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.

TABLE OF CONTENTS

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 analyze vast amounts of data from and about the consumers who visit their Web sites. This increase in the collection and use of data has raised public awareness and consumer concerns about online privacy. To ensure consumer confidence in this new marketplace and its continued growth, consumer concerns about privacy must be addressed.

The Federal Trade Commission has been studying online privacy issues since 1995. This is the Commission's third report to Congress examining the state of online privacy and the efficacy of industry self-regulation. It presents the results of the Commission's 2000 Online Privacy Survey (the "Survey"), which reviewed the nature and substance of U.S. commercial Web sites' privacy disclosures, and assesses the effectiveness of self-regulation. The Report also considers the recommendations of the Commission-appointed Advisory Committee on Online Access and Security. Finally, the Report sets forth the Commission's conclusion that legislation is necessary to ensure further implementation of fair information practices online and recommends the framework for such legislation.

In its 1998 report, *Privacy Online: A Report to Congress* ("1998 Report"), the Commission described the widely-accepted fair information practice principles of *Notice*, *Choice*, *Access,* and *Security*. The Commission also identified *Enforcement* – the use of a reliable mechanism to provide sanctions for noncompliance – as a critical component of any governmental or self-regulatory program to protect privacy online. In addition, the 1998 Report presented the results of the Commission's first online privacy survey of commercial Web sites. While almost all Web sites (92% of the comprehensive random sample) were collecting great amounts of personal information from consumers, few (14%) disclosed anything at all about their information practices.

Last year, Georgetown University Professor Mary Culnan conducted a survey of a random sample drawn from the most-heavily trafficked sites on the World Wide Web and a survey of the busiest 100 sites. The former, known as the Georgetown Internet Privacy Policy Survey, found significant improvement in the frequency of privacy disclosures, but also that only 10% of the sites posted disclosures that even touched on all four fair information practice principles. Based in part on these results, a majority of the Commission recommended in its 1999 report to Congress, *Self-Regulation and Privacy Online*, that self-regulation be given more time, but called for further industry efforts to implement the fair information practice principles.

In February and March 2000, the Commission conducted another survey of commercial sites' information practices, using a list of the busiest U.S. commercial sites on the World Wide Web. Two groups of sites were studied: (1) a random sample of 335 Web sites (the "Random Sample") and (2) 91 of the 100 busiest sites (the "Most Popular Group"). As was true in 1998, the 2000 Survey results show that Web sites collect a vast amount of personal information from and about consumers. Almost all sites (97% in the Random Sample, and 99% in the Most Popular Group) collect an email address or some other type of personal identifying information.

The 2000 Survey results show that there has been continued improvement in the percent of Web sites that post at least one privacy disclosure (88% in the Random Sample and 100% in the Most Popular Group). The Commission's 2000 Survey went beyond the mere counting of disclosures, however, and analyzed the nature and substance of these privacy disclosures in light of the fair information practice principles of Notice, Choice, Access, and Security. It found that only 20% of Web sites in the Random Sample that collect personal identifying information implement, at least in part, all four fair information practice principles (42% in the Most Popular Group). While these numbers are higher than similar figures obtained in Professor Culnan's studies, the percentage of Web sites that state they are providing protection in the core areas remains low. Further, recognizing the complexity of implementing Access and Security as discussed in the Advisory Committee report, the Commission also examined the data to determine whether Web sites are implementing Notice and Choice only. The data showed that only 41% of sites in the Random Sample and 60% of sites in the Most Popular Group meet the basic Notice and Choice standards.

The 2000 Survey also examined the extent to which industry's primary self-regulatory enforcement initiatives – online privacy seal programs – have been adopted. These programs, which require companies to implement certain fair information practices and monitor their compliance, promise an efficient way to implement privacy protection. However, the 2000 Survey revealed that although the number of sites enrolled in these programs has increased over the past year, the seal programs have yet to establish a significant presence on the Web. The Survey found that less than one-tenth, or approximately 8%, of sites in the Random Sample, and 45% of sites in the Most Popular Group, display a privacy seal.

Based on the past years of work addressing Internet privacy issues, including examination of prior surveys and workshops with consumers and industry, it is evident that online privacy continues to present an enormous public policy challenge. The Commission applauds the significant efforts of the private sector and commends industry leaders in developing self-regulatory initiatives. The 2000 Survey, however, demonstrates that industry efforts alone have not been sufficient. Because self-regulatory initiatives to date fall far short of broad-based implementation of effective self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will emulate the standards

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.[1] 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.[2]

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 (*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.[3]

(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 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.

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 *et seq.*
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 computers that touched the lives of few consumers to a new marketplace where millions of consumers shop for information, purchase goods and services, and participate in discussions. The technological developments that have made e-commerce possible also have enhanced the ability of companies to collect, store, transfer, and analyze vast amounts of data from and about the consumers who visit their sites on the World Wide Web. This increase in the collection and use of data, along with the myriad subsequent uses of this information that interactive technology makes possible, has raised public awareness and increased concern about online consumer privacy.

In June 1998 and again in July 1999, the Commission reported to Congress on the state of online privacy and the efficacy of industry self-regulation. This report is the Commission's third examination of these issues. It presents the results of the Commission's 2000 Online Privacy Survey (the "Survey"), which reviewed the nature and substance of U.S. commercial Web sites' privacy disclosures, and assesses the effectiveness of self-regulation as a means of protecting consumer privacy online. The Report also considers the recommendations of the Commission-appointed Advisory Committee on Online Access and Security. Finally, the Report sets forth the Commission's recommendations to ensure further implementation of fair information practices online.[1]

A. THE GROWTH OF INTERNET COMMERCE

Since its inception in the mid-1990's, the online marketplace has grown at an exponential rate. Recent figures suggest that as many as 90 million Americans now use the Internet on a regular basis.[2] Of these, 69%, or over 60 million people, shopped online in the third quarter of 1999.[3] As many as 54% of Internet users have purchased products or services online.[4] The Census Bureau estimates that retail e-commerce reached $5.3 billion for the fourth quarter of 1999,[5] and other estimates place total online retail sales for all of 1999 in the $20-$33 billion

range.[6] Recent data suggest that consumers spent as much as $2.8 billion online during the month of January 2000 alone.[7]

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,[8] representing a 141% increase over the $1.9 billion reported for 1998[9] and a greater than ten-fold increase from 1996, when $267 million was spent on Internet advertising.[10]

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.[11] Recent survey data demonstrate that 92% of consumers are concerned (67% are "very concerned") about the misuse of their personal information online.[12] 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.[13] 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,[14] and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction.[15] One study estimates that privacy concerns may have resulted in as much as $2.8 billion in lost online retail sales in 1999,[16] 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.[17] 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.[18]

Public concern regarding privacy online appears likely to continue.[19] 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.[20]

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.[21] 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,[22] it has continued to encourage and facilitate effective self-regulation to protect consumers generally.[23]

1. THE FAIR INFORMATION PRACTICE PRINCIPLES AND PRIOR COMMISSION REPORTS

In its 1998 report, *Privacy Online: A Report to Congress*, the Commission summarized widely-accepted principles regarding the collection, use, and dissemination of personal information.[24] 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, *Records, Computers, and the*

Rights of Citizens.[25] 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.[26]

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:[27] 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.[28] 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.[29]

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.[30] 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.[31] After reviewing the GIPPS Report, the Commission issued its 1999 report to Congress, *Self-Regulation and Privacy Online*.[32] 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.[33]

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"[34] 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.[35] In a series of public meetings, the Advisory Committee discussed options, and the costs and benefits of each option, for implementation of these principles. The Committee's report to the Commission is discussed in more detail in Section III of this Report.

In February and March of this year, the Commission conducted its second survey of U.S. commercial Web sites' information collection and privacy disclosure practices. The Survey results are reported in Section II of this Report.

D. SELF-REGULATION THROUGH SEAL PROGRAMS

Industry's primary self-regulatory enforcement initiative has been the development of online privacy seal programs. These programs require their licensees to implement certain fair information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Web sites.[36] If widely adopted, they promise an efficient way to alert consumers to licensees' information practices and to demonstrate licensees' compliance with program requirements. Although the number of sites enrolled in these programs has increased in absolute terms since last year, the seal programs have yet to establish a significant presence on the Web.

TRUSTe, the first online privacy seal program, has grown from over 500 licensed Web sites last year[37] to more than 1200 sites in a variety of industries.[38] Over 450 sites representing 244 companies have been licensed to post the BBB*OnLine* Privacy Seal since the program was launched last March.[39] The CPA WebTrust program, which includes a privacy component in its requirements, has licensed its seal to 28 Web sites;[40] and six companies have been licensed to post the PriceWaterhouseCoopers BetterWeb online privacy seal.[41]

Other online privacy seal programs have been announced or are in the early stages of development,[42] 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.[43]

II. RESULTS OF THE COMMISSION'S 2000 ONLINEPRIVACY 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 cookies[45] by third parties.

