the site will seek a user's consent via an opt-in or opt-out procedure prior to sharing AT LEAST SOME of his/her personal information with third parties.

Circle D if the Privacy Policy contains a statement indicating that the user does not have a choice with regard to sharing his/her personal information with third parties.

Example: We may share your email with our trusted partners so that they could send you occasional communication about their products and services.

Keep in mind that "D" is the correct answer only if there is no other statement in the entire Privacy Policy indicating that a user may opt-out from receiving third-party communication or put a stop to the use of his/her personal information by a third party.

Circle E if the Privacy Policy contains one or more statements indicating that the site requires a user's consent (via an opt-in/ opt-out procedure) prior to sharing AT LEAST SOME of his/her personal information with a third party AND one or more statements indicating that the user does not have a choice with regard to the sharing of AT LEAST SOME of his/her personal information with third parties.

Note. Sharing personal information with third parties does not include, within this answer option, cases of sharing information in aggregate form, as required by law, and as necessary to fulfill the user's order/request.

Circle F if you find at least one statement saying that the site will never share personal information with third parties, or if you find a statement that the site will share personal information only (a) if required to do so by law, (b) in aggregate form, (c) as necessary to process the user's order[11], (d) to protect the security of other users, (e) to protect the integrity of the site, and (f) if the user's actions are in violation of the Web site's terms of use.

Examples: We will not sell or disclose your personal information to third parties.

We may share personal information about our users with advertisers but only in aggregate form.

We will never disclose your information to anyone unless required by law.

Circle G if the Privacy Policy does not contain any sentence offering users a choice and/or requiring their consent with regard to sharing their personal information with third parties.

Q25 Does the Privacy Policy contain at least one complete sentence saying anything about whether the site does or may use cookies?

Answer YES if you can find at least one statement indicating that the site does or may use cookies, or if you find a statement indicating that the site does not use cookies.

Examples: We may use cookies to collect information about your preferences.

---

[11] This includes the sharing of personal information with the companies that are employed by the Web site to perform functions on its behalf, such as shipping companies, Web hosting companies, marketing consultants, and credit card payment processors. These companies may have access to users' personally identifiable information to perform their functions but they may not use the provided information for any other purpose.

We do not use cookies.

Answer NO if you cannot find any statement saying anything about whether the site uses cookies.

Q26 Does the Privacy Policy contain at least one complete sentence indicating what a cookie is and/or explaining the purpose of its use?

Answer YES if you find at least one statement providing explanation to users as to what a cookie is and/or for what purpose the site uses cookies.

Examples: Cookies are pieces of information that a Web site transfers to a user's hard drive for record-keeping purposes so that we may track site and user activity.

We use cookies to collect information about your site use preferences.

Answer NO if you cannot find any statement explaining what a cookie is and /or for what purpose the site uses cookies.

Q27 Does the Privacy Policy contain at least one complete sentence explaining how the user can contact the Web site if he/she has questions related to the site's privacy practices?

Answer YES if you find a statement containing information that a user may utilize to contact the site with questions about the site's privacy.

Examples: Email us if you have any questions about this privacy policy.

Use the contact information below to contact us for any further questions.

Answer NO if you cannot find at least one statement in the Privacy Policy indicating how a user can contact the site if he/she has question/concerns about the site's privacy practices.

Appendix D. Data Tables

TABLE 1

Results of Web site eligibility check for the ".com," ".edu" and ".gov" sampling pools[12]

	".com"		".edu"		".gov"	
	number	percent	number	percent	number	percent
Inaccessible	3	2%	2	1%	4	3%
Same site	0	0	3	1%	0	0
No English version	1	1%	0	0	0	0
Not a business site	21	13%	N/A	N/A	N/A	N/A
Not a US business	9	6%	N/A	N/A	N/A	N/A
Not a college site	N/A	N/A	14	5%	N/A	N/A
No personal information collected	2	1%	5	2%	0	0
No privacy policy	15	9%	174	57%	5	4%
Same privacy policy	12	7%	0	0	21	16%
Unique privacy policy	100	61%	100	34%	100	77%

