



PRIVACY ONLINE:
FAIR INFORMATION PRACTICES
IN THE ELECTRONIC MARKETPLACE
A REPORT TO CONGRESS

FEDERAL TRADE COMMISSION
MAY 2000

Federal Trade Commission*

Robert Pitofsky	Chairman
Sheila F. Anthony	Commissioner
Mozelle W. Thompson	Commissioner
Orson Swindle	Commissioner
Thomas B. Leary	Commissioner

This report was prepared by staff of the Division of Financial Practices, Bureau of Consumer Protection. Advice on survey methodology was provided by staff of the Bureau of Economics.

* The Commission vote to issue this Report was 3-2, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part. Each Commissioner's separate statement is attached to the Report.

EXECUTIVE SUMMARY

The online consumer marketplace is growing at an exponential rate. At the same time, technology has enhanced the capacity of online companies to collect, store, transfer, and ana-

adopted by industry leaders. While there will continue to be a major role for industry self-regulation in the future, the Commission recommends that Congress enact legislation that, in conjunction with continuing self-regulatory programs, will ensure adequate protection of consumer privacy online.

The legislation recommended by the Commission would set forth a basic level of privacy protection for consumer-oriented commercial Web sites. It would establish basic standards of practice for the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act.

Consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online would be required to comply with the four widely-accepted fair information practices:

- (1) Notice – Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (i.e., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
- (2) Choice – Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (i.e., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).
- (3) Access – Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to

As noted above, industry self-regulatory programs would continue to play an essential role under such a statutory structure, as they have in other contexts. The Commission hopes and expects that industry and consumers would participate actively in developing regulations under the new legislation and that industry would continue its self-regulatory initiatives. The Commission also recognizes that effective and widely-adopted seal programs could be an important component of that effort.

For all of these reasons, the Commission believes that its proposed legislation, in conjunction with self-regulation, will ensure important protections for consumer privacy at a critical time in the development of the online marketplace. Without such protections, electronic commerce will not reach its full potential and consumers will not gain the confidence they need in order to participate fully in the electronic marketplace.

-
1. The legislation would cover such sites to the extent not already covered by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 .
 2. 5 U.S.C. § 553.
 3. The Commission will soon be addressing the issue of third-party online collection of personal information for profiling purposes in a separate report to Congress.

I. INTRODUCTION AND BACKGROUND

Over the past five years, the Internet has changed dramatically from a large network of

range. Recent data suggest that consumers spent as much as \$2.8 billion online during the month of January 2000 alone.

In light of such growth in consumer interest and use, it is not surprising that online advertising revenue is also growing at high rates. Internet advertising expenditures climbed to \$4.6 billion in 1999, representing a 141% increase over the \$1.9 billion reported for 1998 and a greater than ten-fold increase from 1996, when \$267 million was spent on Internet advertising.

B. CONSUMER CONCERNS ABOUT ONLINE PRIVACY

With this remarkable growth in e-commerce has come increased consumer awareness that online businesses are collecting and using personal data, and increased consumer concern about the privacy of this data. Recent survey data demonstrate that 92% of consumers are concerned (67% are "very concerned") about the misuse of their personal information online. Concerns about privacy online reach even those not troubled by threats to privacy in the off-line world. Thus, 76% of consumers who are not generally concerned about the misuse of their personal information fear privacy intrusions on the Internet. This apprehension likely translates into lost online sales due to lack of confidence in how personal data will be handled. Indeed, surveys show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce,⁴ and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction. One study estimates that privacy concerns may have resulted in as much as \$2.8 billion in lost online retail sales in 1999, while another suggests potential losses of up to \$18 billion by 2002 (compared to a projected total of \$40 billion in online sales), if nothing is done to allay consumer concerns. The level of consumer unease is reflected in the results of a recent study in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential, and 82% agreed that government should regulate how online companies use personal information.

Public concern regarding privacy online appears likely to continue. A bipartisan caucus has been formed in the Congress and bills addressing online privacy are pending both there and in a number of state legislatures. To ensure the continued growth of the online marketplace, and to ensure that this marketplace reaches its full potential, consumer concerns about privacy must be addressed.

C. THE COMMISSION'S APPROACH TO ONLINE PRIVACY – INITIATIVES SINCE 1995

Since 1995, the Commission has been at the forefront of the public debate on online privacy. Among other activities, the Commission has held public workshops; examined Web site information practices and disclosures regarding the collection, use, and transfer of personal information; and commented on self-regulatory efforts and technological developments intended to enhance consumer privacy. The Commission's goals have been to understand this new marketplace and its information practices, and to assess the costs and benefits to businesses and consumers. While the Commission recommended legislation to address children's privacy in 1998, it has continued to encourage and facilitate effective self-regulation to protect consumers generally.

1. THE AIR INFORMATION PRACTICE PRINCIPLES AND PRIOR COMMISSION REPORTS

In its 1998 report, *Privacy in the Electronic Marketplace*, the Commission summarized widely-accepted principles regarding the collection, use, and dissemination of personal information.⁴ These fair information practice principles, which predate the online medium, have been recognized and developed by government agencies in the United States, Canada, and Europe since 1973, when the United States Department of Health, Education, and Welfare released its seminal report on privacy protections in the age of data collection, *Privacy and Confidentiality*.

The 1998 Report identified the core principles of privacy protection common to the government reports, guidelines, and model codes that had emerged as of that time:

- (1) Notice – data collectors must disclose their information practices before collecting personal information from consumers;
- (2) Choice – consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;
- (3) Access – consumers should be able to view and contest the accuracy and completeness of data collected about them; and
- (4) Security – data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

It also identified Enforcement – the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices – as a critical ingredient in any governmental or self-regulatory program to ensure privacy online.

The 1998 Report also set out the findings of the Commission's first online privacy survey of commercial Web sites' information practices and assessed self-regulatory efforts to protect consumers' privacy online. The 1998 survey demonstrated that, while almost all Web sites (92% of the comprehensive random sample) were collecting large amounts of personal information from consumers, few (14%) disclosed anything at all about the site's information practices: how, for example, personal information was used by the site; whether it was shared with others; and whether consumers had any control over the use or disclosure of their information.

Based on survey data showing that the vast majority of sites directed at children also collected personal information, the Commission called upon Congress to enact legislation protecting this vulnerable population. The Commission deferred its recommendations with respect to all other commercial sites. In subsequent Congressional testimony, the Commission referenced promising self-regulatory efforts suggesting that industry should be given more time to

address online privacy issues. The Commission urged the online industry to expand these efforts by adopting effective, widespread self-regulation based upon the long-standing fair information practice principles – Notice, Choice, Access, and Security – and putting enforcement mechanisms in place to assure adherence to these principles.

Last year, Georgetown University Professor Mary Culnan conducted a survey of a random sample drawn from the most-heavily trafficked sites on the Web and a survey of the busiest 100 sites. The results of the former, the Georgetown Internet Privacy Policy Survey Report (“GIPPS Report”), showed significant improvement in the frequency of privacy disclosures. Notwithstanding this positive change, the results of the GIPPS Report demonstrated that industry still had far to go in improving the nature and substance of those disclosures. Only one-tenth of the sites made disclosures that even touched on all four fair information practice principles. After reviewing the GIPPS Report, the Commission issued its 1999 report to Congress, *Privacy in the Electronic Marketplace*. In the 1999 Report, a majority of the Commission again recommended that self-regulation be given more time, but called for further industry efforts to implement the fair information practice principles and promised continued Commission monitoring of these efforts.

2. COMMISSION INITIATIVES SINCE THE 1999 REPORT

In the past year, the Commission has been involved in several significant initiatives to study and promote online privacy. In November 1999, the Commission, together with the Department of Commerce, held a public workshop on “online profiling”⁴ by third-party advertisers. The workshop was designed to educate the public about this practice, as well as its privacy implications, and to examine current efforts by network advertisers to implement fair information practices. At the workshop, industry leaders announced their commitment to develop self-regulatory principles based on fair information practices. The Commission soon will issue a report addressing concerns raised by online profiling, as well as industry’s self-regulatory efforts in this area.

The Commission also convened an Advisory Committee on Online Access and Security, a group comprising 40 e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates, to provide advice and recommendations to the Commission regarding the implementation of the fair information practice principles of Access and Security online. In a series of public meetings, the Advisory Committee discussed options, and the

Other online privacy seal programs have been announced or are in the early stages of development,⁴ and a complementary effort by major accounting firms to offer online privacy assurance services is underway. Nevertheless, and despite the fact that the established programs have experienced continued growth, the impact of online privacy seal programs on the Web remains limited, as demonstrated by the Survey results discussed below.⁴

II. RESULTS OF THE COMMISSION'S 2000 ONLINE PRIVACY SURVEY

A. OVERVIEW

In February and March 2000, the Commission conducted a survey of the busiest U.S. commercial sites on the World Wide Web.⁴⁴ The objective of the Survey was to gather the information necessary to assess industry's progress in protecting consumer privacy online. Accordingly, the Survey examined how many commercial Web sites collect personal information from consumers and how many provide any privacy disclosures; it also included an analysis of the content of Web sites' privacy disclosures in light of the fair information practice principles. Finally, the Survey provided a first look at the practice of online profiling by measuring the prevalence of the placement of cookies⁴ by third parties.

The Survey examined Web sites that had 39,000 or more unique visitors⁴ each month. These sites were drawn from a list provided by Nielsen//NetRatings based on January 2000 traffic figures. Two separate groups were drawn from this pool of sites: (1) a random sample of all of the sites (the "Random Sample") and (2) the 100 busiest sites (the "Most Popular Group"). A detailed methodology describing the sample selection, data collection, data entry, and data analysis is included in Appendix A. Lists of the sites included in the Random Sample and the Most Popular Group are set forth in Appendix B.

Data collection for the Survey took place in three phases. First, Commission staff surveyed both groups of Web sites during a two-week period in February 2000, searching each site to determine whether it (a) collects personal identifying information and/or non-identifying

information from consumers and (b) posts, privacy disclosures.⁴ Privacy disclosures were defined to include both “privacy policies,” (descriptions of a site’s information practices located together in a paragraph or on a Web page), and “information practice statements,” discrete statements about particular information practices.⁴ Commission staff printed all privacy disclosures they found at a site. Second, a separate group of Commission staff examined each site surveyed to determine whether any entity other than the Web site being visited was attempting to place a cookie on the site.

Finally, a third group of Commission staff reviewed all of the privacy disclosures for each site in the Survey and answered questions about the content of these disclosures. This content analysis assessed a site’s compliance with the four fair information practice principles: Notice, Choice, Access, and Security. Copies of the questionnaires completed by staff in each phase of the Survey, as well as the instructions for use of each form, are set forth in Appendix B.⁴

The results of the Survey are reported below for both the Random Sample and the Most Popular Group. Results for the Random Sample may be generalized to all U.S. “.com” sites with 39,000 or more unique visitors per month (excluding “adult,” children’s, and business-to-business sites). Results for the Most Popular Group refer only to the sites in that group, and cannot be generalized beyond that universe. In addition, a “weighted analysis” figure is also reported. Unlike the other two measures, which reflect the likelihood that a site will follow a particular information practice, the weighted analysis figure reflects the likelihood that a consumer will visit a site that follows that practice. It seeks to represent consumer experience and gives proportionately more weight to sites with more traffic. A detailed explanation of the weighted analysis is included in the Methodology in Appendix A.

B. SURVEY RESULTS

1. SITES SURVEYED

The Random Sample consists of 335 Web sites, including e-commerce sites offering a wide array of consumer goods and services: auctions; banking; cars; clothing; electronics; flowers; groceries; home decorating supplies; investment services; online directories and look-up services; personal care products; software; sporting goods; and Web site hosting services. The Random Sample also includes sites that provide information, such as news and entertainment, as well as financial, medical, sports, and travel information.

The Most Popular Group consists of 91 of the 100 busiest sites on the Web in January 2000. Web sites in this group include search engines, portals, and Internet service providers, as well as e-commerce sites offering consumer goods and services, including computer hardware and software; electronics; email services; books; music; clothing; news and entertainment; auctions and contests; job listings; travel services; real estate listings; and medical information.

2. PERSONAL INFORMATION COLLECTION

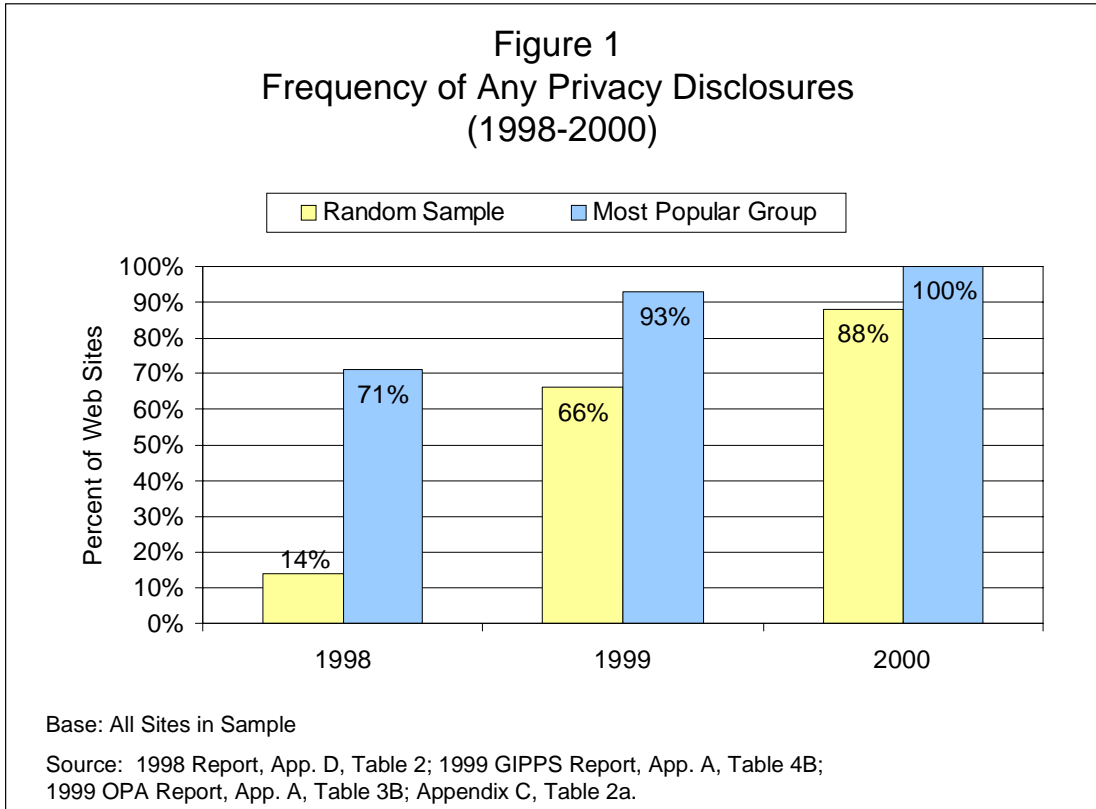
Web sites collect a vast amount of personal information from and about consumers. This information is routinely collected from consumers through registration forms, order forms, surveys, contests, and other methods on Web

weighted analysis figure is 76%. Most of the sites surveyed, therefore, are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior, or surfing behavior information they collect to personal identifying information.

■ FREQUENCY OF PRIVACY DISCLOSURES: COMPARISON WITH PREVIOUS SURVEYS

The results of the 1999 GIPPS Report showed a significant increase over the previous year in the percent of Web sites posting at least one privacy disclosure – . . . , either a unified privacy policy or a discrete information practice statement (such as, “This is a secure order form”). Sixty-six percent of Web sites in the GIPPS random sample, compared with 14% of Web sites in the Commission’s 1998 Comprehensive Sample had such disclosures. This year, the Commission’s Survey findings demonstrate continued improvement on this front, with 88% of Web sites in the Random Sample posting at least one privacy disclosure. Of sites in the Random Sample that collect personal identifying information, 90% post at least one privacy disclosure.⁴ All of the sites in the Most Popular Group post at least one privacy disclosure, compared with 93% of the sites in Professor Culnan’s 1999 survey of the 100 busiest sites, and 71% in the Commission’s 1998 Most Popular Sample. The weighted analysis figure is 96%.