The Survey examined Web sites that had 39,000 or more unique visitors[46] 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 *any* privacy disclosures.[47] 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.[48] 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.[49]

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).[50] 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.[51] 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.[52] 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 means,[53] and includes personal identifying information, which can be used to locate or identify an individual, and non-identifying information.[54] The Commission's Survey findings demonstrate that nearly all Web sites collect personal identifying information from consumers. Ninety-seven percent of the sites in the Random Sample, and 99% in the Most Popular Group, collect an email address or some other type of personal identifying information.[55] In addition, when the traffic of all sites surveyed is taken into account, there is a 99% chance that, during a one-month period, a consumer surfing the busiest sites on the Web will visit a site that collects personal identifying information (this is the "weighted analysis figure").[56] The Survey data also demonstrate that 68% of sites in the Random Sample, and 77% in the Most Popular Group, collect non-identifying information.[57] The

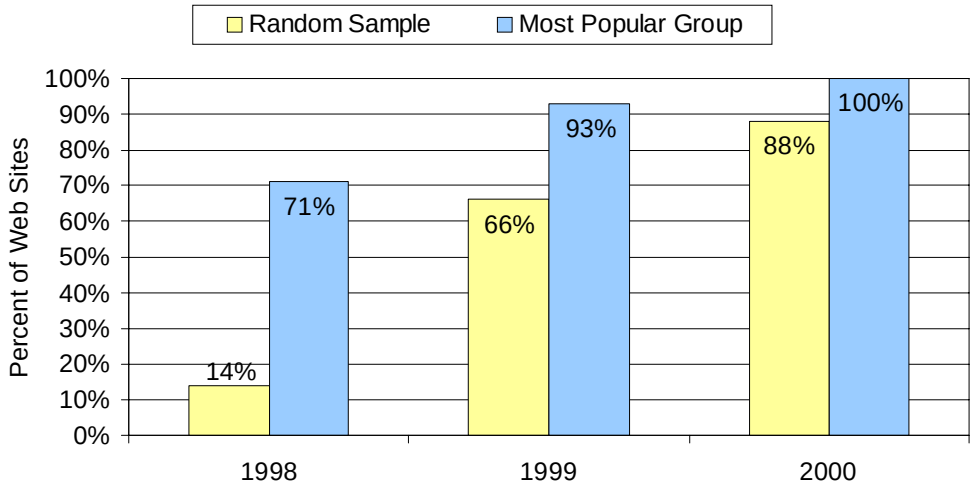
weighted analysis figure is 76%.[58] Most of the sites surveyed, therefore, are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior, or surfing behavior[59] information they collect to personal identifying information.

3. 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 – *i.e.*, either a unified privacy policy or a discrete information practice statement (such as, "This is a secure order form").[60] Sixty-six percent of Web sites in the GIPPS random sample,[61] compared with 14% of Web sites in the Commission's 1998 Comprehensive Sample had such disclosures.[62] 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.[63] Of sites in the Random Sample that collect personal identifying information, 90% post at least one privacy disclosure.[64] All of the sites in the Most Popular Group post at least one privacy disclosure,[65] compared with 93% of the sites in Professor Culnan's 1999 survey of the 100 busiest sites,[66] and 71% in the Commission's 1998 Most Popular Sample.[67] The weighted analysis figure is 96%.[68]

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[69]) and 97% of sites in the Most Popular Group (compared with 81% in the 1999 OPA survey[70]) post a privacy policy.[71] The weighted analysis figure is 82%.[72] 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.

Figure 1
Frequency of Any Privacy Disclosures
(1998-2000)



Base: All Sites in Sample

Source: 1998 Report, App. D, Table 2; 1999 GIPPS Report, App. A, Table 4B; 1999 OPA Report, App. A, Table 3B; Appendix C, Table 2a.

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 *any* 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.

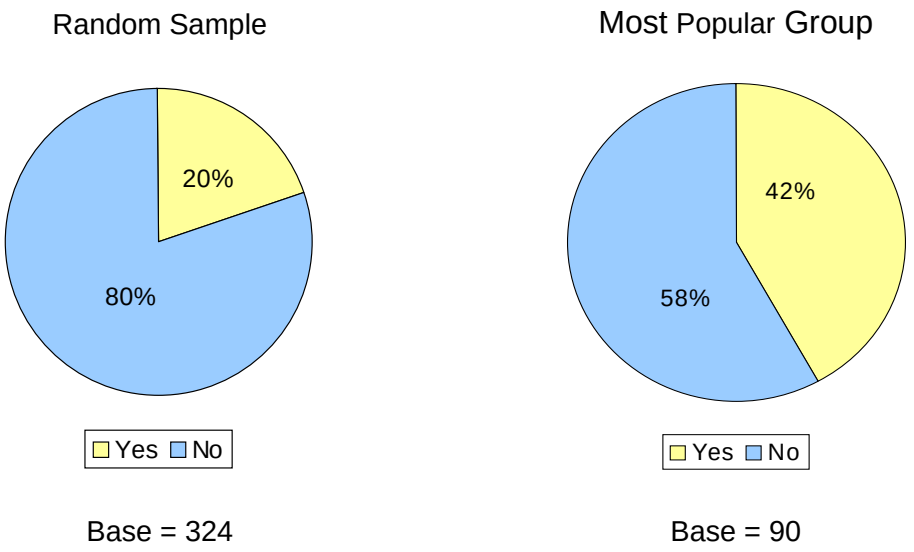
4. CONTENT OF PRIVACY DISCLOSURES: COMPARISON WITH FAIR INFORMATION PRACTICE PRINCIPLES

As discussed above, four key principles have been widely accepted for nearly thirty years as necessary to assuring that information practices are fair and provide adequate privacy protections for consumers: Notice, Choice, Access, and Security.[73] Since 1995, the Commission has actively supported industry self-regulatory efforts to address consumers' privacy concerns, with particular focus in recent years on industry implementation of these fair information practice principles. The Commission's Survey, therefore, included a set of content analysis questions designed to ascertain the extent to which a Web site's privacy disclosures implemented each of these fair information practice principles. In analyzing whether sites' disclosures followed the fair information practices, the Commission focused on sites that collect personal identifying information.[74]

Implementation of All Four Fair Information Practice Principles

Survey results showed that, in the Random Sample, one-fifth, or 20%, of Web sites that collect personal identifying information implement, at least in part, the fair information practice principles of Notice, Choice, Access, and Security.[75] (Figure 2). While this indicates improvement since the release of the GIPPS Report – which found that 10% of sites in the random sample posted disclosures addressing at least one element of each of the four fair information practice principles[76] – it still shows that only a small percentage of sites are providing protection in the core areas. In the Most Popular Group, 42% of Web sites collecting personal identifying information implement, at least in part, each of the fair information practice principles.[77] The weighted analysis figure is 32%.[78]

Figure 2
Of Sites Collecting Personal Identifying Information,
Percent Implementing Notice, Choice, Access & Security

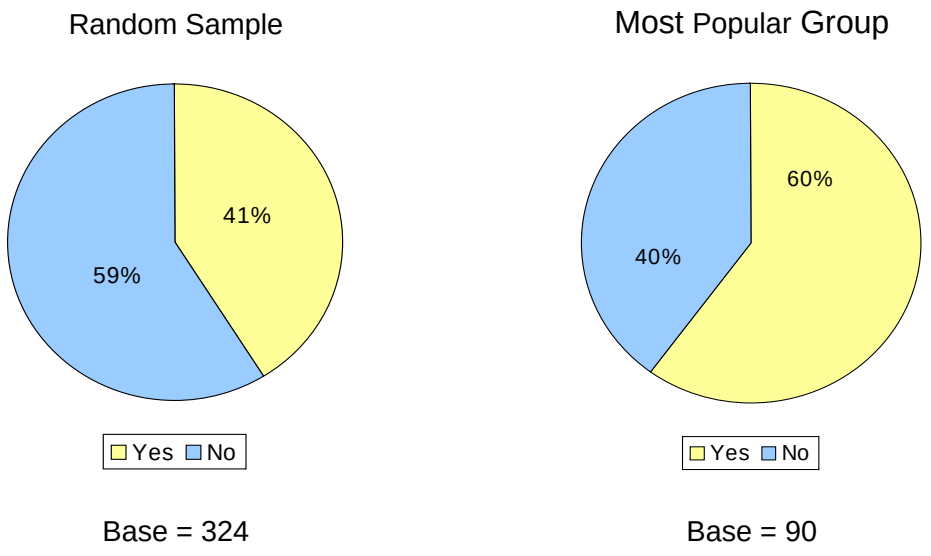


Source: Appendix C, Table 4.