[12] Only mutually exclusive results of the eligibility check are presented. Consequently, the total number of results for each sampling pool equals the number of Web sites in that pool (163 for the ".com" sampling pool, 298 for the ".edu" pool, and 130 for the ".gov" sampling pool)

TABLE 2

Of the pre-qualifying sites[13] in each sampling pool, the number of sites collecting personal information and the number of sites posting privacy policies

	".com"		".edu"		".gov"	
	number	percent	number	percent	number	percent
Pre-qualifying sites	129	100%	279	100%	126	100%
Sites collecting personal information	127	98%	274	98%	126	100%
Sites posting privacy policy	112	87%	100	36%	121	96%
Sites posting unique privacy policies	100	75%	100	36%	100	79%

[13] Pre-qualifying sites in the ".com" sample are the unique Web sites that belong to U.S. businesses. Pre-qualifying sites in the ".edu" sample are the unique Web sites belonging to U.S. institutions of higher education. Pre-qualifying in the ".gov" sample are the unique Web sites belonging to U.S. governmental agencies.

TABLE 3

Of the pre-qualifying sites in each sampling pool, the number of sites collecting email address, name, postal address, phone number and using cookies

	".com"		".edu"		".gov"	
	number	percent	number	percent	number	percent
Email address	126	98%	274	98%	130	100%
Name	110	85%	137	49%	57	45%
Postal address	83	64%	81	29%	47	37%
Phone number	68	53%	67	24%	30	24%
Using cookies	108	84%	148	53%	78	60%

TABLE 4

The number/percentage[14] of sites in the final samples providing individual elements,[15] and partial, full or no coverage of the principle of Notice in their privacy policies

	".com"	".edu"	".gov"
Informing users of types of collected information	93	84	97
Informing users of uses of collected information	98	88	99
Partial coverage[16] of Notice	99	90	99
Full coverage[17] of Notice	92	82	97
No coverage of Notice	1	10	1

[14] From hereon, all the numbers in the tables, unless otherwise noted, represent both an actual number of sites and a percentage since the final samples consist of 100 Web sites

[15] The principle of Notice is made up of two individual elements: (1) informing the user of the type(s) of electronically collected personal information the site gathers, and (2) informing the user of the uses the electronically collected personal information can be put to.

[16] From hereon, partial coverage, unless otherwise noted, refers to the coverage of at least one individual element of a given FIP principle

[17] From hereon, full coverage, unless otherwise noted, refers to the coverage of all individual elements of a given FIP principle

TABLE 5a

The number/percentage of sites in the final samples providing various options of Choice in their privacy policies

	".com"	".edu"	".gov"
(A) opt-out[18]	58	16	6
(B) opt-in[19]	4	0	2
(C) consent (opt-in/opt-out)[20]	5	2	0
(D) no consent[21]	7	9	10
(E) some with & some without consent[22]	12	0	1
(F) never use[23]	5	42	75
(G) no mention[24]	9	31	6

[18] "Opt-out" means that, unless the user requests the collected personal information not to be used, the information may or will be used by the site

[19] "Opt-in" means that, unless the user provides his/her consent, the personal information will not be used by the site

[20] The site requires the user's consent prior to using his/her personal information but it is not clear if such a consent is acquired via an opt-in or opt-out procedure

[21] Personal information may be used by the site without the user's consent

[22] While the site requires consent for the secondary use of some personal information, it may still use some other personal information without the user's consent

[23] The site will never use the user's personal information other than (a) to improve the site, (b) in aggregate form, (c) to analyze trends and/or (d) as necessary to process the user's request/order

[24] The privacy policy does not say anything about the user's choice with respect to the secondary use of his/her personal information by the site