The percent of sites displaying a privacy policy (as opposed to a discrete information practice statement) has also continued to increase. Sixty-two percent of sites in the Random Sample (compared with 44% in the 1999 GIPPS survey) and 97% of sites in the Most Popular Group (compared with 81% in the 1999 OPA survey) post a privacy policy. The weighted analysis figure is 82%. Figure 1 demonstrates the progress Web sites have made in posting any disclosures about their information practices since the Commission’s 1998 Report was issued.



There are limits, however, to the value of this data in assessing the extent of consumer privacy protection online. In ascertaining whether a privacy disclosure was posted on a site, Commission staff credited a disclosure, even if related to only one discrete information practice. Thus, a site posting only a statement such as "Click here if you do not want to receive email updates from us," or "This is a Secure Order Form," was given credit for having a privacy disclosure. Moreover, even the posting of a privacy policy does not necessarily mean that a site follows any or all fair information practices, as the policy might address only certain practices and not others. Accordingly, the Commission's 2000 Survey went beyond the mere counting of disclosures; it analyzed the nature and substance of these privacy disclosures in light of the fair information practice principles described in the 1998 Report.



Implementation of Notice & Choice Only

While views about how Web sites should implement Access and Security differ, Notice and Choice do not present the same implementation issues. Therefore, the Commission also examined the data to determine whether Web sites are implementing Notice and Choice. In evaluating sites in terms of these two principles only, the Survey found that 41% of sites in the Random Sample that collect personal identifying information, and 60% of such sites in the Most Popular Group, meet the basic Notice and Choice standards. The weighted analysis figure for e standards.



collector to ensure the confidentiality, integrity and quality of the data. Notice, then, requires more than simply making an isolated statement about a particular information practice.

Consumers are very interested in learning about a site's information practices before providing personal information. Survey data show that an overwhelming majority of consumers believe that it is "absolutely essential" or "very important" that a site display a privacy policy and explain how personal information will be used before consumers provide information or make a purchase. Indeed, survey data also show that 57% of Internet users have decided not to use or purchase something from a retail Web site because they were not sure how the site would use their personal information.⁴

The Commission's Survey asked several questions designed to ascertain if sites are following the Notice principle. A site was deemed to have provided "Notice" if it met the following criteria: (1) it posts a privacy policy; (2) it says anything about what specific personal information it collects; (3) it says anything about how the site may use personal information internally; and (4) it says anything about whether it discloses personal information to third parties.⁵

tions. In addition, an overwhelming majority of consumers – 88% – want sites to always ask permission before sharing their personal information with others.

Consumer survey research shows that online consumers are also concerned about how their information is used by Web sites for marketing purposes. According to one recent study, online consumers “dread junk mail”: 78% of Internet users who have purchased online report being concerned that the company from which they have made a purchase will use personal information to send them unwanted email, or “spam.” Of those Internet users who have not made any purchases online, nearly all – 94% – are concerned about being spammed, and concern among both buyers and non-buyers has increased since 1998.⁴ Further, over 70% of consumers identified the ability to be removed from a site’s mailing list as a “very important” criterion in assessing a site’s privacy protections.

Consistent with these consumer concerns, the Cna juhn0.0421 Tw(Con8.0-en)]Tr.00Tj/F1tall/F18 TD-0.0

consider important. A recent survey found that 79% of Internet users believe that a procedure allowing the consumer to see the information the company has stored about them is “absolutely essential” or “very important.” The Commission also believes that the ability to address any inaccuracies found – through correction or deletion – benefits consumers and data collectors by improving the accuracy of data and increasing consumer trust. Based on the work of the Advisory Committee, however, the Commission still believes that the specific terms of Access (. . . , the scope of information made available) and the burdens and costs it imposes should be carefully considered in any determination of what constitutes “reasonable access.”

Security: The fourth fair information practice principle, Security, refers to a data collector’s obligation to protect personal information against unauthorized access, use, or disclosure, and against loss or destruction. Security involves both managerial and technical measures to provide such protections. ⁴ The Commission believes that Security, like Access, presents unique implementation issues and that the security provided by a Web site should be “adequate” in light of the costs and benefits.

As discussed in greater detail below, the Advisory Committee also explored the meaning of “adequate security” and developed implementation options. There was strong agreement among Committee members that security is a process: no one static standard can assure adequate security, as threats, technology, and the Internet itself are constantly evolving. There was also consensus that commercial Web sites should maintain security programs to protect personal data and that data security requirements may vary depending on the nature of the data collected; therefore, the Advisory Committee Report recommends that each Web site maintain a security program that is “appropriate to the circumstances.” The Advisory Committee pointed out that, while most consumers worry about security for the transmission of personal information to a site, security threats to that information once a site receives it are far more substantial and pervasive.

The Advisory Committee also examined whether, and to what extent, Web sites should make disclosures about security. As discussed in greater detail below, the Committee agreed



C. BEYOND THE NUMBERS

The Survey results described above must be assessed in light of the Survey's limitations and the complexity of many Web sites' information practices. This section of the Report provides that context by describing in greater detail the scope of the Survey – and, specifically, the scope of the content analysis – and by addressing qualitative issues not captured by the Survey.

1. SCOPE OF CONTENT ANALYSIS

In light of the complexity of actual business practices and the myriad ways in which companies can handle personal information, it is difficult to categorize the many disparate information practices embodied in the privacy disclosures that were analyzed. Many Web sites have multiple information practices that differ according to the nature or source of the information at issue or the context in which it was collected. While some sites have a single practice that applies to all information (for example, a site may state that it never shares any personal information with third parties), other sites have multiple policies that apply in different circumstances (for example, a site may share certain types of information with third parties if a consumer enters a sweepstakes, but not if a purchase is made). Capturing information at this level of detail was beyond the scope of the Survey.

Further, many Web sites' privacy disclosures are unclear as to whether certain stated practices are universally applied. Thus, for example, a site may state that it provides consumers choice with respect to receiving a newsletter from the site. While such a disclosure provides choice with respect to receiving further communications from the site, it says nothing about whether the site will or will not contact the consumer in other ways. Similarly, a site may identify certain items of personal information that it collects, or certain uses made of that information; however, because the Survey assesses only a Web site's stated fair information practices, and not its actual practices, it is impossible to assess whether such a disclosure is complete – . . ., whether it describes of the information the site collects or of the uses made of that information.

- With respect to

materially from the details disclosed further in the privacy policy. Unfortunately, this is not an uncommon practice, as many sites describe their policies in general, privacy-protective language, only to reveal further in the policy that many exceptions exist to the general rule.

Examples of confusing policies abound. Thus, one site represents:

As a general rule, [the company] will not disclose any of your personally identifiable information except when we have your permission or under special circumstances, such as when we believe in good faith that the law requires it or under the circumstances described below.

Elsewhere in the privacy policy the site says that it “does not sell or rent user information to anyone.” Such statements give the impression that personal information will not be provided to third parties absent a consumer’s consent or some special circumstance. In reality, however, the privacy policy goes on to disclose myriad circumstances in which information may be provided to third parties, including the disclosure of information to business partners, sponsors, and other third parties. While it is commendable that the site discloses these information sharing practices, the general statements quoted above serve to obfuscate these sharing arrangements.

Another site “invite[s] all customers who would like to receive [company] information via email to contact us” This gives the impression that absent some affirmative step by the consumer (. .

contradictory language is likely to confuse consumers and negate the value of posting informa-

d. Best Practices

The Commission commends those sites that have posted privacy policies and implemented the fair information practices. Improving the clarity and comprehensibility of such policies, however, is essential to overcoming consumer concerns about the misuse of their personal information. Based upon the Survey, the Commission has identified the following guidelines that may help ensure that consumers understand what a Web site's information practices are.

Of utmost importance, privacy policies and other information practice disclosures should be clear and conspicuous, and written in language that is simple and easy to understand. These disclosures should be site-specific and should be based on the site's actual information practices. Web sites should also strive to avoid the confusing practices discussed above – such as using misleading general statements and ambiguous language regarding choice. In light of the complexity of many entities' information practices, the Commission recognizes the tension inherent in drafting disclosures that are succinct and easy to read on the one hand and accurate on the other; it believes that, consistent with the existing practices of many Web sites, this tension is appropriately dealt with by providing consumers both summary and detailed information regarding an entity's information practices. The summary information should reflect the entity's basic practices with respect to consumer information, and should accurately depict the nature of those

information is collected. Without clear and understandable information practice disclosures, it is unlikely that consumer concerns regarding online privacy will abate.

III. THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY

As discussed above, the Commission believes that the fair information practice principles of Access and Security are important elements in safeguarding privacy, but recognizes that implementing these principles may raise a number of issues. Accordingly, in December 1999, the Commission established the Federal Trade Commission Advisory Committee on Online Access and Security ("Advisory Committee") pursuant to the Federal Advisory Committee Act, 5 U.S.C. App. §§ 1-15 (the "FACA").⁴⁴

proach, a consumer would be able to access all personal information, regardless of medium, method or source of collection, or the type of data in question. Such information might include physical address, phone number, email address, bank account numbers, credit card numbers, gender, age, income, browser type, operating system type, preference data, transactional data, navigational and clickstream data, and inferred or derived data. The principle underlying this approach is that businesses' information practices should be completely transparent to consumers.

Under the "default to consumer access" approach, a Web site would establish a mechanism to make available personal information collected online that is "retrievable in the ordinary course of business." Information "retrievable in the ordinary course of business" is information that can be retrieved by taking steps that are regularly taken by the business with respect to the information, or that the organization is capable of taking under its existing procedures, so long as doing so is not unreasonably burdensome. The "unreasonable burden" concept helps define what is and what is not retrievable in the ordinary course of business.⁴ Thus, the business would not need to set up new databases to maintain information in order to provide access, although the business would need to provide access to aggregations of data that it possesses and retrieves itself. Finally, the business could limit a consumer's access to information where considerations such as another individual's privacy outweigh the individual's interest in access.

Finally, under the “access for correction” approach, a Web site would grant access to personal data in its files only where the Web site uses the personal information to grant or deny significant benefits to an individual, and where granting access would improve the accuracy of the data in a way that justifies the costs. Examples of personal information used to grant or deny significant benefits include credit reports, financial qualifications, and medical records.

The Advisory Committee Report also evaluates whether the Access principle should apply to entities other than the original data collector. ⁴ Members of the Advisory Committee generally agreed that businesses should provide access to data held by their agents. Some members believed that the obligation to provide access should also be extended to “downstream” recipients of the data in order to provide adequate privacy protections for consumers. Others believed that this requirement would be too burdensome.

In addition to examining scope of access issues, the Advisory Committee Report also identifies authentication procedures designed to ensure that only authorized individuals can obtain personal information through an access request. Web sites can employ various levels of authentication in response to an access request – . . . , requiring that the requestor provide the account name, specific personal information (such as a mother’s maiden name), a specific password, information about recent account activity, a physical object that a consumer owns, a biometric characteristic, a piece of information passed to the consumer by a different means, such as the mail, or any combination of these. Requiring an extremely high level of authentication would be very costly to businesses, and also might discourage consumers from accessing and correcting their own information. Thus, members agreed that the level of authentication necessary before providing access to information should vary depending on the circumstances, such as the data’s sensitivity and whether correction is permitted. /

The Commission believes that all of these implementation options will be useful to Web sites in developing procedures to facilitate consumer access to personal information collected from and about them, and that the options will be relevant to any determination as to the scope of “reasonable access.”

B. SECURITY

In considering the parameters of “adequate security” for personal information collected online, the Advisory Committee focused on such issues as the proper standards to assess and ensure “adequate security,” and the managerial and technical measures that should be undertaken to protect information from unauthorized use or disclosure. There was generally far more agreement about how to implement this principle than there was on implementing Access. Advisory Committee members agreed that security is a process, and that no single standard can assure adequate security, because technology and security threats are constantly evolving. Members also generally agreed that there are greater security risks to consumer information after a Web site receives the information than there are during transmission of the information.⁴

The Advisory Committee Report recommends implementation of a security approach that requires that each commercial Web site have a security program to protect personal data that it maintains, and that the program specify its elements and be “appropriate to the circumstances.” The elements of the security program may include conducting a risk assessment; establishing and implementing a security system; managing policies and procedures based on the risk assessment; conducting periodic training for employees; conducting audits; conducting internal reviews; and conducting periodic reassessment of risk. The “appropriateness” standard, which would be defined through case-by-case adjudication, takes into account changing security needs over time as well as the particular circumstances of the Web site, including the risks it faces, the costs of protection, and the type of the data it maintains.

In addition, as noted above, the Advisory Committee Report considers whether Web sites should disclose their security practices. The Report states that a security disclosure is an appropriate tool for informing consumers about a company’s information practices, and is critical to consumers’ ability to make informed choices about those practices. At the same time, it states that while security disclosures could be useful in conjunction with a security program, a disclosure alone does not ensure adequate security.

and deceptive practices in and affecting commerce. It authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain fair information practices. For instance, failure to comply with stated information practices may constitute a deceptive practice in certain circumstances, and the Commission has authority to pursue the remedies available under the Act for such violations. Indeed, the Commission has done so in several cases. The Commission also has authority to enforce the COPPA. As a general matter, however, the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair informa-

could demonstrate that it had developed and implemented broad-based and effective self-regulatory programs, additional government authority in this area might be necessary. In its 1999 Report, a majority of the Commission again determined that legislation was not then appropriate, but noted the "substantial challenges" that industry continued to face in implementing widespread self-regulation.

The Commission recognizes the magnitude of the public policy challenge presented by Internet privacy and applauds the significant accomplishments of the private sector in developing self-regulatory initiatives to date. The improved statistics regarding the number of Web sites with privacy disclosures and the development of online seal programs are a tribute to industry's ongoing efforts in this area. The Commission also applauds the industry leaders who have adopted fair information practices. The 2000 Survey data, however, demonstrate that industry efforts alone have not been sufficient. Because self-regulatory initiatives to date fall far short of broad-based implementation of self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders.

Indeed, as noted above, only 20% of the busiest sites on the World Wide Web implement to some extent all four fair information practices in their privacy disclosures. Even when only Notice and Choice are considered, fewer than half of the sites surveyed (41%) meet the relevant standards. These numbers fall well short of the meaningful broad-based privacy protections the Commission was seeking and that consumers want. Moreover, the enforcement mechanism so crucial to the success and credibility of self-regulation is absent. Notwithstanding several years of industry and governmental effort, only 8% of heavily-trafficked Web sites display a seal from one of the self-regulatory seal programs.

C. LEGISLATIVE RECOMMENDATION

Ongoing consumer concerns regarding privacy online and the limited success of self-regulatory efforts to date make it time for government to act to protect consumers' privacy on the Internet. Accordingly, the Commission recommends that Congress enact legislation to ensure adequate protection of consumer privacy online. In doing so, however, the Commission recognizes that industry self-regulation, as well as consumer and business education, should still play important roles in any legislative framework, as they have in other contexts.

The proposed legislation would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites to the extent not already provided by the COPPA. Such legislation would set out the basic standards of practice governing the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act, including authority to enforce those standards. All consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online, to the extent not covered by the COPPA, would be required to comply with the four widely-accepted fair information practices:

- (1) Notice – Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
- (2) Choice – Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

- (3) Access – Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review the information and to correct inaccuracies or delete information.
- (4) Security – Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.

The Commission recognizes that the implementation of these practices may vary with the nature of the information collected and the uses to which it is put, as well as with technological developments. For this reason, the Commission recommends that any legislation be phrased in general terms and be technologically neutral. Thus, the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules or regulations.