Implementation of Notice & Choice Only

While views about how Web sites should implement Access and Security differ,[79] 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.[80] The weighted analysis figure for Notice and Choice is 58%.[81] Figure 3 shows the proportion of sites collecting personal identifying information in the Random Sample and in the Most Popular Group that meet the Notice and Choice standards.

Figure 3
Of Sites Collecting Personal Identifying Information,
Percent Implementing Notice & Choice



Source: Appendix C, Table 4.

The following discussion describes the types of disclosures for which sites were awarded credit for each of the fair information practice principles of Notice, Choice, Access, and Security, and the results for each principle individually.

Content Analysis Results for Each Fair Information Practice Principle

Notice: The Notice principle is the most fundamental of the fair information practice principles, because it is a prerequisite to implementing other fair information practice principles, such as Choice or Access. As described in more detail in the Commission's 1998 Report, the Notice principle states that consumers should be given clear and conspicuous notice of an entity's information practices before any personal information is collected from them, including: identification of the entity collecting the data, the uses to which the data will be put, and the recipients of the data; the nature of the data collected and the means by which it is collected; whether provision of the requested data is voluntary or required; and the steps taken by the data

collector to ensure the confidentiality, integrity and quality of the data.[82] 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.[83] 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.[84]

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.[85] In the Random Sample, just over one-half, or 55%, of the Web sites that collect personal identifying information follow the Notice principle.[86] The results were significantly better for the Most Popular Group, in which 89% of the Web sites that collect personal identifying information adhere to the Notice principle.[87] The weighted analysis figure is 77%.[88]

Choice: The Choice principle relates to giving consumers options as to how any personal information collected from them may be used for purposes beyond those necessary to complete a contemplated transaction.[89] Under the Choice principle, data collectors must afford consumers an opportunity to consent to secondary uses of their personal information, such as the placement of consumers' names on a list for marketing additional products or the transfer of personal information to entities other than the data collector.[90]

Consumers are very concerned about whether Web sites will share their personal information with other entities. According to one survey, 92% of Internet users would be uncomfortable (67% "not at all comfortable") if a Web site shared their information with other organiza-

tions.[91] In addition, an overwhelming majority of consumers – 88% – want sites to always ask permission before sharing their personal information with others.[92]

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."[93] 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.[94] 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.[95]

Consistent with these consumer concerns, the Commission's Survey included questions about whether sites provide choice with respect to their use of personal information to send communications (other than those related to processing an order) back to consumers ("internal choice"), and whether they provide choice with respect to their disclosure of personal identifying information to other entities, defined in the Survey as "third parties" ("third-party choice").[96] Sites that provide both internal and third-party choice received credit for Choice.[97]

In the Random Sample, one-half (50%) of the sites that collect personal identifying information satisfy the Choice principle.[98] Two-thirds (67%) of the sites in the Most Popular Group provide Choice.[99] The weighted analysis figure is 61%.[100]

Access: The third core principle, Access, refers to an individual's ability both to access data about him or herself – *i.e.*, to view the data in an entity's files – and to contest that data's accuracy and completeness.[101] Access is essential to improving the accuracy of data collected, which benefits both data collectors who rely on such data, and consumers who might otherwise be harmed by adverse decisions based on incorrect data.[102] It also makes data collectors accountable to consumers for the information they collect and maintain about consumers, and enables consumers to confirm that Web sites are following their stated practices.[103]

While Access is widely recognized as an important fair information practice, the Commission believes that Access presents unique implementation issues that require consideration before its parameters can be defined. Specifically, the Commission believes that Access should be "reasonable," and that the costs and benefits of providing access should be considered in defining its scope. As discussed in greater detail below, the Advisory Committee on Online Access and Security was formed to identify these costs and benefits and develop options for the implementation of reasonable access by Web sites. Some of the issues considered by the Advisory Committee include: the scope of access, including what categories of data must be made available;[104] the costs and benefits of providing access;[105] and how to ensure adequate authentication that the person requesting access is the data subject.[106] While the views of Committee members differed on these issues, the Committee was able to identify several options for providing consumers with Access that should inform any determination as to the parameters of "reasonable access."

The Commission's Survey asked three questions about Access: whether the site says that it allows consumers to (1) review at least some personal information about them; (2) have inaccuracies in at least some personal information about them corrected; and (3) have at least some personal information about them deleted.[107] In recognition of the unique implementation issues presented by Access, which were only recently examined by the Advisory Committee, a site was given credit for Access if it provides *any one* of these disclosures. In the Random Sample, 43% of sites that collect personal identifying information post a disclosure relating to review, correction, or deletion of at least some personal information.[108] For the Most Popular Group, 83% provide such an Access disclosure.[109] The weighted analysis figure is 68%.[110]

Although a site received Access credit for disclosures about any one of its three elements (review, correction, or deletion), the Commission believes that fair information practices require that consumers be afforded *both* an opportunity to review information *and* an opportunity to contest the data's accuracy or completeness – *i.e.*, to correct or delete the data.[111] An opportunity to review personal information is consistent with what a majority of consumers want and

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."[112] 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.[113] Based on the work of the Advisory Committee, however, the Commission still believes that the specific terms of Access (*e.g.*, 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.[114] 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.[115] There was also concensus 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."[116] 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.[117]

The Advisory Committee also examined whether, and to what extent, Web sites should make disclosures about security. As discussed in greater detail below,[118] the Committee agreed

that *providing* security is more important than making disclosures about it, but that disclosures could be useful in conjunction with implementing actual security measures.[119] Specifically, the Advisory Committee's report states that a security notice is an appropriate tool for informing consumers about a company's information practices and that such a notice is critical to consumers' ability to make informed choices about such practices.[120] It also states that security disclosures would be most useful if they allow meaningful comparisons between sites, but warns against detailed disclosures, which could confuse consumers and invite security breaches.[121]

The Commission believes that, in addition to taking steps to assure adequate security (including the steps outlined in the Advisory Committee's report), it is important that sites make some disclosures about their security practices in order to enhance consumer confidence and demonstrate sites' commitment to fair information practices. Surveys show that disclosures about online security would encourage consumers to use the Internet more in general, to register at sites, and to purchase products or services from sites.[122] The Commission is mindful, however, of the challenges of providing security notices that are concise, meaningful, and not counter-productive.

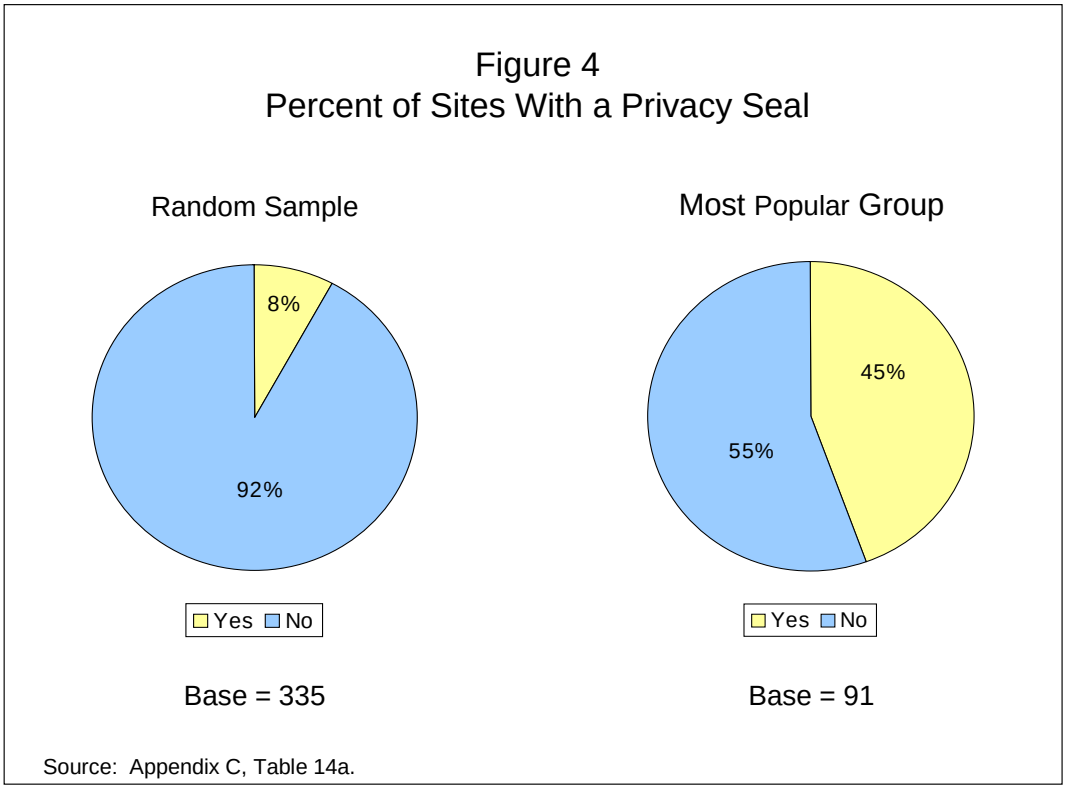
The Commission's Survey asked whether sites disclose that they (1) take any steps to provide security,[123] and if so, whether they (2) take any steps to provide security for information during transmission, or (3) take any steps to provide security for information after receipt.[124] A site was awarded credit for Security if it made any of these disclosures. Slightly more than half, or 55%, of the sites that collect personal identifying information in the Random Sample, and approximately three-quarters, or 74%, of those in the Most Popular Group, post any security disclosure.[125] The weighted analysis figure is 65%.[126]

In light of the Advisory Committee's discussions showing that security is most important once the site has received personal data, the Commission believes that, going forward, sites should post disclosures about security that specifically address the fact that security measures are taken after such receipt.