TABLE 5b

The number/percentage of sites in the final samples providing partial, full or no coverage of the Choice principle in their privacy policies

	".com"	".edu"	".gov"
Partial coverage of Choice[25]	84	60	84
Full coverage of Choice[26]	72	60	83
Do not provide Choice[27]	16	40	16

[25] Partial coverage of Choice is implemented if the privacy policy states that the site will seek the user's consent prior to the secondary use of *at least some* personally identifiable information collected by the site
[26] Full coverage of Choice is implemented if the privacy policy states that the site will seek the user's consent prior to the secondary use of *any* personally identifiable information collected by the site
[27] This includes the sites mentioning that the user's personal information may be used with his/her consent and the sites that do not mention if the user has any choice wit respect to the secondary use of his/her personal information

TABLE 6

The number/percentage of sites in the final samples providing individual elements[28], and partial, full or no coverage of the principle of Access in their privacy policies

	".com"	".edu"	".gov"
Allowing the user to review information	64	19	8
Allowing the user to edit information	64	22	8
Allowing the user to review and edit information	63	18	7
Allowing the user to delete information	39	8	8
Partial coverage of Access	68	24	13
Full coverage of Access	36	5	3
No coverage of Access	32	76	87

[28] The principle of Access is made up of three individual elements: (1) allowing the user to review at least some of his/her personal information collected by the site, (2) allowing the user to edit at least some of his/her personal information, and (3) allowing the user to delete at least some of his/her personal information collected by the site.

TABLE 7

The number/percentage of sites in the final samples providing individual elements,[29] and partial, full or no coverage of the principle of Security in their privacy policies

	".com"	".edu"	".gov"
Security for collected personal information	69	42	24
Security during transmission	47	22	16
Security during storage	55	23	10
Security during transmission and storage	40	13	9
Specific security mechanisms	58	27	18
Partial coverage of Security	69	42	24
Full coverage of Security	39	12	8
No coverage of Security	31	58	76

[29] The principle of Security is made up of four individual elements: (1) providing general security for the user's personal information, (2) providing security during transmission of information to the site, (3) providing security during storage of information by the site, and (4) informing the user of the specific security mechanisms employed to protect the collected personal information.

TABLE 8a

The number/percentage of sites in the final samples providing various options of Disclosure to Third Parties in their privacy policies

	".com"	".edu"	".gov"
(A) opt-out[30]	34	2	1
(B) opt-in[31]	2	3	0
(C) consent (opt-in/opt-out)[32]	23	16	6
(D) no consent[33]	2	8	33
(E) some with & some without consent[34]	10	0	2
(F) never use[35]	28	53	50
(G) no mention[36]	1	18	8

[30] "Opt-out" means that, unless the user requests the collected personal information not to be shared, the information may or will be shared with third parties

[31] "Opt-in" means that, unless the user provides his/her consent, the personal information will not be shared with third parties

[32] The site requires the user's consent prior to sharing his/her personal information but it is not clear if such a consent is acquired via an opt-in or opt-out procedure

[33] Personal information may be shared with third parties without the user's consent

[34] While the site requires consent for the sharing of some personal information with third parties, it may still share some other personal information without the user's consent

[35] The site will never share the user's personal information wit third parties other than (a) if required to do so by law, (b) in aggregate form, (c) as necessary to process the user's order[35], (d) to protect the security of other users, (e) to protect the integrity of the site, and (f) if the user's actions are in violation of the Web site's terms of use

[36] The privacy policy does not say anything about the user's choice with respect to the sharing of his/her personal information with third parties

TABLE 8b

The number/percentage of sites in the final samples providing partial, full or no coverage of the Disclosure to Third Parties principle in their privacy policies

	".com"	".edu"	".gov"
Partial coverage of Disclosure to Third Parties[37]	97	74	59
Full coverage of Disclosure to Third Parties [38]	87	74	57
No coverage of Disclosure to Third Parties [39]	3	26	41