Such rules or regulations could provide further guidance to Web sites by defining fair information practices with greater specificity. ⁴ For example, after soliciting public comment, the implementing agency could expand on what constitutes “reasonable access” and “adequate security” in light of the implementation issues and recommendations identified and discussed by the Advisory Committee (i.e., it could identify those circumstances where access would be required and those where the burdens imposed, the intended use of the information, or other considerations would lead to the conclusion that no access is required). Similarly, the agency could examine the specific contours of the Choice requirement, particularly its application to programs in which the sole reason for providing consumers a particular benefit is the collection and use of personal information (i.e., providing discounts to consumers expressly conditioned on the exchange of personal information).

Finally, the Commission notes that industry self-regulatory programs would continue to play an essential role under such a statutory structure. The Commission hopes and expects that industry and consumers would participate actively in developing regulations under the new

legislation and that industry would continue its self-regulatory initiatives. The Commission also recognizes that effective and widely-adopted seal programs could be an important component of that effort.

V. CONCLUSION

The Commission believes that industry's limited success in implementing fair information practices online, as well as ongoing consumer concerns about Internet privacy, make this the appropriate time for legislative action. The Commission's proposed legislation would require all consumer-oriented commercial Web sites, to the extent not already covered by the COPPA, to implement the four widely-accepted fair information practice principles, in accordance with more specific regulations to follow. Such legislation, in conjunction with self-regulation, would ensure important protections for consumer privacy at a critical time in the development of the online marketplace.

represent a significant increase from several years ago, when an estimated 48 million American and Canadian adults were on the Web and only ten million had actually purchased a product or service online. CommerceNet and Nielsen Media Research, *CommerceNet and Nielsen Media Research*, Fall '97 (Dec. 11, 1997), available at < <http://www.commerce.net/news/press/121197.html> > . Online shopping is also increasingly popular with young consumers. "More than one-third of 16- to 22-year-olds will buy online this year, spending \$4.5 billion – more than 10% of their disposable income." Forrester Research, Inc., *Forrester Research, Inc.* (Feb. 2000) (quoting Ekaterina O. Walsh, analyst, Technographics Data & Analysis), available at < <http://www.forrester.com/ER/Press/Release/0,1769,248,FF.html> > .

8. Internet Advertising Bureau, *Internet Advertising Bureau*, \$4.6 billion, 1999 (Apr. 18, 2000), available at < <http://www.iab.net/news/content/revenues.html> > [hereinafter "IAB 1999 Revenue Report"]. This indicates that Internet advertising spending is growing faster than historical trends in other media. Internet ad revenues hit the \$4 billion/year mark after just five years. In inflation-adjusted dollars, it took six years before television ad revenues hit \$4 billion/year, 13 years for cable television, and 30 years for radio. Internet Advertising Bureau, *Internet Advertising Bureau*, 1999, available at < <http://www.iab.net/news/content/3Q99exec.html> > .
9. IAB 1999 Revenue Report.
10. Internet Advertising Bureau, *Internet Advertising Bureau*, 1996 (Mar. 25, 1997), available at < <http://www.iab.net> > .
11. The exchange of personal identifying information as part of a commercial transaction or other online exchange raises special concerns. Once disclosed, such information may be subject to myriad uses, many if not all of which may be unknown to the consumer. Also, once disclosed to entities other than the data collector, the consumer may lose all control over the use and further dissemination of the information.
12. Alan F. Westin, *Privacy and Personal Information* at 11 (Nov. 1999) [hereinafter "Westin/PAB 1999"]. *Privacy and Personal Information* at 72 (Oct. 1999), prepared by Louis Harris & Associates Inc. [hereinafter "IBM Privacy Survey"] (72% of Internet users very concerned and 20% somewhat concerned about threats to personal privacy when using the Internet); Forrester Research, Inc., *Forrester Research, Inc.* (Oct. 1999), available at < <http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html> > (two-thirds of American and Canadian online shoppers feel insecure about exchanging personal information over the Internet).
13. IBM Privacy Survey at 73.
14. Fewer than 20% of adults who agree that the Internet threatens their privacy have placed orders online, while 54% of those who disagree that the Internet threatens pri-

vacy have placed orders. Cyber Dialogue E-Commerce Survey. IBM Privacy Survey at 96 (a majority of consumers on all but health sites have made a decision to not use or purchase from a Web site because of concerns regarding privacy).

21. The Commission held its first public workshop on privacy in April 1995. In a series of

22. p. 4 and accompanying notes.
23. The Commission's review of privacy has mainly focused on online issues because the Commission believes privacy is a critical component in the development of electronic commerce. However, the FTC Act and most other statutes enforced by the Commission apply equally in the offline and online worlds. Further, as described in n.21, the agency has examined privacy issues affecting both arenas, such as those implicated by the Individual Reference Services Group, and in the areas of financial and medical privacy. It also has pursued law enforcement, where appropriate, to address offline privacy concerns. *United States v. ...*, No. 99-WM-783 (D. Colo. filed Apr. 21, 1999); *...*, Docket No. 9255 (Feb. 10, 2000), *...*, No. 00-1141 (D.C. Cir. Apr. 4, 2000). This experience – as well as recent concerns about the merging of online and offline databases, the blurring of distinctions between online and offline merchants, and the fact that a vast amount of personal identifying information is collected and used offline – make clear that significant attention to offline privacy issues is warranted.
24. *...* at 7-14 (June 1998), available at < <http://www.ftc.gov/reports/privacy3/index.htm> > [hereinafter "1998 Report"]. December 1996 Staff Report at 8-12, available at < <http://www.ftc.gov/reports/privacy/privacy1.htm> > (summarizing participants' testimony on fair information practices).
25. 1998 Report at 7-11. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The U.S. Privacy Protection Study Commission, *...* (1977); Organization for Economic Cooperation and Development, *...* (1980); U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: *...* (1995); U.S. Dept. of Commerce, *...* (1995); *...* (1995); and the Canadian Standards Association, *...* (1996).
26. 1998 Report at 7-11.
27. *...* at 23, 27.
28. *...* at 42-43. In October 1998, Congress passed the Children's Online Privacy Protection Act of 1998. 15 U.S.C. §§ 6501, *...*. The Act requires that operators of Web sites directed to children under 13 or who knowingly collect personal information from children under 13 on the Internet: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of

38. A list of current participants in the TRUSTe program is available at < http://www.truste.org/users/users_lookup.html > .
39. A list of current BBB licensees is available at < <http://www.bbbonline.org/businesses/privacy/approved.html> > .
40. A list of current CPA Webtrust licensees is available at < <http://www.verisign.com/webtrust/siteindex.html> > .
41. A list of current PriceWaterhouseCoopers BetterWeb licensees is available at < <http://www.pwcbetterweb.com/betterweb/BWsitesDir/index.cfm> > . Twenty-three companies have applied for the BetterWeb seal.
42. The Entertainment Software Ratings Board (“ESRB”) Privacy Online seal program, designed for members of the entertainment software industry, was launched one year ago. A description of the ESRB program is available at < <http://www.esrb.org> > . In addition, the S.A.F.E. (Secure Assure Faith Entrusted) Dependability Seal Program was launched in October 1999. A description of this program is available at < <http://www.secureassure.org> > .
43. p. 20 and accompanying notes.
44. In this study, we define “Web site” as a domain, the unit of analysis for the Survey. Appendix A at 1.
45. A cookie is a small text file placed on a consumer’s computer hard drive by a Web server. The cookie transmits information back to the server that placed it, and, in general, can be read only by that server. For more information about cookies, < <http://www.cookiecentral.com> > .
46. “Unique visitors” refers to an estimate of the number of different individuals that visited a Web site in a particular time period, without regard to the number of visits made to or the amount of time spent at the Web site by each individual during that time period. Appendix A at 1.
47. “Adult” sites, sites that were inaccessible for technical reasons, sites directed to children under the age of 18, business-to-business sites, and sites registered to companies outside the U.S. were excluded from the Survey and the results. Appendix A at 3.
48. Information practice statements include both explicit statements describing a site’s information practices (e.g., “we will not share your personal information with third parties”) as well as statements implicitly offering consumers choice (e.g., “click here to be on our mailing list”).
49. The staff who participated in the data collection and content analysis were not involved in designing the Survey, in the subsequent data analysis, or in drafting this report.
50. There were over 5,600 such sites in January 2000, whose total unduplicated reach is 98.3%. Appendix A at n.2. That is, it was estimated that 98.3% of all active Web users visited at least one of these sites at least once in the month of January 2000.

51. As discussed in Appendix A at 7, the weighted results are not generally representative of consumers' online experiences because the population from which the Random Sample was drawn excluded sites with fewer than 39,000 unique visitors in one month. The weighted results, therefore, represent consumer experiences only on that part of the Web from which the sample was drawn.
52. Nine sites were excluded as either non-U.S. registered sites, business-to-business sites, children's sites, duplicates, or inaccessible. Appendix A at 3.
53. Sites may also collect information about consumers in ways that are less obvious to consumers, such as through cookies or through server logs that capture information about the consumer's computer. Although information collected via these "passive" means is usually non-identifying, it may be linked with personal identifying information. To determine whether Web sites were collecting personal information from consumers, the Commission's Survey looked for direct methods of data collection from consumers. It did not examine whether the sites surveyed placed cookies (which can be used to store a consumer's password or items selected for purchase in a "shopping cart," as well as to track consumers' browsing patterns), although it did ask whether sites their use of cookies. As discussed below, the Survey separately collected information on whether third parties were placing cookies at Web sites.
54. Personal identifying information includes such information as name, email, postal ad-

62. 1998 Report, Appendix D, Table 2. The difference may also be due in part to the differences in the populations surveyed. The 1998 Commission sample was drawn from a list of over 225,000 commercial Web sites. 1998 Report, Appendix A at 2. The 1999 GIPPS random sample was drawn from a list of the 7,500 busiest commercial sites. GIPPS Report at 3.

98. Appendix C, Table 4. If, under an alternative scoring model, sites were credited with Choice for providing either internal or third-party choice, 82% of sites in the Random Sample that collect personal identifying information would receive Choice credit. Further, 27% of such sites would receive credit for meeting all four fair information practice principles (compared with 20%, *_____*, p. 12), and 54% would receive credit for meeting Notice & Choice (compared with 41%, *_____*, p. 13). Appendix C, Table 10.
99. Appendix C, Table 4. If sites were credited for Choice for providing either internal or third-party choice, 98% of sites in the Most Popular Group that collect personal identifying information would receive Choice credit. Further, 63% of such sites would receive credit for meeting all four fair information practice principles (compared with 42%, *_____*, p. 12), and 87% would receive credit for meeting Notice & Choice (compared with 60%, *_____*, p. 13). Appendix C, Table 10.
100. Appendix C, Table 4.
101. 1998 Report at 9.
102. *_____*, 102. *102.*

10.

102.

1

113. Many Committee members also agreed that Access is an important framework for addressing data inaccuracies. Advisory Committee Report at 8-14 (describing four options for implementing Access, each of which takes into account the importance of correcting data inaccuracies).
114. 1998 Report at 10. Advisory Committee Report at 22-23, 26.
115. Advisory Committee Report at 19.
116. . at 26.
117. Advisory Committee Transcript of February 4, 2000, at 127 (S. Baker, Steptoe & Johnson), available at < www.ftc.gov/acoas > ; . at 128 (T. Gau, America Online, Inc.).
118. See Section III, below.
119. Advisory Committee Report at 20-21. As the Committee noted, sites that do not disclose anything about security may in fact be providing security measures. . at 20.
120. . at 20.
121. . at 20-21.
122. Business Week/Harris Poll. Eighty percent of Internet users stated that they would be encouraged to use the Internet more in general, 69% to register at a site, and 73% to

136. Appendix C, Table 15a.
137. .
138. To determine whether third-party cookies observed during the online phase of data collection for the Survey were sent by network advertising companies engaged in profiling, Commission staff reviewed the completed Third-Party Cookie Survey Forms, Appendix B, and visited the Web sites associated with the domains of the observed cookies. Only companies whose Web sites explicitly stated that the company targeted banner ads on the basis of consumer characteristics were classified as "profilers." Appendix A. The vast majority of these companies are members of the Network Advertising Initiative (NAI), an industry group that has been working to create a self-regulatory program for network advertising companies that collect information about consumers. As noted above, the Commission will soon address online profiling in a separate report to Congress.
139. Appendix C, Table 15b.
140. .
141. , B E WEE , Mar. 20, 2000, at 86-87; CNET News; T E L D S A DA D, Mar. 13, 2000, at 208-09; C E RE , May 2000, at 43, 47.
142. Jupiter Communications, Inc., : 64 (Aug. 17, 1999), press release available at < <http://www.jupitercommunications.com> > .
143. Such pre-checked boxes were deemed to provide opt-out choice, as they require an affirmative act by the consumer – unchecking the box – in order to prevent the further use of the information.
144. Notice of Establishment of the Federal Trade Commission Advisory Committee on Online and Access and Security and Request for Nominations, 64 Fed. Reg. 71,457 (1999), available at < <http://www.ftc.gov/acoas> > [hereinafter "Establishment and Nomination Notice"]. The FACA applies to groups, such as this one, established by a government agency that include non-federal members, involve deliberation among the group's members, and provide advice or recommendations as a group to the agency. 5 U.S.C. App. § 3; 16 C.F.R. § 16.2; , 997 F.2d 898, 913-14 (D.C. Cir. 1993).
145. Charter of the Federal Trade Commission Advisory Committee on Online Access and Security, available at < <http://www.ftc.gov/acoas/acoascharter.htm> > [hereinafter "Charter"].
146. Establishment and Nomination Notice at 71,459; Charter.
147. Establishment and Nomination Notice. The Commission received approximately 190 nominations from highly qualified individuals. The complete list of nominees is available at < <http://www.ftc.gov/acoas/nominations/index.htm> > .

148. The members included representatives from online businesses, computer security firms, database management companies, privacy and consumer groups, and trade associations, as well as academics, experts in interactive technology, and attorneys. The complete list of members is available at < <http://www.ftc.gov/acoas/acoasmemberlist.htm> > .
149. Shortly after each meeting, a complete transcript of the meeting was posted on the

167. . at 11.
168. .
169. . at 11-12.
170. . at 12.
171. .
172. . at 13.
173. . at 14.
174. . at 6-8.
175. . at 7.
176. .
177. .
178. . at 16.
179. . at 15.
180. .
181. . at 21-26.
182. .
183. . at 19.
184. Advisory Committee Transcript of February 4, 2000, at 127 (S. Baker, Steptoe & Johnson), available at < www.ftc.gov/acoas > ; . at 128 (T. Gau, America Online, Inc.).
185. Advisory Committee Report at 26. The Advisory Committee presents five options before making its recommendation. These options are 1) rely on existing remedies; 2) require that Web sites maintain a security program; 3) rely on industry-specific security standards; 4) require security procedures that are "appropriate under the circumstances;" and 5) establish a sliding scale of security standards. . at 21-26.
186. . at 26.
187. . at 25.
188. Section II.B.4 .
189. Advisory Committee Report at 19. The Report also states that notice is important in triggering one of the few available enforcement mechanisms for ensuring adequate security online – an FTC action for deceptive trade practices. . at 20.
190. . at 20.
191. .

204. , , Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6502(b) (directing Commission to issue rules to implement statutory requirements).



or unfounded fears of new technology? Is it the online dissemination of personal information or the offline availability of such information? How is the proposed solution related to the problem? Why is law enforcement against violations of posted privacy policies inadequate? Why not encourage consumers to “vote with your mouse”? In light of the widespread adoption of privacy policies and developments in privacy protection technology, consumers can choose to make purchases at sites compatible with their privacy preferences and not use sites that are incompatible with their preferences. Consumers who feel very strongly about privacy can use technological tools to further enhance their privacy online, such as anonymizer programs or cookie crumblers, and may simply rely on information available online to make an offline purchase.

Isn't the real privacy problem the lack of information and education? This can be addressed by self-regulation. Legislation is not necessary.