5. ENFORCEMENT OF FAIR INFORMATION PRACTICE PRINCIPLES

In addition to the substantive fair information practice principles of Notice, Choice, Access, and Security, a fifth principle is essential to ensuring consumer protection: Enforcement.[127] The key enforcement mechanisms to emerge in industry's self-regulatory efforts are the privacy seal programs.[128] This year, Commission staff looked for whether a site displayed a privacy seal, such as the TRUSTe, BBB*OnLine Privacy*, CPA WebTrust, or the Entertainment Software Ratings Board seals. The Survey found that less than one-tenth, or approximately 8%, of sites in the Random Sample display a privacy seal.[129] (Figure 4). The weighted analysis figure is 36%.[130] It also found that of the 27 sites with a privacy seal, approximately one-half (52%) implement, at least in part, all four of the fair information practice principles.[131] Only 63% implement Notice and Choice.[135] Forty-five percent of sites in the Most Popular Group display seals.[133] (Figure 4). Of those 41 sites, 56% implement all four of the fair information practice principles, and 71% implement Notice and Choice.[134]

Figure 4
Percent of Sites With a Privacy Seal



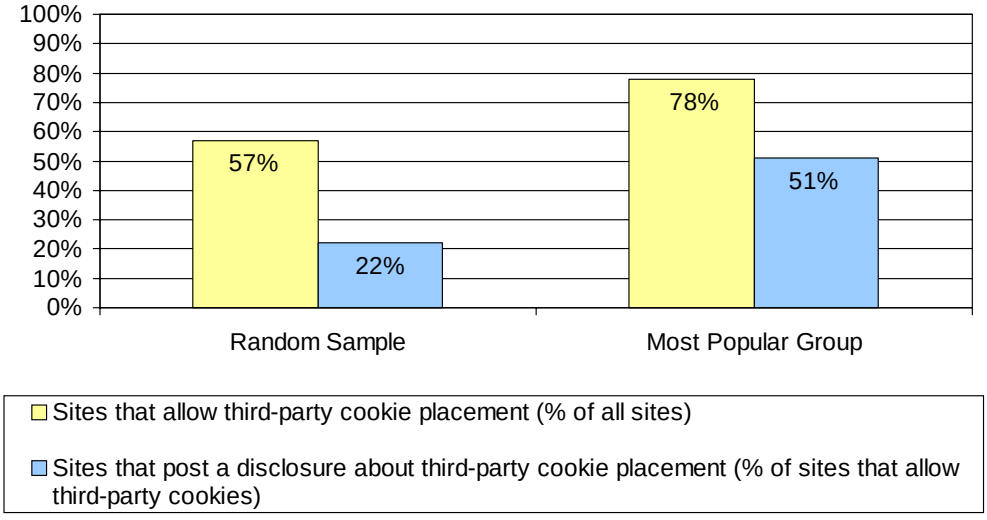
Source: Appendix C, Table 14a.

6. THIRD-PARTY COOKIES

The Commission's Survey also collected data on the number of sites at which a third party, defined as any domain other than the site being surveyed, attempts to place a cookie on the consumer's computer.[135] The Survey findings demonstrate that most sites – 57% of the sites in the Random Sample and 78% of the sites in the Most Popular Group – allow the placement of cookies by third parties.[136] The weighted analysis figure is 69%.[137] The majority of the third-party cookies in the Random Sample and in the Most Popular Group are from network advertising companies that engage in online profiling.[138]

In addition, the majority of Web sites that allow third-party cookies do not disclose that fact to consumers. As shown in Figure 5, only 22% of the sites in the Random Sample at which a third party attempts to place a cookie, and 51% of such sites in the Most Popular group, tell consumers that third parties may place cookies or collect information about them as they visit the site.[139] The weighted analysis figure is 41%.[140]

Figure 5
Third-Party Cookies:
Placement and Disclosure Rates



Source: Appendix C, Tables 15a & b.

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 *some* 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 – *i.e.*, whether it describes *all* of the information the site collects or *all* of the uses made of that information.

Thus, the questions in the content analysis form follow an "at least some" rule: they consistently ask whether a certain practice is true with respect to *at least some* information collected by the site. For example, for Notice, the form asks whether a site identifies *at least one type* of specific information the site collects from consumers, and not whether the site identifies all such information. Similarly, for Access, the form asks whether a site states that it allows consumers to review *at least some* information about them, or to have *at least some* personal information corrected or deleted.

The Survey results described above should be considered in light of this methodology. Thus, with respect to each fair information practice, the results reflect the number of Web sites implementing the practice *at least in part*, but not necessarily in a complete manner.

- With respect to **Notice**, this means that a site received credit if it posts a privacy policy, and identifies at least one specific type of information it collects, at least one use to which such information will be put, and whether any of the information will or will not be shared with third parties. This is so notwithstanding that the Web site may collect many additional pieces of personal information, use that information in many other undisclosed ways, and share some or all of the information in contexts not described in the site's privacy policy.
- With respect to **Choice**, this means that a site received "internal choice" credit if it offers choice for only one type of communication to a consumer, and received "third-party choice" credit if it offers choice for the sharing of only one type of information with third parties, even though the site may, in practice, send other communications and share other information without offering consumers choice.
- With respect to **Access**, a site received credit if it offers the ability to review, correct, or delete at least one item of personal information it has collected – oftentimes simply an opportunity to update an email address – without regard to what other information a site may actually have collected and compiled.

- With respect to **Security**, a site received credit if it makes only a single statement regarding security, regardless of the extent of security precautions taken by a site.

Thus, the Survey results paint a picture that is both simpler and clearer than the underlying reality.

2. CLARITY OF DISCLOSURES

While the objective numbers described above provide a benchmark by which to assess the quantity and content of privacy disclosures, they do not reflect their clarity. Recent news reports have highlighted the often confusing nature of privacy policies,[141] and the staff who reviewed the content of privacy policies reported similar frustration in parsing the sometimes contradictory language of many of these policies. Perhaps as a result of such confusing policies, 64% of consumers have indicated that they do not trust even those sites with posted privacy policies.[142] Whether disclosures are clear and understandable or confusing and misleading is more difficult to quantify than the objective criteria described above. It is clear, however, that many privacy disclosures are internally contradictory, and the data must be assessed with this in mind. The confusion caused by poorly-drafted privacy disclosures can be broadly grouped into three problem areas: contradictory language, unclear descriptions of how consumers can exercise choice, and the possibility of changes to the policy at any time. Each is briefly discussed below.

a. Contradictory Language

As with many consumer disclosures, there is a tension between providing full and accurate information about a site's information practices and providing short and easily understandable disclosures that consumers are likely to read and understand. Many sites appear to reconcile this tension by providing general descriptions of their practices, followed by more detailed descriptions. While such an approach serves to convey the information in a concise format while also providing full disclosure, it can also be confusing if the general description varies

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 (*i.e.*, an "opt-in"), no information will be sent. In the very next sentence, however, the privacy policy states:

> If you prefer not to receive e-mail from [the company] in the future or prefer that your information not be shared with organizations other than [the company] or its affiliates, please feel free to send us an e-mail to that effect as well, and we will do our best to honor your request.