[37] Partial coverage of Disclosure to Third Parties is implemented if the privacy policy states that the site will seek the user's consent prior to disclosure of *at least some* personally identifiable information collected by the site

[38] Full coverage of Disclosure to Third Parties is implemented if the privacy policy states that the site will seek the user's consent prior to disclosure of *any* personally identifiable information collected by the site

[39] This includes the sites mentioning that the user's personal information may be disclosed to third parties with his/her consent and the sites not mentioning if the user has any choice wit respect to the disclosure of his/her personal information to third parties.

TABLE 9

The number/percentage of sites in the final samples providing individual elements[40] of the Cookies principle in their privacy policies

	".com"	".edu"	".gov"
Inform the user if cookies are used	87	57	62
Explain what a cookie is	84	53	55
Partial coverage of Cookies	87	57	62
Full coverage of Cookies	84	53	54
No coverage of Cookies	13	43	38

[40] The principle of Cookies is made up of two individual elements: (1) providing the user with information if the site does or may use cookies, and (2) explaining the user what a cookie is or what it is used for.

TABLE 10

The number/percentage of sites in the final samples covering the principle of Contact Information[41] in their privacy policies

	".com"	".edu"	".gov"
Provide contact information for privacy issues	92	68	48
Do not provide contact information	8	32	52

[41] The principle of Contact Information requires the site to post contact information within the privacy policy for those users who may have questions or concerns about the site's privacy practices.

TABLE 11

The number/percentage of sites in the final samples covering the individual elements of each FIP principle in their privacy policies

	".com"	".edu"	".gov"
Informing users of types of collected information (Notice)	93	84	97
Informing users of uses of collected information (Notice)	98	88	99
Choice[42]	84	60	84
Allowing the user to review information (Access)	64	19	8
Allowing the user to edit information (Access)	64	22	8
Allowing the user to delete information (Access)	39	8	8
Security for collected personal information	69	42	24
Security during transmission	47	22	16
Security during storage	55	23	10
Specific mechanisms (Security)	58	27	18
Disclosure to Third Parties[43]	97	74	59
Inform the user if cookies are used (Cookies)	87	57	62
Explain what a cookie is (Cookies)	84	53	55
Contact Information	92	68	48

[42] Choice here is considered to be covered unless the privacy policy does not contain a single statement related to Choice or specifically mentions the possibility of sending a user communication without his/her prior consent

[43] Disclosure to Third Parties here is considered to be covered unless the privacy policy does not contain a single statement related to Disclosure to Third Parties or specifically mentions the possibility of sharing the user's personal information without his/her prior consent

TABLE 12

The number/percentage of sites in the final samples providing full and partial coverage of various combinations of fair information practice principles

	".com"		".edu"		".gov"	
	Partial	Full	Partial	Full	Partial	Full
All seven FIP principles[44]	55	13	9	1	4	2
Notice, Choice, Access, Security, Disclosure to Third Parties, & Contact Information	56	14	11	1	4	2
Notice, Choice, Access, Security, & Disclosure to Third Parties	57	14	12	1	5	2
Notice, Choice, Access, Security, & Contact Information	56	17	13	1	10	2
Notice, Choice, Access, & Security	57	17	14	1	11	2
Notice, Choice, & Access	66	28	18	5	13	3
Notice, Choice, & Disclosure to Third Parties	84	62	48	48	53	51
Notice & Choice	84	68	56	55	84	82

[44] The seven FIP principles in the present study include the principles of Notice, Choice, Access, Security, Disclosure to Third Parties, Cookies, and Contact Information.