I. WHAT DO THE SURVEY RESULTS SHOW?

A. The Survey Shows Continued, Significant Progress in the Frequency of Privacy Disclosures

It is critical to recognize what the majority's Report does and does not do. First, it presents a survey that is a one-time snapshot of the characteristics of privacy disclosures provided online in late February 2000. The survey results show noteworthy progress on two measurements that are directly comparable to similar figures from surveys described to Congress in the Commission's 1998 and 1999 reports on online privacy: the posting of privacy disclosures (or information statements) and the posting of privacy policies. The first set of these comparative figures, displayed in Figure 1 of the Privacy Report, shows that 88% of Web sites in the Random Sample post at least one privacy disclosure and that 100% of the Most Popular Web sites post at least one privacy disclosure. (PR at 10, Appendix C, Table 2a). These figures rose to 66% and 93% respectively last year, up from 14% and 71% respectively in 1998. (PR at 11, Figure 1). The second set of comparative figures shows that fully 62% of Web sites in the Random Sample and 97% of the Most Popular Web

sites post a privacy policy. (PR at 10). This also shows noteworthy progress from comparable 1999 figures of 44% and 81%. (.).

B. The Survey Provides a Unique Baseline for Measuring the Quality of Privacy Disclosures

manner also increases the number of sites that meet the 2000 Survey's full FIPPs standard to 27% (Random Sample) and 63% (Most Popular). ().

II. PROBLEMS WITH THE REPORT'S INTERPRETATION OF SURVEY RESULTS

A. The Report's Direct Comparisons to Earlier FIPPs Numbers Are Bogus

Regardless of the manner in which the qualitative measures of Notice, Choice, Access, and Security are combined or separated, the FIPPs figures from the 2000 Survey stand alone and are beyond the scope of earlier surveys. The Privacy Report's repeated comparison of full FIPPs numbers of 20% of the Random Sample and 42% of the Most Popular Group to what it calls "similar figures" of 10% and 22% from Professor Culnan's 1999 surveys is a misleading

actually given credit for the majority's concession that in some cases "reasonable Access" might mean "no Access," the Access and full FIPPs numbers would be dramatically improved.

Moreover, as discussed below in section III.C.4, Access and Security disclosures do not reflect whether a Web site actually provides Access and Security.

C. Equating Self-Regulatory Enforcement with the Prevalence of Seal Programs Is Misleading

Another striking feature of the Privacy Report is that, without analysis, it equates seal programs with enforcement and concludes that self-regulation has failed because the results of this first-time survey of the prevalence of participation in seal programs show that 8% of Web sites in the Random Sample and 45% in the Most Popular Group display privacy seals. The weighted analysis figure, which reflects how often consumers surfing the Random Sample Web sites are likely to encounter a privacy seal, is 36%. (PR Appendix C, Table 14a). Despite the fact that nearly one-half of the most frequently visited sites use a seal program, the Report states flatly that "the enforcement mechanism so crucial to the success and credibility of self-regulation is *absent*." (PR at 35) (emphasis added).

Moreover, the FTC already has power to take action against violations of privacy policies. The Privacy Report does not comment on the FTC's challenges to privacy policies that violate Section 5 of the FTC Act and how often such government enforcement actually has been needed.

Once again, the Privacy Report fails to ask "why?" Instead of considering why participation in seal programs is more than five times higher among the Most Popular Web sites than among the Random Sample sites, the majority simply concludes that the presence of seal programs on the Web is "not significant." (PR at 6). Nowhere does the Report discuss the costs of participating in a seal program, such as fees charged by the program, the time involved in applying and being granted approval to use a seal, and the costs of implementing seal program requirements. Nor does the Report ask whether the prevalence of seal programs may reflect how frequently consumers seek out and rely on privacy seals before purchasing from an online retailer, or whether seal programs may have positive effects on online privacy by

indirectly encouraging Web sites not participating in seal programs to adopt privacy policies to better compete with sites that are. Instead, it leaps to the conclusion that the number of sites displaying seals means that enforcement is lacking and that government enforcement of new privacy regulations is the solution.

D. The Report Confirms the Exponential Growth in Online Commerce, but Misuses Consumer Confidence Surveys and Lost Sales Projections

The Privacy Report seeks to justify legislation and regulation on the ground that privacy concerns are limiting the commercial growth of the Internet. It does acknowledge the exponential growth that has occurred in recent years in the online economy. But it also boldly asserts that consumer fear about privacy “likely translates into lost online sales due to lack of confidence in how personal data will be handled” (PR at 2), and concludes that government intervention will reduce such lost sales. There is little empirical support for these conclusions.

1. Misuse of Consumer Confidence Surveys

Not surprisingly, the attention paid by the media and government to online privacy concerns is reflected in consumer surveys showing a general lack of confidence in online privacy protections. The Privacy Report, however, overstates the extent and significance of consumer concern about online privacy to support its call for government regulation. (PR at 2).

a. Odyssey Study Example

For example, the Privacy Report states that there is “consumer unease” about online privacy based on a “recent study [by Odyssey] in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential, and 82% agreed that the government should regulate how online companies use personal information.” (PR at 2). The Odyssey Study itself states that 47% of online households strongly agree, 35% somewhat agree, and 18% strongly disagree with the statement that government regulation is needed. The majority has arrived at its 82% figure by adding

¹ Odyssey, “Odyssey Study” at 2. (2000)

positive response any consumer who has ever been dissuaded from making any purchase online from the relevant type of Web site. Positive responses therefore include consumers who may well have simply decided to make their online purchase from some other online retailer, thereby resulting in no lost online sale at all. Positive responses thus also include consumers who may well have been dissuaded from making a purchase in the relatively distant past but are now undeterred from making purchases online, which means that the responses could very well overstate the risk of current and future lost sales online due to privacy concerns. In fact, these results suggest that many consumers want information about privacy practices and that consumers can and do exercise choice based on their privacy preferences.

2. *The Report's Reliance on Lost Sales Projections Is Misplaced*

Nor are the lost sales projections relied upon by the majority valid justifications for government regulation of privacy. The Report's sweeping statements about consumer privacy fears likely resulting in billions of dollars of lost sales are based primarily on two consumer surveys conducted in mid-1999 or earlier. These surveys were the basis for estimates that sales lost to lack of consumer confidence in privacy protections were \$2.8 billion in 1999 and could be as much as \$18 billion by 2002.

i. Forrester Privacy Best Practice Report

The Privacy Report obtained the \$2.8 billion estimate from a study that Forrester Research, Inc., released in September 1999. (PR at 2 n.16). The Forrester Report stated merely that "concerned consumers who buy spend 21% less online than their more at-ease counterparts, leaving \$2.8 billion on the table in 1999." It did not explain, however, how

The question in the IBM Privacy Survey asked: "When you've visited health, financial, insurance, or retail websites, have you EVER DECIDED NOT TO USE OR PURCHASE SOMETHING from this type of website because you weren't sure how they would use your personal information?" IBM Multi-National Consumer Privacy Survey (Oct. 1999), prepared by Louis Harris & Associates, Inc. at 96, 99 (Exh. 5.1) (emphasis added) (capitalization in original).

Christopher M. Kelley, et al., *Privacy: A Consumer's Guide*, The Forrester Report (Sept. 1999) at 2.

this estimate was calculated, much less reveal the underlying data on which its estimate was based. In fact, the 21% figure was based on what this group of consumers reported spending during the three-month period prior to the survey. Forrester has not updated these data for 2000. The Forrester lost sales projection therefore does not reflect changes that have occurred in online commerce since mid-1999.

Study.⁴ That study provides the full scenario underlying the \$18 billion lost sales projection. The projection rests on four assumptions: (1) the online “[i]ndustry does nothing”; (2) “[c]onsumers’ concerns [about Internet privacy] grow” as media attention increases; (3) the “Government implements legislation” signaling to consumers that their concerns regarding privacy were justified; and (4) “[c]onsumers’ fear impacts revenue.”

Thus, the majority is relying on a projection of lost sales that is based on one assumption already proven wrong by the 2000 Survey — that industry does nothing to protect privacy — and another assumption — that the government regulates privacy — that has not yet come to pass. The Privacy Report’s use of Jupiter’s lost sales projection as the basis for recommending such legislation is indefensible.

In fact, the Jupiter Study appears to have used the projection to encourage self-regulation. That Study also concluded that “consumers do not see government regulation as the solution to the online privacy issue. The vast majority of respondents to a Jupiter Consumer Survey — 86 percent — said that they would not trust a Web site with their privacy even if the government regulated it.” The Jupiter study also found that only 14% of consumers asked to identify the top two factors that would positively affect their trust in Web sites with regard to their privacy “indicated that they would more likely trust a Web site on privacy issues if the site were subject to government regulation.” These figures clearly cut against the Privacy Report’s recommendation for rulemaking.

⁴Michele Slack, Jupiter Communications, *Jupiter Study* (June 1999).

⁵Jupiter Study at 12-13 and Figure 9 (emphasis added).

⁶Jupiter Study at 16.

⁷Id. at 19.

⁸Id. at 4.

suggests that many consumers do not act upon their fears or that they have generalized fears that are overcome by the provision of additional information by the sites with which they choose to do business. In fact, some of the studies cited by the majority's Privacy Report confirm that consumers' fears about privacy are mingled with fears about the security of their credit card information. The Jupiter Study, for instance, reports that 78% of consumers surveyed stated that security of credit card information is the privacy issue that concerns them the most. Current encryption standards provide a lot of protection in this area, and it is probably less risky to use a credit card online than to use it in a restaurant or over the telephone. If consumers' fears about security are exaggerated, then the solution is to find a way to reassure consumers by notice and education rather than promulgating rules that may restrict their choices.

III. WHAT DOES THE REPORT FAIL TO DO?

The Privacy Report fails to provide a reasoned basis for its legislative recommendation. As discussed above, it relies only on a one-sided interpretation of the 2000 Survey results and the existence of consumer concern about privacy. The Report fails to adequately address the alternatives to legislation. Its discussion of self-regulation does not give appropriate credit to self-regulatory efforts other than seal programs, nor does it address the continued development of privacy-related technology.

Most fundamentally, the Privacy Report fails to pose and to answer basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could severely stifle the New Economy. Shockingly, there is absolutely no consideration of the costs and benefits of regulation; nor the effects on competition and consumer choice; nor the experience to date with government regulation of privacy; nor constitutional implications and concerns; nor how this vague and vast mandate will be enforced.

Respondents were asked to choose the top three factors that most concerned them. Jupiter Study at 3-4.

news release — seen by more than four million Americans — on protecting privacy while shopping online for Christmas.

The American Electronics Association (“AEA”) sponsored a series of seminars in January 2000, entitled “E-Commerce Privacy: Building Customer Trust.” AEA has established a significant business relationship with BBBOnline in which a significant discount is offered to its 3,400 member companies who gain certification under BBBOnline’s strenuous online privacy program.

The Direct Marketing Association (“DMA”) Privacy Promise was successfully launched on July 1, 1999. Under DMA’s Privacy Promise program, its members commit to provide customers with notice of their right to opt out of information exchanges, honor opt-out requests, maintain an in-house file of consumers who have asked not to be recontacted, and use DMA’s mail and telephone do-not-call lists when prospecting. DMA membership is contingent on compliance with the Privacy Promise. Fewer than 1% of DMA members refused to comply. More than 2,000 DMA member companies signed up, making this the largest self-regulatory program based on numbers of participants. DMA has revised its Privacy Policy Generator to reflect the most current issues, making it easier for companies to explain to consumers their access policies, their enforcement programs, and their relationship with ad servers.

In April 2000, the Association for Competitive Technology (“ACT”) unveiled “Net Privacy: You’ve Got the Power,” a multi-faceted campaign designed to educate consumers on how to protect their privacy online. The campaign was launched with public service advertisements educating readers about online privacy and directing them to www.NetPrivacyPower.org. In addition to the Web site, the campaign includes print advertising, online advertising, direct mail and email.

The U.S. Chamber of Commerce continues to reach out through a variety of

robust online privacy practices. The Chamber has worked closely with OPA and NetCoalition to educate trade associations not in the information-technology area regarding the need for their

preferences in sharing personally identifiable information with Web sites, there are many other privacy products.

Those tools can be divided into two types: those that protect or shield a browsing consumer's identity, and those that help the consumer negotiate what information her or she wishes to share. Anonymizer technology like anonymizer.com and Zero Knowledge Systems give a consumer anonymity on the Web. Infomediaries allow a consumer to exercise choice in the types of personally identifiable information that is shared each time a Web site is visited. A consumer can create a personal profile that enables the technology to negotiate the release of information specified by the consumer.

For example, AllAdvantage.com acts as an agent on behalf of consumers to create a market for the use of their information without consumers' losing control over their information. Digital Me from Novell stores a consumer's personal information and uses it to automatically fill out forms at Web sites, allowing the consumer to review what is being submitted. Persona by Priva Seek allows a consumer to surf anonymously and sell his or her specified, personally identifiable information in exchange for discounts.

1. *Notice*

Notice seems less likely to impose tremendous costs and may have many benefits. The 2000 Survey results show that Notice already is widely provided, but there appear to be problems with the clarity and understandability of privacy disclosures. (PR at 24-28). To the extent that Notice is clearly provided, firms can compete on the basis of their privacy policies, and the privacy preferences of one group of consumers need not limit the choices of other groups. Industry adherence to a set of best practice guidelines for Notice should be attempted and assessed before we resort to legislation. To the extent that online companies do not provide clear notice, consumers who care about privacy should shop elsewhere. The workings of the market are preferable to the workings of government.

2. *Choice*

As described in the 2000 Survey and the Privacy Report's legislative recommendation, Choice is not the free-market version of choice that relies on informing the consumer so that the consumer can choose not to use a site if he or she dislikes the privacy policy. Rather than promoting informed comparison shopping for acceptable privacy practices, the Commission asks Congress to impose a mandated version of Choice that appears to entitle the consumer to continue to use any site, but gives the consumer control over the site's internal and external uses of his or her personal information. (PR at 36).

Like other aspects of the Commission's recommendation, Mandated Choice raises policy issues that the Report simply ignores. What are the likely effects on online commerce of Mandated Choice? Would sites have to extend the same level of services and benefits to all consumers, regardless of whether some are unwilling to provide information? To the extent sites rely on the sale or use of information to offset the costs of providing services, would they discontinue services to all or to some consumers? Would all consumers have to pay more for services previously offset by the sale or use of information? Could sites shift costs only to those consumers who demand a higher level of privacy, whether in the form of fees for using the site or by reducing the level of benefits and services offered to those who choose a higher level of

privacy? Or is privacy an absolute right so that all participants in online commerce — retailers and consumers — should bear the costs of Mandated Choice exercised by some consumers? If so, in the name of “Choice,” this legislation may reduce the choices available to consumers in the online market.

These are fundamental policy decisions, not mere issues of implementation that can be resolved later when unelected bureaucrats decide how to regulate the online world. Legislation adopting Mandated Choice will have consequences for online commerce that should be understood before Mandated Choice is written into law.

3. Access

The majority recommends that Congress enact legislation requiring all commercial, consumer-oriented Web sites to provide reasonable access to consumers’ personal information. Again, the majority does not ask why the 2000 Survey’s Access numbers are not as high as the majority evidently expected them to be. As the Advisory Committee found, sites may actually provide Access yet not specifically address it in a notice. (Advisory Committee Report at 4). For example, access may be provided by e-mail to information about what the customer ordered, its price, and where it is to be delivered. The 2000 Survey did not count this type of access unless it was described in a privacy disclosure. Nor did the 2000 Survey take account of the type or sensitivity of information collected by sites that fail to provide Access. To the extent that the majority may be prepared to treat “reasonable Access” as “no Access” under some circumstances, it is noteworthy that the 2000 Survey gave no credit for “no Access.”

The Advisory Committee’s report discusses the costs and risks of Access, particularly the problem that “the access principle sometimes pits privacy against privacy. . . . Privacy is lost if a security failure results in access being granted to the wrong person.” (Advisory Committee

Interestingly, the Advisory Committee “heard estimates from Web companies that less than one percent of customers who are offered access actually take advantage of the offer.” Concurring Statement of Stewart Baker, Steptoe & Johnson LLP, appended to Advisory Committee Report.