Thus, it appears that the company actually requires consumers to opt-out of receiving communications from the company, and even then there is no guarantee that a consumer's request will be honored (only that the company will do its best to honor the request). Such

contradictory language is likely to confuse consumers and negate the value of posting information practice disclosures.

b. Ambiguous Language Regarding Choice

A second common problem is the use of ambiguous or misleading language in describing how a site implements consumer choice regarding the use of personal information. Often, sites state that information will not be used to contact the consumer, or will not be shared with third parties, without the user's consent or agreement. In practice, however, such "consent" is obtained either through the provision of the information by the consumer (*i.e.*, by providing the information the consumer implicitly agrees to these secondary uses) or by pre-checked "click-boxes" buried at the end of a registration form. In the latter case, a consumer may believe, based on the "consent" language, that he or she need not do anything to prevent the further use of the information. In reality, however, because a click-box had been pre-checked, the consumer is deemed to consent unless he or she unchecks the box.[143] The use of ambiguous language regarding how consumers can exercise choice undercuts the value of offering such choice in the first instance.

c. Changes to Policies

Finally, many privacy policies state that a site reserves the right to make changes to its information practices in the future and urge consumers to check the policy often for such changes. The chance that new, inconsistent policies may be applied to previously collected information is troubling and may undermine consumer confidence in the rest of the privacy policy. In certain circumstances, the application of new information practices to information collected pursuant to different, stated practices may constitute an unfair and/or deceptive practice. At the very least, Web sites should inform consumers whose information they have collected of material changes in their information practices. In some instances, affirmative choice by the consumer may be required.

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 practices. For example, an entity that sometimes shares personal information with third parties should clearly state as much, even if information is not always shared. The details of the entity's disclosure practices can follow the general description, allowing those consumers who want more detail to understand more fully an entity's practices.

The privacy policy should also clearly explain how a consumer can exercise choice over the use of his or her information, rather than simply stating that a consumer's personal information will not be shared without his "consent." Web sites should also strive to provide consumers with Notice and Choice if their information practices change in a material way. Finally, links to a privacy policy, as well as discrete and relevant information practice disclosures, should be prominently displayed on a site's home page and on every page on which personal

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").[144] The Commission asked the Advisory Committee to consider the parameters of "reasonable access" to personal information collected from and about consumers online and "adequate security" for such information. Based on this mandate, the Advisory Committee prepared a report presenting options for implementation of these fair information practices and the costs and benefits of each option.[145] The duties of the Advisory Committee were solely advisory, and were focused only on developing implementation options for Access and Security.[146]

The Commission requested nominations for the Advisory Committee in a Federal Register Notice[147] and appointed forty Advisory Committee members who effectively represented the varied viewpoints on implementing Access and Security online.[148] The Advisory Committee held four public meetings between February and May, 2000.[149] In addition, Advisory Committee members worked in subgroups between meetings to address specific topics in more depth and to draft working papers and sections of the Advisory Committee's report for discussion at the public meetings.[150] The Advisory Committee submitted a final report to the Commission on May 15, 2000, which is bound separately as Appendix D to this Report.

The Commission commends the Advisory Committee for identifying the many challenging issues surrounding implementation of Access and Security, as well as the costs and benefits – to

both businesses and consumers – of various implementation options. As discussed above, the Advisory Committee's discussions and findings are extremely helpful in providing a framework from which to analyze the Survey results and to consider general standards for implementing Access and Security in the future. The Advisory Committee's findings also reveal that the issues raised by implementing Access and Security are indeed complex, and are worthy of further examination. A brief summary of the Advisory Committee's meetings and Report follows.

A. ACCESS

To define "reasonable access," the Advisory Committee focused on such issues as the scope of information to which consumers should have access;[151] the entities that should be obligated to provide consumers access to information about them;[152] and appropriate and feasible means for authenticating access requests to prevent unauthorized access.[153] The Advisory Committee Report acknowledges that implementing the fair information practice principle of Access is a complex task, and there was considerable disagreement among members as to how "reasonable access" should be defined, including whether access should vary with the use or type of data.[154] The Report states that providing the consumer with access to information can promote accuracy and safeguard against errors or fraud in various circumstances,[155] although members disagreed on the circumstances under which access should be provided and the data to which consumers should have access.[156] Some members believed that allowing consumers to review all types of information held by businesses, including marketing data and data from offline sources linked to data collected online, is essential;[157] others believed that "reasonable access" should be interpreted only as a framework for the correction of data used in making important decisions about a consumer.[158]

The Advisory Committee Report presents four options for defining the scope of access: 1) the "total access" approach; 2) the "default to consumer access" approach; 3) the "case-by-case" approach; and 4) the "access for correction" approach. Under the "total access" ap-

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.[159] 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.[160] The principle underlying this approach is that businesses' information practices should be completely transparent to consumers.[161]

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."[162] 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.[163] The "unreasonable burden" concept helps define what is and what is not retrievable in the ordinary course of business.[164] 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.[165] 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.[166]

Under the "case-by-case" approach, access would depend on factors such as the content of the information, the holder of the information, the source of the information, and the likely use of the information.[167] Differences in industry sectors would also be considered.[168] Under this approach, there is no presumption for or against access, and implementation could result in broad or narrow access.[169] For example, consumers could have access to sensitive information collected about them, such as financial and health data,[170] but consumers may have less access to other data, such as inferred data and internal identifiers.[171]

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.[172] Examples of personal information used to grant or deny significant benefits include credit reports, financial qualifications, and medical records.[173]

The Advisory Committee Report also evaluates whether the Access principle should apply to entities other than the original data collector.[174] Members of the Advisory Committee generally agreed that businesses should provide access to data held by their agents.[175] 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.[176] Others believed that this requirement would be too burdensome.[177]

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 – *e.g.*, 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.[178] 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.[179] 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.[180]

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,"[181] and the managerial and technical measures that should be undertaken to protect information from unauthorized use or disclosure.[182] 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.[183] 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.[184]

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."[185] 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.[186] 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.[187]

In addition, as noted above,[188] 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.[189] 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.[190] The Report also states that a

security disclosure could be more useful if it allows consumers to compare security among sites in an understandable way.[191] It warns against providing too many technical details, however, which could aid hackers in attacking the Web site, and also states that it may be difficult to convey useful information in a short statement dealing with a subject as complex as computer security.[192] These findings have been extremely useful in analyzing the Survey results, and in considering whether Web sites should be given Security credit for a disclosure that alerts consumers to the fact that a Web site has taken any steps to provide security.

Like the implementation options set forth for Access, the security options provide valuable guidance, and should be considered in any determination as to the parameters of "adequate security."

IV. COMMISSION RECOMMENDATIONS

The Internet provides a host of opportunities for businesses to gather a vast array of personal information from and about consumers. It also provides unprecedented opportunities for compiling, analyzing, and disseminating such information. While American businesses have always collected some data from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of unprecedented amounts of data that can be used for myriad subsequent purposes. It is the prevalence, ease, and relatively low cost of such information collection and use that distinguishes the online environment from more traditional means of commerce and information collection and thereby raises significant consumer privacy concerns.[193]

A. CURRENT FTC AUTHORITY

The Commission's authority over the collection and dissemination of personal data collected online stems from Section 5 of the Federal Trade Commission Act (the "FTC Act" or "Act"),[194] and the Children's Online Privacy Protection Act ("COPPA"), which governs the collection of information from children under the age of 13.[195] The FTC Act prohibits unfair

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.[196] 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 information practice principles on their Web sites, or portions of their Web sites, not directed to children.

B. SELF-REGULATION

The Commission has long encouraged industry to address consumer concerns regarding online privacy through self-regulation. The Commission's efforts to encourage self-regulation have included bringing industry and consumer and privacy advocates together to address online privacy issues in public workshops, and meeting with, and encouraging, industry leaders to adopt effective self-regulatory programs. These efforts have been based on the belief that greater protection of personal privacy on the Internet will benefit businesses as well as consumers by increasing consumer confidence and participation in the online marketplace.

In its 1998 testimony before Congress, the Commission stated that is was "hopeful that self-regulation [would] achieve adequate online privacy protections for consumers."[197] The Commission, however, also "recognize[d] that there [were] considerable barriers to be surmounted for self-regulation to work."[198] Specifically, the Commission noted that "an effective enforcement mechanism is crucial" to the success of self-regulation, and that "it [would] be difficult for self-regulatory programs to govern all or even most commercial Web sites."[199] Nevertheless, in light of industry efforts at that time, the Commission recommended that Congress refrain from passing legislation. The Commission noted, however, that unless industry

could demonstrate that it had developed and implemented broad-based and effective self-regulatory programs, additional government authority in this area might be necessary.[200] 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.[201]

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.[202]

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,[203] 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.[204] 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 (*e.g.*, 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 (*e.g.,* 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.

ENDNOTES

1. The appendices to the Report contain a detailed methodology describing how the Survey was conducted (Appendix A), the Survey instruments and the raw data (Appendix B), and tables representing the results of the Commission's data analysis (Appendix C). Appendix D, the Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security, is bound separately.