Appendix E. Lists of the Web Sites in the Final Samples

The list of the Web sites in the ".com" sample

www.adobe.com

www.nolo.com

www.msnbc.com

www.selfhelpmagazine.com

www.about.com

www.modemhelp.com

www.webring.com

www.real.com

www.m-w.com

www.excite.com

www.globeinvestor.com

www.azcentral.com

www.go.com

www.mp3.com

www.htmlhelpcentral.com

www.algebra.com

www.tbo.com

www.nba.com

www.macromedia.com

www.golfhelp.com

www.newsday.com

www.altavista.com

www.forbes.com

www.homeworkspot.com

www.bayarea.com

www.nasdaq.com

www.thestreet.com

www.stltoday.com

www.lyris.com

www.nwinternet.com

www.microsoft.com

www.networksolutions.com

www.wiley.com

www.nj.com

www.infoplease.com

www.symantec.com

www.cybertechhelp.com

www.staples.com

www.smartpages.com

www.cisco.com

www.resume.com

www.anywho.com

www.oregonlive.com

www.superpages.com

www.rockwellautomation.com

www.sun.com

www.ntlworld.com

www.monster.com

www.imaternity.com

www.quicken.com

www.rootsweb.com

www.wcpo.com

www.advocate.com

www.imdiversity.com

www.reference.com

www.travelocity.com

www.neopets.com

www.usairways.com

www.bmn.com

www.ivillage.com

www.google.com

www.yell.com

www.homerunhelpdesk.com

www.education-world.com

www.zingy.com

www.channelweb.com

www.findlaw.com

www.monstermoving.com

www.alaskaair.com

www.bcentral.com

www.justlinux.com

www.netlibrary.com

www.rhymezone.com

www.wextech.com

www.quia.com

www.englishclub.com

www.animationfactory.com

www.care2.com

www.epnet.com

www.clevermedia.com

www.corning.com

www.bmjjournals.com

www.projo.com

www.nmscommunications.com

www.hrmjobs.com

www.enature.com

www.catalogcity.com

www.builder.com

www.isinet.com

www.wetfeet.com

www.zap2it.com

www.mypostcards.com

www.ringsurf.com

www.superkids.com

www.rottentomatoes.com

www.postini.com

www.bizhosting.com

www.walgreens.com

The list of the Web sites in the ".edu" sample

www.ucla.edu
www.purdue.edu
www.unl.edu
www.berkeley.edu
www.upenn.edu
www.buffalo.edu
www.clarku.edu
www.utexas.edu
www.asri.edu
www.harvard.edu
www.yale.edu
www.umn.edu
www.gwu.edu
www.tayloru.edu
www.unt.edu
www.ucsb.edu
www.gallaudet.edu
www.csbsju.edu
www.ufl.edu
www.gmu.edu
www.spjc.edu
www.lsu.edu
www.pacificu.edu
www.asu.edu
www.ohio-state.edu
www.uillinois.edu
www.virginia.edu
www.usf.edu
www.ksbe.edu
www.tamu.edu
www.neu.edu
www.kumc.edu
www.indiana.edu
www.ua.edu
www.unh.edu
www.ciachef.edu
www.fsu.edu
www.wayne.edu
www.prin.edu
www.berklee.edu
www.reed.edu
www.miami.edu
www.cuny.edu
www.umass.edu
www.shsu.edu
www.bgsu.edu
www.nau.edu
www.vt.edu
www.du.edu
www.umm.edu