Advisory Committee members that the government should mandate security standards or that the Commission should be setting security standards.

5. *Competitive Effects*

This Report is from the leading antitrust agency, yet it contains no consideration of the competitive effects of the remarkably broad legislation it proposes. The Report ignores the likely result that government-created standards for all consumer-oriented, commercial Web sites may cause some online companies, particularly smaller ones, to limit their online services or exit the online marketplace altogether. What are the likely effects of the majority's proposed legislation on consumers and competition? Will the advantages of the bigger players be enhanced, while small entrepreneurs face artificial and costly barriers to entry? How will that affect the innovation and provision of services that consumers want? What costs will it impose on consumers who do not care about privacy or are willing to make some tradeoffs?

6. *Constitutional Issues*

The Privacy Report does not address the fundamental question whether a statute that incorporates its recommendations would violate the First Amendment to the United States Constitution. The majority recommends that the Congress impose broad restrictions on the sale to a third party of personal information collected online by any consumer-oriented commercial Web site. (PR at 38). Both the courts and the Commission have recognized that sales of personal information to third parties are accorded the same level of Constitutional protection as "commercial speech." *National Endowment for the Arts v. Finley*, 472 U.S. 749, 758-59 (1985) (plurality opinion); *FTC v. Actavis*, FTC Dkt. No. 9255, slip op. at 33-37 (Feb. 10, 2000). To determine whether a government restriction on commercial speech passes constitutional muster, a court must examine: (1) whether the expression at issue concerns lawful activity and is not misleading; (2) whether the asserted governmental interest supporting the restriction is substantial; (3) whether the regulation directly and materially advances the

Concurring Statement of Stewart Baker, Steptoe & Johnson LLP, appended to Advisory Committee Report.

harbor program that relies on the creativity of industry to come up with self-regulatory guidelines that satisfy the requirements imposed by statute.

8. Offline Privacy

As Commissioner Leary thoughtfully explains in his concurring and dissenting statement appended to the Privacy Report, online regulation of privacy has implications for the offline world. The Privacy Report acknowledges, but does not analyze, the issue in an ominously vague footnote promising that “significant attention to offline privacy issues is warranted.” (PR at 3 n.23).

IV. WHERE DO WE GO FROM HERE?

The Privacy Report stands as the majority’s “justification” for the recommendation to legislate privacy — a dramatic reversal in position for the Commission and a mandate for the commercial online world to comply with the government’s interpretation of all four fair information practice principles. Yet the Report is extremely flawed in its presentation of fact, its analytical logic, and its conclusions. This is no way to create good law.

Everyone recognizes that there are imperfections and deficiencies in the state of privacy on the Internet, but let us not make the search for the perfect the enemy of the good. The private sector is continuing to address consumer concerns about privacy, because it is in industry’s interest to do so. Congress may wish to enact more limited legislation or may continue to rely on enforcement agencies and corporate leadership. Now is not the time for legislation, but if legislation cannot be avoided, then a basic standard for a readily understandable, clear and conspicuous Notice — combined with a campaign by industry and government to continue to educate consumers about the tools at their disposal — would go a long way to protect consumer privacy by ensuring that consumers could compare privacy policies and make informed choices based on their privacy preferences. If there is to be legislation, it should go no further than Notice. In light of the 2000 Survey’s positive findings about the broad-based implementation of Notice by Web sites, mandating Notice seems less likely to be fraught with severe, unintended consequences for online commerce. Notice allows consumers to exercise informed choice to

use a particular Web site or to seek an alternative.

The current recommendation, however, defies not just logic but also fundamental principles of governance. In recognition of some of the complexities of regulating privacy — particularly Access and Security — the Commission asks Congress to require all commercial consumer-oriented Web sites to comply with extensive, yet vaguely phrased, privacy requirements and to give the Commission (or some other agency) a blank check to resolve the difficult policy issues later. This would constitute a troubling devolution of power from our elected officials to unelected bureaucrats.

I dissent.



scenarios. For example, the most popular sites generally have more comprehensive disclosures, and this could mean that some consumers favor them because of the disclosures. The fact that gains are modest overall, however, may also indicate that consumers are not quite as fixated on privacy issues as might appear from the public opinion polls cited in the Report. Marketers generally know more about consumer demand than regulators do.

Marketers know, for example, that consumers' actual buying habits are not necessarily consistent with their expressed preferences. Their stated interest in various ancillary protections like privacy may fade or become more nuanced, once they learn more about them and realize that there are costs attached. Consumer opinion on privacy issues appears to be a complex subject, and public opinion polls simply do not provide an adequate predicate for a legislative recommendation of the scope contained in the Report.

There Is a Need for Better Disclosures

There is one aspect of the 2000 Web Survey, however, that I find particularly disturbing. The Survey results do show a steadily rising trend in the number of companies that address privacy, one way or another, but we cannot therefore conclude that consumers are better informed today or would be even better informed if the numbers rose even further. In fact, a site's mere mention of privacy may lead to a misperception that the consumer's privacy is well-protected, and a plethora of varying and inconsistent privacy claims could add to consumer confusion. The Survey tells us that the scope of the disclosures varies widely (Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress ("Report") at 38-44) and, in my view, vendors and their customers would both benefit from a legislative initiative to require disclosures of greater clarity and comparability.

Market processes, supplemented by traditional remedies against consumer deception, should ultimately provide the most appropriate mix of disclosures and substantive protections,

Jupiter Communications, \ : \ , at 3-7 (June 1999).

but these forces sometimes work slowly and I am convinced that privacy concerns have some special characteristics that make it prudent to prompt the market to work more rapidly. Some standardization of the disclosures would allow consumers to compare more easily the privacy practices of different vendors. As we learned when considering environmental marketing claims, for example, varied and inconsistent claims lead to consumer confusion. Consumers may not be able to recognize valid and invalid comparisons when they are dealing with unfamiliar concepts. When terms have uniform meaning and basic equivalent information is disclosed for each site, the marketplace should work more efficiently.

Although consumers' knowledge and understanding of these issues is steadily increasing, it still has a long way to go. Not only is the Internet a recent invention, consumers are just beginning to become aware of the potential for data collection both online and offline. Consumers still do not know much about the possible uses of their personal information (and new ones are invented every day), the ramifications of permitting its use, and the costs associated with limiting its dissemination. Because an efficient market presupposes full and accurate information, it is appropriate to mandate more extensive privacy disclosures.

Privacy concerns also differ from concerns about product attributes that consumers may value. An uninformed decision to deal with a vendor that disseminates personal information could have ramifications for years to come, and that decision cannot be retracted. The marketplace may ultimately discipline the less-than-candid vendor, but the potential consumer harm will continue because the personal information may have spread and cannot be retrieved. The privacy loss and consequent harm results from mere participation in the market, with insufficient notice, not from a bad purchase decision. By contrast, if consumers are uninformed

Guides for the Use of Environmental Marketing Claims (the "Green Guides"), 16 C.F.R. pt. 260 (1999). When the Commission requested public comment on these Guides three years later, commentators generally agreed that they benefit both consumers and industry, *inter alia*, by promoting consistency and accuracy in claims, helping consumers to make accurate decisions, and thereby bolstering consumer confidence. Guides for the Use of Environmental Marketing Claims, Final Rule, 61 Fed. Reg. 53,311 (1996).

about particular product attributes, and regret the purchase, the damage may at most be limited to the value of the purchase.

I therefore agree with the Report insofar as it recommends a legislative prod to ensure better disclosures. Thereafter, I part company.

The Report's Proposal Is Too Broad

The Report's recommendation is framed around the so-called "fair information practices" of notice, choice, access, and security. Notwithstanding references to the need for flexibility (, , , Report at 60-61), the overall thrust of the Report is that any privacy policy should, at a minimum, recognize substantive consumer rights in each of these areas. What the Report does not do is adequately explain why.

In addition to its expertise on consumer disclosures, the Commission is supposed to have some expertise in the operation of competitive markets -- when they are likely to succeed and when they are likely to fail. The Report does not explain why an adequately informed body of consumers cannot discipline the marketplace to provide an appropriate mix of substantive

contrary, and there is no indication that the principles are widely accepted in the offline world either. I would not be so quick to conclude that we are right and so many others are wrong.

The Report not only fails to explain why adequate disclosures are insufficient, it passes too lightly over issues of complexity. Granted, these are issues more appropriately addressed in a rule-making proceeding, but Congress needs to have a better understanding of what we mean when we ask for authority to set "reasonable" standards. For example, the Report recognizes that "access" is a complicated matter and indicates that any determination of what is "reasonable" should be informed by the discussion of the Advisory Committee on Access and Security (Report at 30-31, 61). At the same time, however, the Report endorsed by the majority states flatly that "the Commission believes that fair information practices require that consumers be afforded an opportunity to review, discuss, and modify the information that is collected about them, to delete inaccurate information, to suppress or limit disclosure of their information, and to correct or amend existing information." (Report at 30-31, 61). At the same time, however, the Report endorsed by the majority states flatly that "the Commission believes that fair information practices require that consumers be afforded an opportunity to review, discuss, and modify the information that is collected about them, to delete inaccurate information, to suppress or limit disclosure of their information, and to correct or amend existing information." (Report at 30-31, 61).

The Report does recognize (Report at 25) that notice is “the most fundamental of the fair information practice principles,” but it recognizes it for the wrong reason. Notice is not fundamental “because it is a prerequisite to implementing other fair information practice principles, such as Choice or Access” (.); it is fundamental because it helps the marketplace accurately to reflect consumer preferences with respect to the other principles. Consumers, so long as they are informed by clear and conspicuous disclosures, will be able to select the vendors that give them the privacy protections they want and are willing to pay for.

The Report’s Proposal Is Too Narrow

I also disagree with the Report’s legislative recommendation to the extent that it treats issues of online privacy as wholly different from offline privacy. At times the Report acknowledges the existence of offline privacy concerns and the erosion of the distinction between online and offline commerce (Report at 8 n.26, 55 n.196), but it justifies special treatment of Internet privacy on the ground that the technology of the Internet has “enhanced the ability of companies to collect, store, transfer and analyze vast amounts of data[.]” (Report at 1).

Of course, some privacy issues are particular to the Internet. This new technology has permitted uniquely invasive tracking of consumer preferences by recording not just purchases, but consumers’ movements on the Internet as well. This practice of tracking, including third-party profiling, may be particularly threatening and distasteful to many. (Report at 37-38, discussing so-called “cookies”). Any legislative or regulatory scheme can and should ensure that consumers are adequately informed about these Internet capabilities.

However, the majority’s recommendation is not focused on the special characteristics of e-commerce or on particular categories of sensitive information collected online. Instead, the majority would apply the fair information practice principles to any personal information collected by any commercial web site, even though the identical information can be collected

collection, in order to provide potential customers with the most personalized message possible. Already, companies are seeking to merge data collected offline with data collected online.⁴ In light of this reality, the majority's recommendation would result in perverse and arbitrary enforcement. Enforcement actions would depend on the source of and method used to collect a particular piece of consumer data rather than on whether there was a clear-cut violation of a company's announced privacy policy or mandated standards.

Finally, the Report's focus only on online privacy issues could ultimately have a detrimental impact on the growth of online commerce, directly contrary to the Report's objectives. It is clear from the Advisory Committee's Report on Access and Security and from limited portions of the Commission's own Report that implementation of the fair information practices will be complex and may create significant compliance costs. Online companies will be placed at a competitive disadvantage relative to their offline counterparts that are not forced to provide consumers with the substantive rights of notice, choice, access and security. Traditional brick and mortar companies that have an online presence or are considering entry into the electronic marketplace will be forced to assess how the cost of regulation will affect their participation in that sector.

A better approach would be to establish a level playing field for online and offline competitors and to address consumers' privacy concerns through clear and conspicuous privacy disclosures. Any privacy concerns that are unique to a particular medium or that involve particular categories of information (however collected) can continue to be addressed through separate legislation.

The Report's recommendation limits itself to online privacy for reasons that seem primarily historical. The Commission first looked at the online world at a public workshop in 1995,

⁴ Dana James, *Privacy in the Digital Age*, Marketing News, Feb. 14, 2000, at 15.

note 10.

these informational products, the information at issue was primarily collected offline. Finally, just last week, the Commission issued its final rule implementing the privacy provisions of the Gramm-Leach-Bliley Act, a rule that focuses on the treatment of consumer information by financial institutions -- again without regard to how the information was collected.

Even if the Commission majority, who endorse the Report, determined that our experience was insufficient to assess offline privacy concerns, a better course would have been to invite further Congressional inquiry. As it is, the Report's advocacy of legislation limited to the online world suggests that public remedies should be bounded by the scope of the studies we have chosen to conduct. This is thinking upside down.

Existing Remedies Should Be Actively Pursued

Legislation to mandate more comprehensive and clear privacy disclosures should ensure in the long run that the marketplace provides consumers with their desired level of privacy protection. Legislation and rule-making may take considerable time, however, and in the interim some consumers may suffer long-lasting harm because they have not been adequately informed about privacy issues. In order to reduce these potential harms, I would recommend that the Commission take some immediate steps.

First, the Commission should more actively employ its existing authority under Section 5 to prohibit unfair or deceptive practices. We can not only challenge outright violations of express privacy policies, but also challenge policies that deceive because they impliedly offer more protection than they deliver. As noted earlier, although the Survey results demonstrate an increase in the number of privacy disclosures, they also indicate that these disclosures often involve inconsistent or confusing claims. (Of course, enforcement actions should only be brought in cases of clear-cut deception, so that companies which attempt in good faith to

Privacy of Consumer Financial Information, ___ Fed. Reg. ___ (2000) (to be codified at 16 C.F.R. pt. 313).

_____, No. 00-0032 (D.D.C. Jan. 6, 2000);
FTC Dkt. No. C-3849 (Feb. 12, 1999).

provide information, up to now on a voluntary basis, would not be chilled from doing so.) Stepped-up enforcement in this area, as elsewhere, serves a double purpose: it addresses specific situations and sends a message both to consumers and businesses.

Beyond this, the Commission should redouble its efforts to educate consumers directly about the benefits and potential risks associated with the collection and dissemination of their personal information. Without additional authorization, we can help consumers to better understand the meaning of various privacy disclosures. Informed consumers will ultimately be

A **A:**
T **I**

statistical methods.⁴ All “.com” domains with at least 39,000 unique visitors were selected and ranked in order of audience size. This list served as the sampling frame for the Random Sample. Accordingly, results from the Survey of the Random Sample can only be generalized to this population of Web sites, and not to the entire universe of “.com” domains. The busiest 100 sites on the Nielsen//NetRatings list (excluding certain sites, as discussed below) constituted the Most Popular Group.

B. CREATION OF REATIONOREATION

the replicates and thus were included in the Random Sample.

A similar procedure was used to create replicates for the 100 sites in the sampling pool for the Most Popular Group. Specifically, ten replicates with ten sites per replicate were created.

C. FINAL SAMPLES

Once replicates had been created, the final sample was achieved as follows. First, each of the 100 sites in the Most Popular Group was surfed. Next, for the Random Sample, one of the 54 replicates (containing 15 or 16 sites) was chosen at random, and all sites on the replicate were examined by a Committee staff member (“surfed”). This procedure was repeated until the number of sites surfed exceeded the target sample size. Once a replicate had been selected, all sites on that replicate were surfed.

At this stage, some sites were excluded from the Survey for one of three reasons: they were “adult” (. . . , pornographic) sites, they were sites primarily directed to children 12 and under, or they were inaccessible. Forty-five sites were excluded for these reasons. Once the data collection described below was completed, additional sites were excluded from both samples. First, all foreign sites were excluded. Second, all sites primarily directed to other businesses as opposed to consumers (. . . , business-to-business sites) were excluded. ⁴ Finally, certain duplicate sites were excluded. Altogether, 50 sites were excluded as foreign, business-to-business, or duplicates. The following chart sets forth the number of sites in the sampling pool and final sample for both the Random Sample and the Most Popular Group.