2. The Intelliquest Technology Panel, *Panel News*, available at <http://www.techpanel.com/news/index.asp> [hereinafter "Technology Panel"] (90 million adult online users as of third-quarter 1999). Other sources place the number in the 70-75 million user range. *See* Cyber Dialogue, *Internet Users*, available at <http://www.cyberdialogue.com/resource/data/ic/index.html> (69 million users); Cyberstats, *Internet Access and Usage, Percent of Adults 18+*, available at <http://www.mediamark.com/cfdocs/MRI/cs_f99a.cfm> (75 million users).

3. Technology Panel. This represents an increase of over 15 million online shoppers in one year. *See id.*

4. Ernst & Young/Technometrica, *Survey of E-Commerce & Consumer Trust* (Oct. 5, 1999) (unpublished survey on file with the Commission). Other studies estimate that between 27% and 48% of online users have purchased products or information online. *See* The Gallup Organization, *Poll Releases* (Feb. 23, 2000), available at <http://www.gallup.com/poll/releases/pr000223.asp> (48%); Business Week/Harris Poll, *A Growing Threat*, available at <http://www.businessweek.com/2000/00_12/b3673010.htm?scriptFramed.> (some results also available in BUSINESS WEEK, Mar. 20, 2000, at 96) [hereinafter "Business Week/Harris Poll"] (45%); Cyber Dialogue, *E-commerce*, available at <http://www.cyberdialogue.com/resource/data/ecom/index.html> [hereinafter "Cyber Dialogue E-Commerce Survey"] (36%); Technology Panel (27%). In any event, the number is significantly higher than in prior years. *See, e.g.,* Business Week/Harris Poll (increase from 31% to 45%); Technology Panel (increase from 22% to 25%).

5. United States Department of Commerce News, *Retail E-commerce Sales for the Fourth Quarter 1999 Reach $5.3 Billion, Census Bureau Reports* (Mar. 2, 2000), available at <http://www.census.gov/mrts/www/current.html>.

6. Shop.org News, *Online Retailing in North America Reached $33.1 Billion in 1999 and Is Projected to Top $61 Billion in 2000* (Apr. 17, 2000), available at <http://www.shop.org/nr/00/042000.html> ($33.1 billion); The Yankee Group, *The Online Holiday Shopping Market* (Dec. 1999), available at <http://www.yankeegroup.com/webfolder/yg21a.nsf/press/23369333DF5755388025684100 4208EB?OpenDocument> ($24.2 billion); Forrester Research, Inc., *Online Retail to Reach $184 Billion by 2004 as Post-Web Retail Era Unfolds* (Sept. 1999), available at <http://www.forrester.com/ER/Press/Release/0,1769,164,FF.html> ($20.2 billion).

7. Forrester Research, Inc., *NRF/Forrester Online Retail Index* (Jan. 2000), available at <http://www.forrester.com/ER/Press/Release/0,1769,253,FF.html>. These numbers

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/Nielsen Media Demographic and Electronic Commerce Study*, 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., *Young Net Shoppers Soar Ahead of Online Adults* (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 Revenues Soar to $4.6 Billion in 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. *Id.* 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, *IAB Internet Advertising Revenue Report: Executive Summary 1999 Third-Quarter Results*, available at <http://www.iab.net/news/content/3Q99exec.html>.

9. IAB 1999 Revenue Report.

10. Internet Advertising Bureau, *Internet Advertising Bureau Announces 1996 Advertising Revenue Reporting Program Results* (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, *Personalized Marketing and Privacy on the Net: What Consumers Want*, PRIVACY AND AMERICAN BUSINESS at 11 (Nov. 1999) [hereinafter "Westin/PAB 1999"]. *See also IBM Multi-National Consumer Privacy Survey* 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., *Online Consumers Fearful of Privacy Violations* (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. *See also* 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 the use of their personal information); Alan F. Westin, *Report on the IBM-Harris Multi-National Consumer Privacy Survey*, PRIVACY AND AMERICAN BUSINESS at 11 (Jan. 2000) [hereinafter, "2000 Westin Report"] (61% of U.S. Internet users have refused to purchase because of privacy concerns); Christopher M. Kelley, *The Privacy Best Practice*, Forrester Research, Inc. (Sept. 1999) [hereinafter, "Forrester Privacy Best Practice Report"] (48% of consumers who are "very concerned" about privacy do not shop on the Web; concerned consumers who do shop online spend 21% less than consumers who are not concerned about privacy).

15. AARP, *Many Americans Face E-Commerce Skills Gap* (Mar. 2000), available at <http://www.aarp.org/press/2000/nr033000.html> (24% of computer users age 45 and over who have never purchased online cite privacy as the key reason).

16. Forrester Privacy Best Practice Report (cited in Microsoft Advertisement, N.Y. TIMES, Mar. 23, 2000, at A12).

17. Sandeep Junnarkar, *Report: Half of Net Users Mistrust Sites*, CNET News.com (Aug. 17, 1999), available at <http://home.cnet.com//category/0-1007-200-346152.html> [hereinafter "CNET News"] (citing results of study by Jupiter Communications, Inc.); *see* Jupiter Communications, Inc., *Overview: Proactive Online Privacy: Scripting an Informed Dialogue to Allay Consumers' Fears*, available at <http://www.jup.com>.

18. *Survey Shows Few Trust Promises on Online Privacy*, Apr. 17, 2000, available at <http://www.nyt.com> (citing recent Odyssey survey).

19. In the last few months, at least five major publications have featured articles about online privacy. *See* BUSINESS WEEK, Mar. 20, 2000; THE INDUSTRY STANDARD, Mar. 13, 2000; Smart Computing in English, GUIDE TO PC PRIVACY, vol. 8, issue 4; CONSUMER REPORTS, May 2000 (part one of a series); THE NEW YORK TIMES MAGAZINE, Apr. 30, 2000.

20. The Commission, of course, recognizes that other consumer concerns also may hinder the development of e-commerce. As a result, the agency has pursued other initiatives such as combating online fraud through law enforcement efforts. *See FTC Staff Report: The FTC's First Five Years Protecting Consumers Online* (Dec. 1999). The Commission, with the Department of Commerce, is also holding a public workshop and soliciting comment on the potential issues associated with the use of alternative dispute resolution for online consumer transactions. *See* Initial Notice Requesting Public Comment and Announcing Public Workshop, 65 Fed. Reg. 7,831 (Feb. 16, 2000); Notice Announcing Dates and Location of Workshop and Extending Deadline for Public Comments, 65 Fed. Reg. 18,032 (Apr. 6, 2000). The workshop will be held on June 6 and 7, 2000. Information about the workshop, including the federal register notices and public comments received, is available at <http://www.ftc.gov/bcp/altdisresolution/index.htm>.

21. The Commission held its first public workshop on privacy in April 1995. In a series of hearings held in October and November 1995, the Commission examined the implications of globalization and technological innovation for competition and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices regarding the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission held a second workshop in June 1997 to explore issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

    The Commission and its staff have issued reports describing various privacy concerns in the electronic marketplace. *See, e.g.*, *Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997); *FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996) [hereinafter "December 1996 Staff Report"]; *FTC Staff Report: Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996). Recently, at the request of the Department of Health and Human Services ("HHS"), the Commission submitted comments on HHS' proposed Standards for Privacy of Individually Identifiable Health Information (required by the Health Insurance Portability and Accountability Act of 1996). The Commission strongly supported HHS' proposed "individual authorization" or "opt-in" approach to health providers' ancillary use of personally identifiable health information for purposes other than those for which the information was collected. The Commission also offered HHS suggestions it may wish to consider to improve disclosure requirements in two proposed forms that would be required by the regulations. The Commission's comments are available at <http://www.ftc.gov/be/v000001.htm>.

    The Commission also has brought law enforcement actions to protect privacy online pursuant to its general mandate to fight unfair and deceptive practices. *See FTC v. ReverseAuction.com, Inc.,* No. 00-0032 (D.D.C. Jan. 6, 2000) (settling charges that an online auction site obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); *Liberty Financial Companies, Inc.*, FTC Dkt. No. C-3891 (Aug. 12, 1999) (challenging the allegedly false representations by the operator of a "Young Investors" Web site that information collected from children in an online survey would be maintained anonymously); *GeoCities*, FTC Dkt. No. C-3849 (Feb. 12, 1999) (settling charges that Web site misrepresented the purposes for which it was collecting personal identifying information from children and adults).

    Finally, the Commission has recently issued a rule implementing the privacy provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.* *See* 16 C.F.R. Part 313, available at <http://www.ftc.gov/os/2000/05/glb000512.pdf>.