www.albany.edu

www.iastate.edu

www.ucr.edu

www.colorado.edu

www.ucar.edu

www.richmond.edu

www.uconn.edu

www.ttu.edu

www.nyu.edu

www.uta.edu

www.vcu.edu

www.uwc.edu

www.uab.edu

www.unr.edu

www.vcsu.edu

www.smu.edu

www.mesastate.edu

www.claremont.edu

www.nebrwesleyan.edu

www.ncsu.edu

www.excelsior.edu

www.metrostate.edu

www.wellesley.edu

www.mcw.edu

www.uh.edu

www.wisconsin.edu

www.sunysb.edu

www.tamuk.edu

www.frostburg.edu

www.uncc.edu

www.drew.edu

www.usma.edu

www.potsdam.edu

www.csu.edu

www.sinclair.edu

www.wpi.edu

www.waldenu.edu

www.uwf.edu

www.odu.edu

www.austincc.edu

www.uams.edu

www.tarleton.edu

www.lincolninst.edu

www.radford.edu

www.jmu.edu

www.unf.edu

www.pvamu.edu

www.mu.edu

www.bcm.edu

www.agnesscott.edu

The list of the Web sites in the ".gov" sample

www.courtinfo.ca.gov

www.nsf.gov

www.nih.gov

www.fda.gov

www.usgs.gov

www.cde.ca.gov

www.science.gov

www.clinicaltrials.gov

www.senate.gov

www.cdc.gov

www.fcc.gov

www.leg.wa.gov

www.nasa.gov

www.census.gov

www.ed.gov

www.kids.gov

www.usaid.gov

www.nlrb.gov

www.dhhs.gov

www.usda.gov

www.georgia.gov

www.fnal.gov

www.ornl.gov

www.gpo.gov

www.ciwmb.ca.gov

www.regulations.gov

www.nara.gov

www.missouri.gov

www.uscourts.gov

www.osha.gov

www.guideline.gov

www.treas.gov

www.ffiec.gov

www.doi.gov

www.va.gov

www.aoa.gov

www.sba.gov

www.ri.gov

www.usmint.gov

www.usbr.gov

www.transportation.ky.gov

www.nist.gov

www.dca.ca.gov

www.whitehouse.gov

www.lanl.gov

www.lbl.gov

www.rrb.gov

www.bcis.gov

www.osti.gov

www.peacecorps.gov

www.bts.gov

www.dor.mo.gov

www.golearn.gov

www.house.gov

www.anl.gov

www.ferc.gov

www.bls.gov

www.girlpower.gov

www.dot.gov

www.nrel.gov

www.epa.gov

www.oehha.ca.gov

www.drugabuse.gov

www.irs.gov

www.nps.gov

www.dfg.ca.gov

www.flra.gov

www.vermont.gov

www.metrokc.gov

www.4woman.gov

www.ojp.gov

www.gis.ca.gov

www.ezec.gov

www.noaa.gov

www.ncifcrf.gov

www.fws.gov

www.wa.gov

www.dshs.wa.gov

www.hud.gov

www.sannet.gov

www.fbi.gov

www.llnl.gov

www.faa.gov

www.fec.gov

www.nysed.gov

www.gsa.gov

www.sc.gov

www.ntis.gov

www.blm.gov

www.ky.gov

www.ecy.wa.gov

www.sos.mo.gov

www.presidentialserviceawards.gov

www.abmc.gov

www.federalreserve.gov

www.doe.gov

www.nashville.gov

www.sfwmd.gov

www.buyusa.gov

www.doc.gov

References

Adkinson, W., Eisenach, J., & Lenard, T. (2002). *Privacy online: A report on the information practices and policies of commercial Web sites.* Retrieved July 3, 2003, from www.pff.org/publications/privacyonlinefinalael.pdf

Anton, A., & Earp, J.A (2001). *A taxonomy for Web site privacy requirements.* Retrieved July 12, 2003, from http://www.csc.ncsu.edu/faculty/anton/pubs/antonTSE.pdf

BBBOnline, Inc. (n.d.) *Better Business Bureau/ BBBOnline. Code of online business practices. Final version.* Retreived July 14, 2003, from http://www.bbbonline.com/reliability/code/principle3.asp

Brin, S., & Page, L. (n.d.). *The anatomy of a large-scale hypertextual Web search engine.* Retrieved October 10, 2003, from http://www-db.stanford.edu/~backrub/google.html

Business Week, & Louis Harris & Associates, Inc. (1998). *BW/Harris poll: Online insecurity.* Retrieved June 15, 2003, from http://www.businessweek.com/@@4WZJy4cASJ*2SwAA/1998/11/b3569107.htm