Sample	# of Sites in Sampling Pool	# of Sites Excluded	# of Sites in Final Sample
Random Sample	421	6	335
Most Popular Group	100		1



B. THIRD-PARTY COOKIES

All sites not excluded by the surfers were then examined for third-party cookie placement by six Commission interns ("cookie surfers") using two dedicated computers whose cookie cache had been cleared prior to the project. The browsers on the computer were set to notify the user if a cookie was being placed. The interns each underwent a half day's training on how to ascertain whether a third party was attempting to set a cookie on a site and how to complete the third-party cookie questionnaire. Each cookie surfer was randomly assigned sites from the samples to visit. If a cookie alert indicated that a domain other than that listed on a replicate was attempting to set a cookie, the third-party cookie questionnaire was answered in the affirmative and the cookie surfer noted the URL of the domain on the questionnaire. In the event that no third-party cookie was found, a second cookie surfer would check the site to ensure the accuracy of data.

To determine whether third-party cookies observed during the online phase of data collection for the Survey were sent by network advertising companies engaged in profiling, Commission staff reviewed the completed third-party cookie survey forms and visited the Web sites associated with the domains of the observed cookies. Only companies whose Web sites explicitly stated that the company targeted banner ads on the basis of consumer characteristics were classified as "profilers."

C. CONTENT ANALYSIS

A third group of 17 Commission staff served as content analysts who reviewed the privacy disclosures of those sites that had such disclosures (either a privacy policy or an information practice statement). The content analysts underwent four half-days of training in the use of the



weighted analysis represents the proportion of all unique site visits to the most heavily-trafficked sites that were made to sites that post privacy policies.

It is important to note that the population from which the Random Sample was drawn excluded sites with fewer than 39,000 unique visitors in one month. Thus, the weighted results represent only the likelihood that a consumer surfing only sites with 39,000 or more visitors per month will encounter a particular practice. The weighted results represent consumer experiences only on that part of the Web from which the sample was drawn, and are not generally representative of consumers' online experiences.

APPENDIX A: ENDNOTES

1. Nielsen//NetRatings provides online publishers, e-commerce companies, Internet advertising and marketing firms, and others with audience information and analysis about how people use the Internet, including what sites they visit, what ad banners they see, and the demographics of the users.
2. There were over 5,600 domains on the list; the unduplicated reach of all sites on the list was 98.3% (. . . , it was estimated that 98.3% of all active Web users visited at least one of these sites at least once in the month of January 2000).
3. The sampling frame used in the 1999 Georgetown survey was a list of the top 7,500 servers. GIPPS Report, App. B at 4 (1999), available at < <http://www.msb.edu/faculty/culnanm/gippshome.html> > . Multiple servers for a single domain were then

25. The weighted analysis is based on the data from both the Random Sample and the Most Popular Group. Data for both groups were combined in such a way as to give each group its proper weight, as dictated by the size of the population traffic it represented. (Sites appearing in both groups were counted only once.) This procedure was used (as opposed to simply assigning weights to each observation in the Random Sample) because it makes better use of the data regarding the Most Popular sites, where so much of the traffic takes place, and therefore gives a more accurate estimate.
26. The analysis treats the Nielsen//NetRatings estimates of unique site visits as precise measures of site traffic. Because this underlying traffic figure, which is based on estimates from survey panel data, actually contains some margin of error itself, the resulting weighted analysis figures are somewhat less precise than we report.
27. Some of the data is reported as a percentage of sub-samples. For example, the fair information practice figures are reported as a proportion of sites that collect personal identifying information, and not as a proportion of all sites in the samples. Where the data is reported as a percentage of a sub-sample (e.g., all sites that collect personal identifying information), the weighted analysis included only those sites meeting the sub-sample's characteristics and all other sites were excluded.
28. If the sample had been drawn from the entire Web, the weighted analysis would have provided a more useful interpretation of the data. For example, in such a case the weighted analysis figure for "privacy policy" would represent the likelihood that a representative consumer would visit a site that posts a privacy policy each time he or she visits a different Web site. Audience estimates for all sites on the Web, which would be necessary to employ such a methodology, do not appear to be available.

A A I , IT ,
T CT

Random Sample Site List & Survey Forms

www.123inc.com
www.12c4.com
www.180096hotel.com
www.1wrestling.com
www.555-1212.com
www.7search.com
www.800.com
www.800chat.com
www.800florals.com
www.8op.com
www.aa.com
www.abcdistributing.com
www.accessarizona.com
www.activision.com
www.adatom.com
www.adoption.com
www.afreegreetingcard.com
www.africana.com
www.alaskaairlines.com
www.albertsons.com
www.algore2000.com
www.all-ink.com
www.amarillionet.com
www.americanfunds.com
www.ancestry.com
www.andysgarage.com
www.anglefire.com
www.ant.com
www.apcc.com
www.archiecomics.com
www.ardemgaz.com
www.armchairmillionaire.com
www.asd.com
www.ask.com
www.askmerrill.com
www.atlastravelweb.com
www.atomfilms.com
www.attitude99.com
www.atyouroffice.com
www.audiocard.com
www.autoaccessory.com
www.avault.com
www.babiesrus.com
www.babynames.com
www.bbandt.com
www.be.com
www.bellsouth.com
www.bibliofind.com
www.bigplanet.com
www.bizrate.com
www.blairwitch.com
www.bluemountain.com
www.bobbrinker.com
www.borders.com
www.bottlerocket.com
www.bravotv.com
www.brilliantpeople.com
www.britney.com
www.c4.com
www.cai.com
www.calendarlive.com
www.camalott.com
www.cardemporium.com
www.carfinance.com
www.cbot.com
www.ceoexpress.com
www.channel1.com
www.charityfrogs.com
www.chartshop.com
www.checkout.com
www.checksinthemail.com
www.childrensplace.com
www.chryslerfinancial.com
www.cinemark.com
www.clubphoto.com
www.cnet.com
www.commissioner.com
www.compgeeks.com
www.compuserve.com
www.connect-to.com
www.connect2music.com
www.continental.com
www.cosmomag.com
www.costco.com

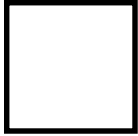
www.courier-journal.com
www.courtstv.com
www.craftassoc.com
www.crafterscommunity.com
www.creaf.com
www.crestar.com
www.crosswalk.com
www.cwssubscribe.com
www.cyber-nation.com
www.cybercities.com
www.datingclub.com
www.dawsonscreek.com
www.daytimer.com
www.decipher.com
www.deerlake.com
www.dellauction.com
www.delphi.com
www.deltavacations.com
www.digitalcity.com
www.discoveromaha.com
www.divorcesource.com
www.dollar.com
www.driveoldsmobile.com
www.drlaura.com
www.eakles.com
www.earlyamerica.com
www.eidosinteractive.com
www.emusic.com
www.epicgames.com
www.etown.com
www.ezthemes.com
www.familymoney.com
www.fidelity.com
www.findlaw.com
www.findwhat.com
www.firstauction.com
www.fishermansnet.com
www.flyaow.com
www.foxnews.com
www.franklincovey.com
www.freecreditreport.com
www.freei.com
www.freemac.com
www.ftd.com
www.funone.com
www.gamegenie.com
www.garfield.com
www.gear.com
www.getsmart.com
www.gmc.com
www.go2orlando.com
www.gocampingamerica.com
www.gocarolinas.com
www.goldenfeather.com
www.goodhome.com
www.goofball.com
www.greatdomains.com
www.greatoutdoors.com
www.grizzly.com
www.grolier.com
www.gurl.com
www.guru.com
www.handspring.com
www.harborfreight.com
www.harryanddavid.com
www.hawaiianair.com
www.healthgrades.com
www.healthquick.com
www.heartwarmers4u.com
www.historyplace.com
www.holiday-inn.com
www.hollowwww.com
www.homegain.com
www.homepage.com
www.hotjobs.com
www.huntington.com
www.ibm.com
www.individualinvestor.com
www.infoarea.com
www.insidetheweb.com
www.intel.com
www.inter800.com
www.invesco.com
www.investoroutlook.com
www.iparty.com
www.iqtest.com
www.irs.com
www.iturf.com
www.ivillage.com
www.iwarp.com

www.jack.com
www.janus.com
www.javascript.com
www.jcpenney.com
www.jfax.com
www.jokes.com
www.katv.com
www.kidrock.com
www.kidscamps.com
www.knowledgeadventure.com
www.korn.com
www.krause.com
www.krmediastream.com
www.kron.com
www.lasvegassun.com
www.lessonplanz.com
www.limp-bizkit.com
www.linux.com
www.localeyes.com
www.lockergnome.com
www.lovequote.com
www.malonefreightlines.com
www.marvel.com
www.mazdausa.com
www.meade.com
www.memolink.com
www.merck-medco.com
www.mervyns.com
www.mexonline.com
www.missingkids.com
www.montelshow.com
www.more.com
www.mortgage101.com
www.musictoday.com
www.myhelpdesk.com
www.nandotimes.com
www.nationjob.com
www.ndb.com
www.netnoir.com
www.netscape.com
www.netsrq.com
www.newjoke.com
www.newsdirectory.com
www.nflshop.com
www.nissan-usa.com
www.northernlights.com
www.ny-lotto.com
www.oag.com
www.officeclick.com
www.officemax.com
www.ohwy.com
www.olsten.com
www.osmond.com
www.outsource2000.com
www.p1cs.com
www.pacbell.com
www.painewebber.com
www.palm.com
www.palmgear.com
www.pcguide.com
www.pcwebopedia.com
www.peoplesearch.com
www.performancebike.com
www.pga.com
www.phantomstar.com
www.photoisland.com
www.photoloft.com
www.physique.com
www.playbill.com
www.playstation.com
www.pollg.com
www.potterybarn.com
www.pricewatch.com
www.prodreg.com
www.publicdata.com
www.quepasa.com
www.quickbooks.com
www.quintcareers.com
www.rampage.com
www.realty.com
www.reebok.com
www remodel.com
www.renegadeolga.com
www.repriserec.com
www.resobase.com
www.reversephonedirectory.com
www.riddler.com
www.rogerwilco.com
www.roughguides.com
www.savvysearch.com

www.sbc.com
www.scoopswrestling.com
www.scream3music.com
www.semaphorecorp.com
www.server.com
www.sfnb.com
www.shaklee.com
www.sharperimage.com
www.shoplet.com
www.showtimeonline.com
www.sitemeter.com
www.smartcollecting.com
www.smartshop1.com
www.snopes.com
www.soapnet.com
www.soapoperadigest.com
www.social-security-number.com
www.softseek.com
www.speedbit.com
www.spiegel.com
www.sportsline.com
www.stampsonline.com
www.starlingtech.com
www.startrekcontinuum.com
www.stonecold.com
www.stonetemplepilots.com
www.surfsouth.com
www.sweepstake0.0m

www.swe(www.sportsline.com)TjT*-rit.com

wtodayswww.spopes.com
www.sportsline.9-0.0038 Topplots.com



Federal Trade Commission
2000 Online Privacy Survey

ID # _____

Surf Survey Form

Surfer's Name _____ Date _____

Assigned Domain (URL) [Random Sample Results] _____

PART 1 - SCREENING

Instructions:



IF YES, STOP HERE RECORD "U"
GO

Is the site an adult site?

IF YES, STOP HERE RECORD "A"
GO

Is the site directed to children under 13?

IF YES, STOP HERE RECORD "K"
GO

If you answered NO to (1) through (3), WRITE
PRINT WRITE
PLACE
GO Survey Question 1.

I u : C N B u u _____ NO YES

Q5 EMAIL ADDRESSES 15 320

Q6 PERSONAL IDENTIFYING INFORMATION 44 291
 other than email address

(Consult a proctor before relying upon "other" to answer YES to this question.)

Q7 NON-IDENTIFYING INFORMATION 108 227

(Consult a proctor before relying upon "other" to answer YES to this question.)

STOP

Go to your next assigned URL.

PART 3 - NOTES

I u :

.

URL _____



Federal Trade Commission
2000 Online Privacy Survey

ID # _____

Content Analysis Form

Content Analyst's Name _____	Date _____
Content Analyst's Name _____	
Assigned Domain (URL) [Random Sample Results] _____	

I u : C N B u u

PART 1 - NOTICE

	NO	YES
Q9 NOT	294	1
If NO, GO Question #10 If YES SKIP Question #24		

Q10 what specific personal information the domain collects	71	223
---	----	-----

Q14 ONE CIRCLE the number
 corresponding to your choice

CIRCLE ONE

domain	opt in	55
domain	opt out	155
domain consent or offers a choice		
does not make clear		9
does not say anything about	choice	
	domain	244

PART 3 - DISCLOSURES TO THIRD PARTIES: NOTICE AND CHOICE

Q15 whether parties disclose personal information it collects to third parties anything about NO YES
 52 242

If NO SKIP Question #18
 If YES, GO Question #16

Q16 ONE CIRCLE the number CIRCLE ONE
 corresponding to your choice

does or may personal identifying information third parties. 169

does NOT disclose personal identifying information third parties or only 73

IF YOU CHOSE #1 GO Question #17
 IF YOU CHOSE #2 SKIP Question #18

Q17 ONE CIRCLE the number CIRCLE ONE
 corresponding to your choice

personal identifying information opt in 14

personal identifying information opt out 274

consent or offers a choice, personal identifying information does not make clear 37

does not say anything about personal identifying information choice 44

Q18

PART 6 - COOKIES

Q24 whether the DOMAIN places cookies anything about NO YES
142 153

If NO, SKIP Question #26
If YES, GO Question #25

Q25 ONE and CIRCLE the number corre-
sponding to your choice CIRCLE ONE
does or may 147
does not 6

Q26 whether THIRD PARTIES may place cookies anything about NO YES
246 48

If NO STOP!
Review accuracy
answered or skipped appropriately
Go to your next folder

If YES, GO Question #27

Q27 ONE CIRCLE the number corre-
sponding to your choice CIRCLE ONE
do or may 48
do not 0

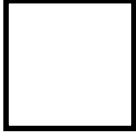
STOP!

Review your answers for accuracy and to ensure that all questions were answered or skipped appropriately.
Then, Go to your next folder.

Most Popular Group Site List & Survey Forms

www.1800ussearch.com
www.about.com
www.adobe.com
www.alexa.com
www.alladvantage.com
www.altavista.com
www.amazon.com
www.americangreetings.com
www.aol.com
www.apple.com
www.ask.com
www.barnesandnoble.com
www.bluemountain.com
www.bonzi.com
www.broadcast.com
www.cdnow.com
www.classmates.com
www.cnet.com
www.cnn.com
www.compuserve.com
www.digitalcity.com
www.dogpile.com
www.ebay.com
www.egreetings.com
www.eonline.com
www.etrade.com
www.excite.com
www.expedia.com
www.freelotto.com
www.geocities.com
www.go.com
www.goto.com
www.homestead.com
www.hotmail.com
www.hp.com
www.icq.com
www.ign.com
www.infospace.com
www.intuit.com
www.ivillage.com
www.iwon.com
www.jcpenney.com
www.justsaywow.com
www.kbb.com
www.looksmart.com
www.lycos.com
www.macromedia.com
www.mailbits.com
www.mapquest.com
www.marketwatch.com
www.mcafee.com
www.microsoft.com
www.mindspring.com
www.monster.com
www.msn.com
www.msnbc.com
www.mtv.com
www.netscape.com
www.nfl.com
www.nytimes.com
www.onhealth.com
www.passport.com
www.pathfinder.com
www.pch.com
www.previewtravel.com
www.priceline.com
www.quicken.com
www.real.com
www.realtor.com
www.shockwave.com
www.simplenet.com
www.snap.com
www.sony.com
www.sportsline.com
www.superpages.com
www.switchboard.com
www.talkcity.com
www.ticketmaster.com
www.travelocity.com
www.treeloot.com
www.tripod.com
www.uproar.com
www.usatoday.com
www.weather.com





Federal Trade Commission
2000 Online Privacy Survey

ID # _____

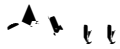
Surf Survey Form

Surfer's Name _____ Date _____

Assigned Domain (URL) [Most Popular Group Results]_____

PART 1 - SCREENING

Instructions:



IF YES, STOP HERE . RECORD "U"
GO . . .