22. *See infra* 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 *supra,* 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. *See FTC v. Rapp*, No. 99-WM-783 (D. Colo. filed Apr. 21, 1999); *In re Trans Union*, Docket No. 9255 (Feb. 10, 2000), *appeal docketed*, 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. *Privacy Online: A Report to Congress* at 7-14 (June 1998), available at <http://www.ftc.gov/reports/privacy3/index.htm> [hereinafter "1998 Report"]. *See also* 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, *Personal Privacy in an Information Society* (1977); Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: *Principles for Providing and Using Personal Information* (1995); U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995); *The European Union Directive on the Protection of Personal Data* (1995); and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

26. 1998 Report at 7-11.

27. *Id.* at 23, 27.

28. *Id.* at 42-43. In October 1998, Congress passed the Children's Online Privacy Protection Act of 1998. 15 U.S.C. §§ 6501, *et seq*. 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

personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

As required by the Act, in October 1999 the Commission issued a rule to implement the Act's fair information practice standards. The rule became effective on April 21, 2000, 16 C.F.R. Part 312, and is available at <http://www.ftc.gov/opa/1999/9910/childfinal>.

29. Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web" before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, U.S. House of Representatives (July 21, 1998), available at <http://www.ftc.gov/os/1998/9807/privac98.htm> [hereinafter "1998 Testimony"].

30. The results for the random sample of 361 Web sites are reported in *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission* (June 1999), available at <http://www.msb.edu/faculty/culnanm/gippshome.html> [hereinafter "GIPPS Report"]. The results of Professor Culnan's study of the top 100 Web sites, conducted for the Online Privacy Alliance, are reported in Online Privacy Alliance, *Privacy and the Top 100 Sites: Report to the Federal Trade Commission* (June 1999), available at <http://www.msb.edu/faculty/culnanm/gippshome.html> [hereinafter "OPA Report"].

31. *See* GIPPS Report, Appendix A, Table 8C .

32. *Self-Regulation and Privacy Online* (July 1999), available at <http://www.ftc.gov/os/1999/9907/index.htm#13> [hereinafter "1999 Report"].

33. 1999 Report at 12-14.

34. Online profiling is the practice of aggregating information about consumers' interests, gathered primarily by tracking their movements online, and using the resulting consumer profiles to deliver targeted advertisements on Web sites. The transcript of the Workshop, as well as public comments filed in connection with the workshop, are available at <http://www.ftc.gov/bcp/profiling/index.htm>.

35. The Advisory Committee was established in December 1999, pursuant to the Federal Advisory Committee Act, 5 U.S.C. App. § 9(c). Members were selected in January 2000, and the Advisory Committee's first meeting was held in February 2000. Advisory Committee documents, including transcripts of meetings, drafts of subgroup documents, public comments, and other materials, are all available at <http://www.ftc.gov/acoas/index.htm>.

36. A description of the key components of several of these programs is included in the 1999 Report. 1999 Report at 9-12.

37. *Id.* at 9.

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*Online* 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. *Id.*

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. *See infra* p. 20 and accompanying notes.

44. In this study, we define "Web site" as a domain, the unit of analysis for the Survey. *See* 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, *see, e.g.,* <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. *See* 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. *See* 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%. *See* 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. *Id.*

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. *See* 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 *disclosed* 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 address, phone or fax number, Social Security number, or credit card number. Non-identifying information includes information, such as age, gender, education level, income, hobbies, and interests, which *alone* (*i.e.*, when not combined with other information) cannot be used to locate or identify individuals.

55. Appendix C, Table 1. These results are slightly higher than those for the previous two years. In 1998, 92% of sites in the Comprehensive Sample, and 97% in the Most Popular, collected personal identifying information. *See* 1998 Report, Appendix D, Tables 3 and 4. Last year, 93% of sites in the Random Sample (GIPPS Report, Appendix A, Table 2B), and 98% in the busiest 100 (OPA Report, Appendix A, Table 1B), collected personal identifying information.

56. Appendix C, Table 1.

57. *Id.*

58. *Id.*

59. Surfing behavior, such as the Web pages that a consumer visits and the amount of time he or she spends there, the ad banners viewed, and the frequency of visits to the site, is commonly referred to as "clickstream" data. Clickstream data is gathered through cookies and other non-obvious means. As noted above, the Survey did not assess whether the sites surveyed (as opposed to third parties) gathered clickstream data.

60. *See supra* n.48.

61. GIPPS Report at 8.

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.

63. Appendix C, Table 2a.

64. Appendix C, Table 3.

65. Appendix C, Table 2a.

66. OPA Report at 8.

67. 1998 Report, Appendix D, Table 2.

68. Appendix C, Table 2a.

69. GIPPS Report, Appendix A, Table 4B.

70. OPA Report, Appendix A, Table 3B.

71. Appendix C, Table 2a. Most, but not all, sites that have a privacy policy provide a link to it from the home page. Seventy-six percent of those sites with a privacy policy in the Random Sample (which represents 47% of all sites in the sample) and 94% of those in the Most Popular Group (91% of all sites in the group) link to the policy from the home page. Appendix C, Table 2b.

72. Appendix C, Table 2a.

73. 1998 Report at 7-10.

74. As discussed in greater detail in Section II.C, the content analysis assessed whether each fair information practice was implemented with respect to *at least some* information collected by a Web site, and does not purport to represent full adherence to each of the fair information practices for *all* information collected. Furthermore, the findings of this Survey are limited to whether Web sites posted privacy disclosures and what those privacy disclosures said. They do not address the Web sites' actual conduct, *i.e.*, whether sites in fact follow the practices disclosed or the fair information practice principles.

75. Appendix C, Table 4.

76. *See* GIPPS Report, Appendix A, Table 8C. The GIPPS survey asked questions about elements of each of the fair information practice principles, and then determined whether the disclosures found reflected any of these elements. The Notice elements included whether the site said anything about what information was collected, how information was collected, how information collected would be used, whether the information would be re-used or disclosed to third parties, and its use or non-use of cookies. The Choice elements included statements regarding choice offered with respect to the site's use of information to market back to the consumer and the site's disclosure of non-aggregate personal information disclosed to third parties. Access included statements that the site

allowed consumers to review or to ask questions about information collected, and statements about how inaccuracies were handled. Finally, Security included statements about steps to provide security for information during transmission or after it was received by the site. GIPPS Report at 9. If a site's privacy disclosures included at least one element for a particular fair information practice principle (*e.g.*, Notice, Choice, Access, or Security), the site was credited as reflecting that principle.

As discussed below, the Commission's Survey examined whether sites address essential elements of each of the principles, not simply whether sites address a *single* element of each principle, and thus is not directly comparable to the GIPPS survey. If, however, the Survey results were analyzed using a scoring model comparable to that used in the GIPPS survey (differences still remain, as the questions in the two surveys are not identical, and some questions were asked in one survey but not the other), 25% of sites in the Random Sample that collect personal identifying information would receive credit for making disclosures regarding Notice, Choice, Access, and Security.

77. Appendix C, Table 4. The 1999 OPA Report found that 22% of the 100 busiest sites posted disclosures addressing at least one element of each of the four fair information practice principles. *See* OPA Report, Appendix A, Table 6C. If the Survey results were analyzed using the OPA survey scoring model, 57% of sites in the Most Popular Group that collect personal identifying information would receive credit for making disclosures regarding Notice, Choice, Access, and Security.

78. Appendix C, Table 4.

79. For example, *see* Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security (May 15, 2000) [hereinafter "Advisory Committee Report"] at 5.

80. Appendix C, Table 4.

81. *Id.*

82. 1998 Report at 7-8.

83. IBM Privacy Survey at 104-05, 121-23 (finding that 85% of Internet users believe that it is very important or absolutely essential that sites post a privacy policy and provide notice); Business Week/Harris Poll (finding that 96% of online consumers that have ever seen a privacy policy consider it somewhat important, very important, or absolutely essential that sites post a privacy policy and provide notice). Both surveys also found that approximately half of consumers report having seen a privacy policy, and most of those report that they read the policy. IBM Privacy Survey at 104, 117; Business Week/Harris Poll.

84. IBM Privacy Survey at 98-100.

85. Appendix B, Surf Survey Form at Q2; Content Analysis Form at Q10, 11, 15. *See infra* n.96 for the definition of "third parties." The results for each element of Notice individually are found in Appendix C, Table 5.

The Commission's Survey also asked whether sites disclose that they use cookies, which is a disclosure that may relate to *how* information is collected from consumers (also an important element of Notice). Appendix B, Content Analysis Form at Q24-25. Forty-six percent of sites in the Random Sample and 87% of sites in the Most Popular Group post a disclosure about their use or non-use of cookies. Appendix C, Table 6.

86. Appendix C, Table 4.

87. *Id.*

88. *Id.*

89. 1998 Report at 8-9.

90. *Id.* at 16.