Center for Democracy and Technology (CDT). (2001, July). *Online banking privacy: A slow, confusing start to giving customers control over their information.* Retrieved July 16, 2003, from http://www.cdt.org/privacy/financial/010829onlinebanking.pdf

Center for Media and Education (CME). (2001, April). *COPPA, the first year: A survey of sites.* Retrieved July 15, 2003, from http://www.cme.org/children/privacy/coppa_rept.pdf

Clarke, R. (1999, September 16). *Introduction to dataveillance and information privacy, and definitions of terms.* Retrieved June 28, 2003, from http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Cranor, L.F., Reagle, J., & Ackerman, M.S. (1999) *Beyond concern: Understanding Net users' attitudes about online privacy.* AT&T Labs-Research Technical Report TR 99.4.3. Retrieved July 4, 2003, from http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm

Culnan, M. (1999). *Georgetown Internet privacy policy survey: Report to Federal Trade Commission.* Retrieved July 5, 2003, from http://www.msb.edu/faculty/culnanm/gippshome.html

Earp, J., & Baumer, D. (2003). Innovative Web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46,* 81-83. Retrieved August 2, 2003, from http://portal.acm.org/citation.cfm?id=641209&coll=GUIDE&dl=ACM&CFID=11263948&CFTOKEN=3700586&ret=1#Fulltext

EDUCAUSE, the association for information technology in higher educaiton. (n.d.). *.edu eligibility.* Retrieved July 20, 2003, from http://www.educause.edu/edudomain/eligibility.asp

Etzioni, A.(1999). *The limits of privacy.* New York: Basic Books

Extreme Searcher's Web Page – News & Updates, The. (n.d.). Retrieved September 10, 2003, from http://extremesearcher.com/news.htm#Google

Fair Credit Reporting Act, The. (n.d.) Retrieved July 12, 2003, from http://www.consumerprivacyguide.org/law/fcra.shtml

Federal Trade Commission Act. (1993). Retrieved July 18, 2003, from http://www.fda.gov/opacom/laws/ftca.htm

Federal Trade Commission (FTC). (1998, June). *Privacy online: A report to Congress.* Retrieved July 5, 2003, from http://www.ftc.gov/reports/privacy3/toc.htm

Federal Trade Commission (FTC). (2000, May). *Privacy online: Fair information practices in the electronic marketplace.* Retrieved July 15, 2003, from http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Federal Trade Commission (FTC). (2000a, October). *Remarks by Commissioner Sheila F. Anthony before the first national HIPPA summit. Grand Hyatt Hotel Washington, D.C., October 15-17, 2000.* Retrieved August 10, 2003, from http://www.ftc.gov/speeches/anthony/hippa.htm

Garfinkel, S. (2002). *Web security, privacy, and commerce.* (2nd ed.). Sebastopol, California: O'Reilly & Associates, Inc.

General Accounting Office (GAO). (2000, September). *Internet privacy: Comparison of federal agency practices with FTC's fair information principles.* GGAO/AIMD-00-296R. Retrieved July 16, 2003, from www.gao.gov

General Services Administration. (n.d.) *Eligibility requirements: .GOV registration.* Retrieved July 20, 2003, from http://www.nic.gov/help_qualify.html

Goldman, J., Hudson, Z., & Smith, R. (2000). *Privacy: Report on the privacy policies and practices of health Web sites.* Retrieved September 13, 2003, from http://www.chcf.org/documents/ihealth/privacywebreport.pdf

Google. (n.d.). *Our search: Google technology.* Retrieved October 10, 2003, from http://www.google.com/technology/index.html

Gregory, C., & Kalven, H. (1969). *Cases on torts.* Boston: Little, Brown & Co.