▪ . . . *adult site?*

IF YES, STOP HERE . RECORD A
GO . . .

▪ . . . *directed to children under 13*

If YES, STOP HERE . RECORD K
GO . . .

If you answered NO to (1) through (3), WRITE
PRINT . . . WRITE . . .
PLACE
GO Survey Question 1.

I u : C N B u u

Q1 ■ PRIVACY SEAL



BetterWeb

(Consult a proctor before relying upon "other" to answer YES to this question.)

ASKCOPY

Q2 ■ PRIVACY POLICY

If NO, SKIP Question #4

If YES PRINT

PLACE

ASK
COPY

WRITE
Part 3

PART 3 - NOTES

I u :

.

URL _____

Federal Trade Commission
2000 Online Privacy Survey

ID # _____

Third-Party Cookie Survey Form

Surfer's Name _____	Date _____
Assigned Domain (URL) [Most Popular Group Results]_____	



Instructions: Circle NO or YES.

Q8 ■ THIRD PARTY ■ OTHER THAN ■
 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
 IF YES ■ URL ■ ■ ■ ■ ■ ■ ■ ■

STOP

RIVACY NLINE:

Federal Trade Commission
2000 Online Privacy Survey

ID # _____

Content Analysis Form

Content Analyst's Name _____	Date _____
Content Analyst's Name _____	
Assigned Domain (URL) [Most Popular Group Results] _____	

I u : C N B u u
u .

PART 1 - NOTICE

Q9 NOT
If NO, GO Question #10
If YES SKIP Question #24

Q10 about anything

PART 2 - INTERNAL USE: NOTICE AND CHOICE

Q11	how the domain may use purposes	anything about for internal	NO 0	YES 91
-----	---------------------------------	-----------------------------	---------	-----------

If NO, SKIP Question #15
If YES, GO Question #12

Q12	whether domain communications to the consumer?	anything about to send communi-	2	89
-----	--	---------------------------------	---	----

If NO, SKIP Question #15
If YES, GO Question #13

Q13 ONE CIRCLE the number corresponding to your choice

domain does or may send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question)	87
--	----

domain does not send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question)	2
---	---

IF YOU CHOSE #1 GO Question #14
IF YOU CHOSE #2 SKIP Question #15

Q14 ONE ✓ .
corresponding to your choice

• CIRCLE the number

Q16 ONE CIRCLE the number CIRCLE ONE
 corresponding to your choice

does or may disclose personal identifying information to third parties. 73

does NOT disclose personal identifying information to third parties or only 16

IF YOU CHOSE #1 GO Question #17
 IF YOU CHOSE #2 SKIP Question #18


Q17 ONE CIRCLE the number CIRCLE ONE
 corresponding to your choice


opt in personal identifying information 8

opt out personal identifying information 26

consent or offers a choice, personal identifying information does not make clear 20

does not say anything about personal identifying information choice 19

Q18  review at least some personal information

Q19  have inaccuracies corrected in at least some

PART 6 - COOKIES

Q24 whether the DOMAIN places cookies anything about NO YES
 12 79
 If NO, SKIP Question #26
 If YES, GO Question #25

Q25 ONE and CIRCLE the number corresponding to your choice
 CIRCLE ONE
 does or may 79
 does not 0

Q26 whether THIRD PARTIES may place cookies anything about NO YES
 53 38
 If NO STOP!
 Review accuracy answered or skipped appropriately
 Go to your next folder
 If YES, GO Question #27

Q27 ONE CIRCLE the number corresponding to your choice
 CIRCLE ONE
 do or may 38
 do not 0

STOP!

Review your answers for accuracy and to ensure that all questions were answered or skipped appropriately.
Then, Go to your next folder.

2000 Online Privacy Survey Instructions for Surf Survey Form

GENERAL INSTRUCTIONS

1. Your role in the survey is to determine whether your assigned domains collect personal information from online consumers and post disclosures about the collection and use of this information. We refer to these disclosures as "Privacy Policies" or "Information Practice Statements." The following step-by-step instructions provide guidance on these terms.
2. In this survey, we use the term "personal identifying information" to refer to information that can be used to identify or locate an individual. We use the term "non-identifying information" to refer to information that, taken alone, cannot be used to identify or locate an individual. We use the more general "personal information" to include EITHER "personal identifying information" AND/OR "non-identifying information." The step-by-step instructions provide further guidance on these terms.
3. Surf each domain for a maximum of 20 minutes, looking for a privacy seal, Privacy Policy, Information Practice Statements, and places where personal information is collected (see step-by step instructions for more details). Be sure to stay within the assigned domain as you move from Web page to Web page.
4. If you have any questions, or if you are uncertain at any point as to what you should do, consult a proctor.

STEP-BY-STEP INSTRUCTIONS

Start with the first assigned domain (URL) on your list. Enter the domain's ID Number (shown on your list of assigned URLs), URL, your name and the date on page 1.

PART I SCREENING

This part of the form requires you to answer a series of screening questions to determine whether the domain should be included in the survey. Where possible, answer these questions by looking at the home page. If the home page does not provide enough information, skim the domain. If you determine that a domain should be excluded from the survey, indicate the reason for your decision by entering the appropriate letter in the box on page 1.

(1) Are you unable to access this URL?

Exclude a domain from the survey if you are unable to access it because you receive a message that the domain is "Under Construction," "Inactive," or "Unavailable," or because you receive a "404 error" or "No DNS Entry" message. Record a "U" in the box at the upper left on page 1 and to go your next assigned URL.

If you are able to access the domain, answer screening question (2).

Note: If, when typing in an assigned URL, you are automatically referred to another URL, apply the following screening criteria to the new URL.

(2) Is the domain an "adult site?"

Determine whether, in your judgment, the domain's content and graphics are pornographic in nature. If the domain is an _____, exclude it from the survey. Record an "A" in the box at upper left on page 1 and go to your next assigned URL. If the domain is not an _____, answer screening question (3).

(3) Is the domain *directed to children under the age of 13*?

Consider the following factors (taken from the Children's Online Privacy Protection Rule, 16 CFR § 312.2): the domain's subject matter, visual or audio content, age of models, language or other characteristics; whether advertising appearing on the domain is directed to children; and whether the domain uses animated characters and/or child-oriented activities and incentives. Use these factors to form a judgment as to whether the domain is _____ (_____, _____) _____ 13. If the domain is _____ 13, exclude it from the survey. Record a "K" in the box at upper left of page 1 and go to your next assigned URL.

If, after answering all three screening questions, you have not excluded the domain from the survey, print the home page, write the domain's ID number on it, and place it in a folder. Write the domain's ID Number on the folder tab. You are now ready to answer the survey questions in PART 2.

PART 2 DOMAIN ATTRIBUTES

This part of the form requires you to answer questions about the domain's content. Proceed through the form from beginning to end, in the order directed by the instructions on the form. Do not answer questions out of order, unless instructed to skip a question. Circle NO or YES for each question, unless instructed to skip the question.

PLACES TO LOOK FOR PRIVACY SEALS, PRIVACY POLICIES, INFORMATION PRACTICE STATEMENTS, AND COLLECTION OF PERSONAL INFORMATION

Try to view every screen on the domain. If the domain is extremely large, look for screens where personal information collection is likely to occur or where privacy disclosures are likely to be posted. Here are some ideas:

registration form	order form	survey form
terms of service	terms of use	guest book / "About You"
FAQs	contest registration	Help
account page	"feedback"	legal page
membership page	"subscribe here"	"shop here"

If the domain has a search tool, type terms such as "privacy," "security," "mailing list," or "order form."

PRIVACY DISCLOSURES

Question 1 Is a PRIVACY SEAL posted on this domain?

Several privacy assurance programs have been developed that license privacy seals to online companies whose information practices meet program standards. This question asks whether such a privacy seal is posted on the domain. Typically, these seals appear on the home page or with a domain's Privacy Policy, but you should not stop there if you find no seal. Continue to search the domain until you are satisfied that a privacy seal either is or is not posted.

Color reproductions of each of the privacy assurance program seals listed as examples in this question accompany this training manual. If you find a seal or icon that is not listed as an example but appears to be a privacy seal, consult a proctor before Circling "YES" and writing the name of the seal on the line provided.

Question 2 Is a PRIVACY POLICY posted on this domain?

Increasingly, online companies are posting descriptions of their information practices. In this survey, we refer to these descriptions as "Privacy Policies." A Privacy Policy may, for example, describe what an online company does with any personal information it collects from online consumers, as well as any options it provides online consumers regarding how it will use this information. It may also describe the steps the domain takes to provide security for personal information it collects, or procedures available to online consumers to see what information has been collected about them. Companies don't always use the term "Privacy Policy," so look for terms such as "Privacy Statement," "Privacy," "Security," "Online Privacy Practices," or "Our Policies."

If you find a Privacy Policy, print it, write the domain's ID Number on the printout, and place it in the domain's folder. Check to be sure that you have printed the entire Privacy Policy. If the domain has both a Privacy Policy and a Security Policy, be sure to print them both. If, after trying the printing tips listed below, you cannot print the Privacy Policy, copy it verbatim in Part 3 of the survey form.

Note: If a Privacy Seal is posted on the domain, clicking on it may take you to the seal program's standards rather than the domain's Privacy Policy. Be sure you find and print the domain's Privacy Policy.

Note:

Question 4 Is one or more INFORMATION PRACTICE STATEMENT(S) posted on this domain?

Often online companies post disclosures about particular information practices in various locations on a domain where they are most relevant, for example, on order forms or registration pages. We refer to such individual disclosures as "Information Practice Statements." This is our term; it is unlikely that you will see the phrase "Information Practice Statement" on domains. A list of sample Information Practice Statements accompanies these instructions. These are the types of disclosures that you are looking for. If you are uncertain as to whether a disclosure is an Information Practice Statement, consult a proctor.

refearr

tse

a2

Question 5 Does the domain collect EMAIL ADDRESSES?

For purposes of this question, all opportunities for providing the domain an online consumer's email address, including the online forms listed in the box on page 3, sending email to the online company, or contacting the domain's Webmaster, are considered collection of an email address.

Question 6 Does the domain collect PERSONAL IDENTIFYING INFORMATION other than an email address?

As noted above, we define "personal identifying information" as information that can be used to identify or locate an individual. An email address is one type of personal identifying information. Other examples include name, postal address, telephone number, fax number, credit card number, and Social Security number. This question asks you to determine whether the site is collecting

PRINTING TIPS

- (1) Wait for the Web page to finish loading ("Document Done" on lower tool bar), click on the "Stop" button, then print.
- (2) If you cannot print the entire screen, but the text you want to print appears in a "frame," print the frame by clicking on it and then clicking on "File" and "Print Frame."
- (3) If you experience difficulty, highlight the text you want to print and type Ctrl-C (or use the "Copy" button) to copy the text to the clipboard. Then go into WordPerfect 8 and

RIVACY NLINE:

2000 Online Privacy Survey Instructions for Third-Party Cookie Survey Form

1. Delete all cookie files in your computer's cookie cache.
2. Be sure that your browser preferences are set to warn you before accepting a cookie.
3. Write your name and the date in the spaces provided.
4. Write the assigned domain's URL, and the assigned domain's ID Number, in the spaces provided (see folder tab or list of assigned URLs for ID Numbers).
5. Enter the assigned domain's URL in your browser.
6. Check for the domain shown in the first cookie alert that appears. If the domain shown in the cookie alert is NOT the assigned domain, CIRCLE YES for Question 8 and RECORD the URL of the domain shown in the cookie alert in the space provided. THEN GO to your next assigned domain.
7. If the domain shown in the cookie alert is the assigned domain, choose "cancel" to reject the cookie and continue observing for any other cookie alerts. RECORD the URL of the first domain other than the assigned domain to appear in a cookie alert and CIRCLE YES for Question 8. If no other alerts appear, or if the assigned domain is the only domain to appear in a cookie alert, CIRCLE NO for Question 8 and go to your next assigned domain.
8. Remember to reject all cookies by clicking on "Cancel" in the alert box.
9. In some cases, it may be necessary to search beyond the home page in order to ascertain whether a third party is attempting to place a cookie. Be certain to stay within the assigned domain. In any case, spend no more than five minutes checking for cookie alerts on the assigned domain (URL).

RIVACY NLINE:

2000 Online Privacy Survey
Instructions for Content Analysis Form

GENERAL INSTRUCTIONS

1. Your role in the survey is to answer questions about the content of the

DEFINITION OF KEY TERMS

1. "Privacy Disclosure:" Privacy disclosures refer to any statement on a domain regarding that domain's information practices i.e., what information they collect, what they do with it, and how they treat it. Privacy disclosures include both "privacy policies" and "information practice statements." A privacy policy is a detailed or unified description of a domain's information practices. Often, online companies also post disclosures about particular information practices in various locations on a domain where they are most relevant, for example, on order forms or registration pages. We refer to such discrete disclosures as information practice statements, although they are not titled as such. They are simply privacy disclosures that appear outside a privacy policy. The information practice statements that the surfer found should be highlighted. Your answers on the Content Analysis Form should be based on all of the privacy disclosures found in the domain's folder, read together.
2. "Personal identifying information:" We use the term "personal identifying information" to refer to information that can be used to identify or locate an individual. Examples: email address, name, address, phone number, fax number, credit card number, Social Security number.
3. "Non-identifying information:" We use the term "non-identifying information" to refer to information that, taken alone, cannot be used to identify or locate an individual. Examples: Age/date of birth, gender, occupation, education, ZIP code with no address, interests, hobbies, types of hardware/software using, income.
Note: Non-identifying information refers to the type of information, regardless of whether such information is collected along with, or is linked to, personal identifying information.
4. "Personal information:" We use this term to refer to EITHER "personal identifying information" AND/OR "non-identifying information."
Note: Domains use different terms to describe personal information. You must read a domain's privacy disclosures carefully to understand what information a statement is referring to. You should not necessarily equate the term "personal information" as it appears in a privacy disclosure with the term as it is used in these instructions or on the Content Analysis Form.
5. "Third party:" Any entity other than the assigned domain. Examples: advertisers, affiliates, subsidiaries, business partners, or other companies.

PRIVACY NOTICE:

Answer N[-p 0/F12 15.38122.06 TD05.0017 Tc80.0166[(If you do not find a statement about wh

Send us an email to get on our email updates list.

Click here if you do not want to receive emails from us in the future.

Put me on your mailing list [click-box checked]

We never send you email about our products and services without your consent.

When you send a question to "Ask the Doctor," you must provide us an email address. We use this address to answer your question.

Answer NO: If you do not find a statement about how the domain may use personal information it collects for internal purposes, i.e., the privacy disclosures are silent with respect to how the domain may use personal information it collects for internal purposes.

Note: Questions 12, 13 and 14 are a group. All three deal with one particular use of personal information for internal purposes — namely, the use of personal information by the domain to send communications to the consumer. Question 12 asks if there is any statement (positive or negative) about this type of use. If there is such a statement, Question 13 asks what the statement says, i.e., whether the domain says that it does or does not use personal information to send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question). If the domain says that it does use personal information in this way, Question 14 asks whether the domain says that it provides consumers with any choice with respect to this use of personal information.

Question 12 / *anything about*
whether domain *to send communica-*
tions to the consumer

orses.

A

information is not or is never used by the domain to send communications to the consumer. You should also answer YES to this question if you find a statement whose clear implication is that the information will or will not be used to send communications to the consumer.

Examples: We never use your personal information for any purpose.

We only use your email address to send you a message confirming that your order was processed and to tell you the date your product will be shipped.

We only use your information to process your order.

We use your email address to send you newsletters that may be of interest to you.

Send us an email to get on our email updates list.

[Click here](#) if you do not want to receive emails from us in the future.

Put me on your mailing list [click-box checked]

We never send you email about our products and services without your consent.

consumer, the information will be used.

Note: If the domain provides choice with respect to sending at least some communications to the consumer (other than those directly related to processing an order or responding to a consumer's question), then answer Question 14 based on that choice. Thus, for example, if the domain provides consumers choice with respect to being on the domain's mailing list, but does not state that it provides choice with respect to other communications it may send, answer Question 14 based on the choice provided with respect to mailing lists.

Circle 1 ("opt in"): If the domain requires an affirmative act by the consumer before it will use personal information to send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question). The personal information is not used until the consumer takes some required action. Thus, if the consumer does not want his or her personal information used in this way, he or she does not have to do anything.

Examples: Send us an email to get on our email updates list.

Click here to be included in our mailing list.

If you would like to receive email updates with information about sales and discounts, fill out this form.

Circle 2 ("opt out"): If the domain will use personal information to send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question), unless the consumer takes some required action to stop this use of personal information. Thus, if the consumer does not want his or her personal information used in this way, he or she must take some required action.

Examples: Click here if you do not want to receive emails from us in the future.

Put me on your mailing list [click-box checked]

If you do not want to receive email updates with information about sales and discounts, please send an email to the following address.

Circle 3 ("consent or choice, but unclear what type"): If the domain states that it requires the consumer's consent before sending, or that it offers a choice with respect to receiving communications from the domain (other than those directly related to processing an order or responding to a consumer's question), but does not make clear whether the choice is opt-in or opt-out.



if you find a statement that personal information is not or is never disclosed by the domain to third parties.

Examples: We never share your name and address with any third party.

We may share information about our visitors with our advertisers, but we will only share such information in the aggregate. We will never disclose your identity to any third party.

We may disclose your information to third parties, but only to complete delivery of your order.

We occasionally disclose our mailing list to our affiliates so that they can send you information about special offers that may interest you.

If you want to receive special offers from our business partners, send us an email.

If you do not want us to share your personal information with any other parties, click here.

I'd like to receive special offers from your business partners [click-box checked]

We will never disclose your personal information without your consent.

Answer NO: If you do not find a statement about whether the domain discloses personal information it collects to third parties, i.e., the privacy disclosures are silent with respect to whether the domain discloses personal information it collects to third parties.

Example: We will use your personal information to process your order and serve you better.

Question 16 This question requires you to characterize what the domain says regarding the disclosure of personal identifying information to third parties.

Note: This question refers to personal identifying information. You must read the privacy disclosures carefully to see whether the domain does or may disclose such information, as opposed to non-identifying information. If the domain speaks generally about disclosure of personal information — without distinguishing between identifying or non-identifying informa-

tion — YOU SHOULD TREAT THE STATEMENT AS REFERRING TO PERSONAL IDENTIFYING INFORMATION.

Circle 1 (“does or may”): If you find a statement that the domain does or may disclose personal identifying information to third parties.

Examples: We occasionally disclose our mailing list to our affiliates so that they can send you information about special offers that may interest you.

If you want to receive special offers from our business partners, send us an email.

If you do not want us to share your personal information with any other parties, click here.

I'd like to receive special offers from your business partners [click-box checked]

9.34 you find a statem domain

Note: We ask about two types of choice — “opt-in” and “opt-out.” Please review the notes on this issue accompanying Question 14.

Note: If the domain provides choice with respect to the disclosure of at least some personal identifying information to at least some third parties, answer Question 17 based on that choice. Thus, for example, if the domain says that it provides consumers choice with respect to the disclosure of personal identifying information to advertisers, but does not say that it provides choice with respect to the disclosure of personal identifying information to other third parties, answer the question based on the choice provided with respect to advertisers.

Circle 1 (“Opt in”): If the domain requires an affirmative act by the consumer before it will disclose personal identifying information to third parties. The personal identifying information is not disclosed until the consumer takes some required action. Thus, if the consumer _____

the choice is opt-in or opt-out.

Examples: We will never disclose your personal information without your consent.

We only disclose your personal information to our trusted business partners with your permission.

Circle 4 (“no choice”): If, after reviewing all of the privacy disclosures in your folder, you can find no statement about whether the domain offers consumers choice with respect to disclosures of personal identifying information to third parties, i.e., the privacy disclosures are silent with respect to this issue.

Examples: We occasionally disclose our mailing list to our affiliates so that they can send you information about special offers that may interest you.

PART 4 ACCESS

Questions 18 - 20 deal with statements about a consumer’s ability to review, correct, or delete at least some personal information about them.

Question 18

review at least some personal information

Answer YES: If you find a statement that the domain allows consumers to review at least some personal information about them.

Example: To see the account information we have about you, click on “My Account.”

Answer NO: If you do not find a statement that the domain allows consumers to review at least some personal information about them (i.e., the privacy disclosures are silent on this issue), or if you find a statement that the domain does not allow consumers to review at least some personal information about them.

Note: To answer YES to this question, you must find a statement that the domain allows consumers to see or review at least some of the personal information about them. Do not infer the ability to review based upon your answers to Questions 19 or 20.

Question 19

have inaccuracies corrected in at least some personal information

Note: Privacy disclosures may use terms such as “edit” or “update” rather than “correct.”

Answer YES: If you find a statement that the domain allows consumers to have inaccuracies corrected in at least some personal information about them.

Examples: To correct your account information, select the “Edit” feature under “My Account.”

If you’ve moved, send us an email with your new address and we will update your information.

Answer NO: If you do not find a statement that the domain allows consumers to have inaccuracies corrected in at least some personal information about them (i.e., the privacy disclosures are silent on this issue), or if you find a statement that the domain does not allow consumers to have inaccuracies corrected in at least some personal information about them.

Question 20

have at least some personal information about them deleted

Answer YES: If you find a statement that the domain allows consumers to have at least some personal information about them deleted.

Examples: You may also delete information.

To have your name and address deleted from our database, send us an email.

Answer NO: If you do not find a statement that the domain allows consumers to have at least some personal information about them deleted (i.e., the privacy disclosures are silent on this issue), or if you find a statement that the domain does not allow consumers to have at least some personal information about them deleted.

Question 22

security,
during transmission

Note: Secured Socket Layer or "SSL" refers to security during transmission.

Answer YES: If you find a statement that the domain takes steps to provide security during transmission of the information from the consumer to the domain.

Examples: We use SSL to protect your credit card information.

We encrypt your information when you send it to us.

Answer NO: If you do not find a statement that the domain takes steps to provide security during transmission of the information (i.e., the privacy disclosures are silent on this issue), or if you find a statement that the domain does not take steps to provide security during transmission.

Note: General statements about security, which do not relate to transmission specifically, result in a "No" answer to this question.

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

We provide security for all information we collect.

This is a secure site.

We strive to ensure the security of your information. However, we cannot guarantee such security.

We store all our customer information on a secure server.

We use firewalls to prevent unauthorized access to our databases and servers.

Question 23

security,
, after the domain has received the information (. . .)

Answer YES: If you find a statement that the domain takes steps to provide security for personal information after the domain has received the information.

Examples: We store all our customer information on a secure server.

We use firewalls to prevent unauthorized access to our databases and servers.

Answer NO: If you do not find a statement that the domain takes steps to provide security for personal information after the domain has received the information (i.e., the privacy disclosures are silent on this issue), or if you find a statement that the domain does not take steps to provide security for personal information after the domain has received the information.

Note: General statements about security, which do not specifically relate to security

We do not use "cookies."

Answer NO: If you do not find a statement about whether the domain places cookies, i.e., the privacy disclosures are silent on this issue.

Question 25 This question requires you to characterize what the domain says about its use of cookies.

Circle 1 ("does or may"): If the domain says that the domain does or may place cookies.

Examples: We use cookies on this site.

We also collect certain information through cookies.

We might in the future use cookies.

Circle 2 ("does not"): If the domain says that the domain does not place cookies.

Example: We do not use "cookies."

Question 26 *whether THIRD PARTIES may place cookies / anything about*

Answer YES: If you find a statement that third parties may place cookies and/or collect personal information on the domain. Also answer YES if you find a statement that third parties do not place cookies and/or collect personal information on the domain.

Examples: Advertisers whose ads appear on our site may use cookies.

We cannot control the use of cookies by advertisers or partners on our site.

We do not allow third parties to place cookies or collect personal information on our site.

Answer NO: If you do not find a statement about whether third parties may place cookies and/or collect personal information on the domain, i.e., the privacy disclosures are silent on this issue.

Question 27 This question requires you to characterize what the domain says about third parties' use of cookies on the domain.

Circle 1 ("do or may"): If the domain says that third parties do or may place cookies and/or collect personal information on the domain.

Examples: Advertisers whose ads appear on our site may use cookies.

We cannot control the use of cookies by advertisers or partners on our site.

Circle 2 ("do not"): If the domain says that third parties do not place cookies and/or collect personal information on the domain.

Example: We do not allow third parties to place cookies or collect personal information on our site.

A C:
ATA TABI

TABLE 1

Percent of Web Sites That Collect Personal Information

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Collect Personal Information:	97% (95.0%-98.8%) ²	326/335	99% ³	90/91	99% (+/- 0.8%) ⁴
Collect Personal Identifying Information:	97% (94.2%-98.3%)	324/335	99%	90/91	99% (+/- 0.9%)
Collect Personal Identifying Information Other Than Email:	87% (82.8%-90.3%)	291/335	96%	87/91	94% (+/- 2.7%)
Collect Email:	96% (92.7%-97.5%)	320/335	99%	90/91	98% (+/- 1.0%)
Collect Non-Identifying Information:	68% (62.5%-72.7%)	227/335	77%	70/91	76% (+/- 5.2%)
Collect Non-Identifying Information Only:	1% (0.1%-2.1%)	2/335	0%	0/91	0% (+/- 0.2%)

1. "Personal Information" is defined to include any of the following: personal identifying information (. . . , name, postal address, email address, telephone number); and non-identifying information, including demographic information (. . . , age, gender, education level, income) and preference information (. . . , hobbies, interests).
2. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.
3. There is no sampling error for Most Popular Group data, because the results were obtained using a census as opposed to a sample.
4. Figures in parentheses represent 95% confidence intervals calculated using the Normal distribution.



TABLE 3

Of Those Web Sites That Collect Personal Identifying Information,
Percent With a Privacy Disclosure

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Post at Least One Privacy Disclosure:	90% (86.7%-93.4%) ²	293/324	100% ³	90/90	97% (+/- 1.4%) ⁴
Post a Privacy Policy:	64% (58.1%-68.2%)	206/324	97%	87/90	78% (+/- 6.6%)
Post an Information Practice Statement:					

1. A "Privacy Disclosure" can be either a "privacy policy," defined as a comprehensive description of a Web site's information practices that is located in one place on the site and may be reached by clicking on an icon or hyperlink, or an "information practice statement," defined as a discrete statement that describes a particular practice regarding consumers' personal information (such as "we may share your personal information with third parties").
2. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.
3. There is no sampling error for Most Popular Group data, because the results were obtained using a census as opposed to a sample.
4. Figures in parentheses represent 95% confidence intervals calculated using the Normal distribution.

TABLE 4

Of Those Web Sites That Collect Personal Identifying Information,

TABLE 5

Of Those Web Sites That Collect Personal Identifying Information,
Percent That Provide Elements of Notice

1. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.

TABLE 6

Percent of Web Sites That Post Disclosures About the Site's Use or Non-Use of Cookies

1. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.

TABLE 8a

Of Those Web Sites That Collect Personal Identifying Information,
Percent That Disclose Whether They Do or May Use Personal Information
to Send Communications to Consumers

TABLE 8b

Of Those Web Sites That Collect Personal Identifying Information and Offer Choice Regarding the Use of Personal Information to Send Communications to Consumers, Percent That Offer Opt-In or Opt-Out

1. This table does not include sites that say they do not use personal information to send communications to consumers. (Compare Table 7 (including both sites that provide choice and sites that say they do not use personal information to send communications to consumers)).

2. "Opt-in" is defined as choice that requires an affirmative act by the consumer (such as chec8.4 0 0 8.4 392.64 735.2res ane65

TABLE 9a

Of Those Web Sites That Collect Personal Identifying Information,
Percent That Say They May Disclose Personal Identifying Information to Third Parties

	Random Sample	Most Popular Group	Weighted Analysis
	Percent10		

TABLE 9b

Of Those Web Sites That Collect Personal Identifying Information and
Say That They Offer Choice Regarding the Disclosure of Personal Identifying
Information to Third Parties, Percent That Offer Opt-In or Opt-Out

1. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.
2. There is no sampling error for Most Popular Group data, because the results were obtained using a census as opposed to a sample.
3. Figures in parentheses represent 95% confidence intervals calculated using the Normal distribution.
4. This table does not include sites that say they do not disclose personal identifying information to third parties. (Compare Table 7 (including both sites that provide choice and sites that say they do not disclose personal identifying information to third parties)).

TABLE 10

Of Those Web Sites That Collect Personal Identifying Information,
Percent That Provide Choice For Either Sending Communications to Consumers or
Disclosure to Third Parties (and Percent That Implement Notice,

TABLE 11

Of Those Web Sites That Collect Personal Identifying Information,
Percent That Provide Elements of Access

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Allow Consumers to Review at Least Some Personal Information:	21% (16.4%-25.5%) ¹	67/324	48% ²	43/90	32% (+/- 4.8%) ³
Allow Consumers to Have at Least Some Personal Information Corrected:	37% (31.8%-42.5%)	120/324	78%	70/90	64% (+/- 6.0%)
Allow Consumers to Have at Least Some Personal Information Deleted:	17% (13.3%-21.8%)	56/324	31%	28/90	26% (+/- 5.0%)

1. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.
2. There is no sampling error for Most Popular Group data, because the results were obtained using a census as opposed to a sample.
3. Figures in parentheses represent 95% confidence intervals calculated using the Normal distribution.

TABLE 12

Of Those Web Sites That Collect Personal Identifying Information,
 Percent That Provide Opportunity to Review and to Correct or Delete Information
 (and Percent That Implement Notice, Choice, Modified Access,
 and Security to Some Extent)

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Say Consumers May Review <u>and</u> Correct or Delete at Least Some Personal Information the Site					

1. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.
2. There is no sampling error for Most Popular Group data, because the results were obtained using a census as opposed to a sample.
3. Figures in parentheses represent 95% confidence intervals calculated using the Normal distribution.

TABLE 13

Of Those Web Sites That Collect Personal Identifying Information,
Percent That Provide Disclosures About Elements of Security

	Random Sample	Most Popular Group	Weighted Analysis
--	----------------------	---------------------------	--------------------------

1. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.
2. There is no sampling error for Most Popular Group data, because the results were obtained using a census as opposed to a sample.
3. Figures in parentheses represent 95% confidence intervals calculated using the Normal distribution.

TABLE 14a

Percent of All Web Sites That Display a Privacy Seal

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Display a Privacy Seal:	8% (5.4%-11.5%) ¹	27/335	45% ²	41/91	36% (4.6%) ³

TABLE 14b

Of Those Web Sites That Collect Personal Identifying Information and Display a Privacy Seal,⁴ Percent that Implement

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Implement Notice, Choice, Access & Security to Some Extent:	52% (31.9%-71.3%)	14/27	56%	23/41	54% (+/- 6.8%)
Implement Notice & Choice to Some Extent:	63% (42.4%-80.6%)	17/27	71%	29/41	72% (+/- 7.2%)

1. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.
2. There is no sampling error for Most Popular Group data, because the results were obtained using a census as opposed to a sample.
3. Figures in parentheses represent 95% confidence intervals calculated using the Normal distribution.
4. All sites that displayed a privacy seal also collected personal identifying information.

/ a a/	- 1-877- -
/ / / ~ .	4