Henkin, L. (1974). Privacy and autonomy. *Columbia Law Review, 74.*

Lemos, R. (2000, April 26). Intel disables ID tracking in new chips. *ZDNet News.* Retrieved July 28, 2003, from http://zdnet.com.com/2100-11-520265.html?legacy=zdnn

Locke, J. (1956). *The second treatise of civil government.* New York: Hafner Publishing.

Lund, W. R. (1997). Politics, virtue, and the right to do wrong: Assessing the communitarian crutique of rights. *Journal of Social Philosophy, 91.*

National Academy of Sciences, Computer Science & Engineering Board. (1972). *Databanks in a free society: Report of the project on computer databanks.* New York: Quadrangle Books

National Electronic Commerce Coordinating Council (NECCC). (2000, December). Privacy policies – Are you prepared? A guidebook for state and local government. Retrieved July 16, 2003, from http://www.ec3.org/Downloads/2000/Privacy_Policies_Paper_III.pdf

Organisation for Economic Co-operation and Development (OECD). (1980, September). *Guidelines on the protection of privacy and transborder flows of personal data.* Retrieved July 10, 2003 from http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html

Pember, D. (2003). *Mass media law.* (2003-2004 ed.) New York: McGraw-Hill

Pew Research Center for the People and the Press, The. (2000, August 20). *Pew Internet & American Life Project: Trust and privacy online: Why Americans want to*

rewrite the rules. Retrieved August 10, 2003, from http://www.pewinternet.org/reports/reports.asp?Report=19&Section=ReportLevel1&Field=Level1ID&ID=43

Schwartz, J. (2000, March 3). DoubleClick halts profiling plan. *The Washington Post*, p. A01. Retrieved August 10, 2003, from http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A61991-2000Mar2&notFound=true

TRUSTe. (n.d.). *We're building a Web you can believe in!* Retrieved July 15, 2003, from http://www.truste.org/about/truste/index.html

U.S. Congress. (1993). Federal Trade Commission Act. Title 15, para 45. Retrieved July 20, 2003, from http://www.fda.gov/opacom/laws/ftca.htm

U.S. Department of Health, Education, & Welfare (USDHEW), Secretary's Advisory Committee on Automated Personal Data Systems. (1973, July). *Records, computers, and the rights of citizens.* Retrieved July 12, 2003, from http://www.epic.org/privacy/hew1973report

Warren, S., & Brandeis, L. (1890, December 15). The right to privacy. *Harvard Law Review*, *4*, (5). Retrieved September 14, 2003, from http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html

West, D.M. (2000). *Assessing e-government: The Internet, democracy, and service delivery by state and federal governments*. Retrieved July 10, 2003, from http://www.insidepolitics.org/egovtreport00.html

Westin, A. (1970). *Privacy and freedom*. London: Bodley Head

About the Author

Rashad Bayramov was born in Baku, Azerbaijan, one of the republics of the former Soviet Union. He received his B.A. degree with honors in the English Language and Roman-Germanic Philology (1999) and his M.A. with honors in the English Language and Linguistics (2001) from Azerbaijan University of Languages.

Mr. Bayramov started his professional career in 1998 as English language interpreter. A growing interest in the field of communications urged him to take the position of Communications Assistant in Internews Network, a U.S.-based non-governmental institution working in the field of media education in Baku, Azerbaijan, and further switch to the position of Public Relations and Media Assistant in the local office of the Organization for Security and Co-operation in Europe.

Mr. Bayramov authored two monographs: *The Use of Articles in Modern English* (2001), a textbook for senior and graduate English language students, and *A Collection of Tests and Exercises on English for University Entrants* (1997), a self-training aid for high school graduates.

In 2001, Mr. Bayramov won an Edmund S. Muskie scholarship for graduate studies in the U.S. in the field of communications and was admitted to the Communication and Media Technologies program at Rochester Institute of Technology.

Since 2003, Mr. Bayramov has been a member of Public Relations Society of America.