91. Business Week/Harris Poll.

92. *Id. See also* IBM Privacy Study at 105, 124-25 (81% of Internet users believe that having a choice to not have their name and address passed along to other companies for sending them marketing offers is "absolutely essential" or "very important").

93. Business Week/Harris Poll. Forty-one percent of online consumers reported being "very" concerned. *Id.*

94. *Id.* In 1998, 65% of online buyers and 86% of Internet users who had not bought online reported being concerned about spam. *Id.*

95. Lorrie Faith Cranor, *et al.*, *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, AT&T Labs-Research Technical Report TR 99.4.1 at 10-11 (Apr. 14, 1999), available at <http://www.research.att.com/projects/privacystudy/> [hereinafter "AT&T Privacy Study"] (removal from a site's mailing list upon request was important even to consumers who were only "marginally concerned" about privacy, with 76% rating this ability as "very important").

96. Appendix B, Content Analysis Form at Q12-17. For purposes of the Survey, a "third party" was defined as "[a]ny entity other than the assigned domain. Examples: advertisers, affiliates, subsidiaries, business partners, or other companies." Appendix B, Instructions for Content Analysis Form at 2.

    The Survey also asked whether the form of choice was an opt-in or an opt-out. *Id.* at Q14, 17. Survey results for the internal and third-party choice questions, including the type of choice offered, are reported in Appendix C, Tables 7-9.

97. An express statement that the site does not use personal information to market back to the consumer or disclose personal identifying information to third parties was included as credit for internal and third-party choice, respectively. Statements that the site only discloses personal identifying information as required by law or as necessary to process the consumer's order, or that information is disclosed only in aggregate or non-identifying form, were included as statements that the site does not disclose personal identifying information to third parties. *See* Appendix B, Content Analysis Form at Q16.

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%, *see supra* p. 12), and 54% would receive credit for meeting Notice & Choice (compared with 41%, *see supra* 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%, *see supra* p. 12), and 87% would receive credit for meeting Notice & Choice (compared with 60%, *see supra* p. 13). Appendix C, Table 10.

100. Appendix C, Table 4.

101. 1998 Report at 9.

102. *Id. See also* Advisory Committee Report at 13.

103. *See* Advisory Committee Report at 9.

104. *See id.* at 5-6; 8-14.

105. *See id.* at 4-14.

106. *See id.* at 15-18.

107. Appendix B, Content Analysis Form at Q18-20. The results for each element of Access individually are found in Appendix C, Table 11.

108. Appendix C, Table 4.

109. *Id.*

110. *Id.*

111. This standard is consistent with the standard for Access set forth in the 1998 Report. 1998 Report at 9. If Access were scored in this manner, only 18% of sites in the Random Sample, and 47% of sites in the Most Popular Group, would receive credit for Access. Further, only 11% of sites in the Random Sample, and 27% of sites in the Most Popular Group, would have been credited with meeting all four fair information practice principles (compared with 20% and 42%, respectively, *see supra* p. 12). Appendix C, Table 12.

112. IBM Privacy Study at 105, 124-25. *See also* Westin/PAB 1999 at 11-12 (83% of Internet users consider the ability to review online profiles about themselves and to remove information from those profiles as important, with 70% rating these access features as "absolutely vital" or "very important").

113. Many Committee members also agreed that Access is an important framework for addressing data inaccuracies. *See* 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. *See also* Advisory Committee Report at 22-23, 26.

115. Advisory Committee Report at 19.

116. *Id.* at 26.

117. Advisory Committee Transcript of February 4, 2000, at 127 (S. Baker, Steptoe & Johnson), available at <www.ftc.gov/acoas>; *id.* 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. *See id.* at 20.

120. *Id.* at 20.

121. *Id.* 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 purchase products or services if sites provided security disclosures. *Id.*

123. For example, a general statement that "We implement measures to protect the security of your information" was credited as a security disclosure.

124. Appendix B, Content Analysis Form at Q21-23. The results for elements of Security individually are found in Appendix C, Table 13.

125. Appendix C, Table 4.

126. *Id.*

127. 1998 Report at 10-11.

128. *See* Section I.D, *supra*.

129. Appendix C, Table 14a.

130. *Id.*

131. Appendix C, Table 14b.

132. *Id.*

133. Appendix C, Table 14a.

134. Appendix C, Table 14b.

135. The Survey did not collect information on the *number* of third parties that attempt to place cookies at a particular site. *See* Appendix A at 5.

136. Appendix C, Table15a.

137. *Id.*

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. *Id.*

141. *Our Four Point Plan*, BUSINESS WEEK, Mar. 20, 2000, at 86-87; CNET News; *see also* THE INDUSTRY STANDARD, Mar. 13, 2000, at 208-09; *Big Browser is Watching You!*, CONSUMER REPORTS, May 2000, at 43, 47.

142. Jupiter Communications, Inc., *Jupiter Communications: 64 Percent of Online Consumers Are Unlikely to Trust a Web Site* (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; *Association of American Physicians and Surgeons, Inc. v. Clinton*, 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 Advisory Committee's public Web site. Meetings were held on February 4, February 25, March 31, and April 28, 2000. The meeting date and agenda were announced in the Federal Register fifteen days prior to the meeting. The Federal Register Notice meeting announcements are available at <http://www.ftc.gov/acoas>. More detailed agendas were posted about two weeks before each meeting and are also available at <http://www.ftc.gov/acoas>.

150. Draft outlines, working papers, and draft sections of the Advisory Committee Report were posted on the Advisory Committee Web site as they were developed and are available at <http://www.ftc.gov/acoas>. The Advisory Committee also reviewed and considered public comments throughout the process. The list of public comments submitted (and links to each comment) is available at <http://www.ftc.gov/acoas/comments/index.htm>.

151. Advisory Committee Report at 4-6, 8-14.

152. *Id.* at 6-8.

153. *Id.* at 15-18.

154. *See id.* at 4-14.

155. *Id.* at 4.

156. *See id.* at 5.

157. *Id.* at 9.

158. *Id.* at 13-14.

159. *Id.* at 9.

160. *See id.* at 5-6 (defining personal information). "Inferred or derived data" is information that the business has not collected either passively or actively from the user, but rather has inferred, using data about a sample population (inferred data), or information gathered from or about the individual subject (derived data). *Id.* at 6.

161. *Id.* at 9.

162. *Id.* at 10.

163. *Id.*

164. *Id.*

165. *See id.*

166. *Id.*

167. *Id.* at 11.

168. *Id.*

169. *Id.* at 11-12.

170. *Id.* at 12.

171. *Id.*

172. *Id.* at 13.

173. *Id.* at 14.

174. *Id.* at 6-8.

175. *Id.* at 7.

176. *Id.*

177. *Id.*

178. *See id.* at 16.

179. *Id.* at 15.

180. *Id.*

181. *Id.* at 21-26.

182. *Id.*

183. *Id.* at 19.

184. Advisory Committee Transcript of February 4, 2000, at 127 (S. Baker, Steptoe & Johnson), available at <www.ftc.gov/acoas>; *id.* 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. *Id.* at 21-26.

186. *Id.* at 26.

187. *Id.* at 25.

188. *See* Section II.B.4 *supra*.

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. *Id.* at 20.

190. *Id.* at 20.

191. *Id.*

192. *Id.* at 20-21. For these reasons, the Report states that it is not possible to judge the adequacy of security at Web sites by performing a "sweep" that focuses on the presence or absence of notices. *Id.* at 21. While the Commission recognizes that a security disclosure, by itself, does not necessarily ensure a thorough security program, it believes that a security disclosure is essential to informed consumer choice, and serves to enhance consumer confidence.

193. As noted earlier, *supra* n.23, and as illustrated by legislative decisions made in the areas of medical and financial privacy, offline privacy issues are also significant.

194. 15 U.S.C. §§ 41 *et seq*.

195. 15 U.S.C. §§ 6501 *et seq*. The COPPA, which took effect on April 21, 2000, governs the collection of information from children under the age of 13 at Web sites, or portions of Web sites, directed to children or which have actual knowledge that a user from which they seek personal information is a child under 13 years old. The legislation proposed below would apply to those Web sites or portions of Web sites to the extent not governed by the COPPA.

196. *See supra* n.21.

197. 1998 Testimony.

198. *Id.*

199. *Id.*

200. *Id.*

201. 1999 Report at 12.

202. For example, the program administered by the National Advertising Division of the Council of Better Business Bureaus, Inc. ("NAD") is a model self-regulatory program that complements the Commission's authority to regulate unfair and deceptive advertising. The NAD expeditiously investigates complaints made by consumers or competitors about the truthfulness of advertising. An advertiser that disagrees with the NAD's conclusion may appeal to the National Advertising Review Board ("NARB"), which includes members from inside and outside the advertising industry. The vast majority of disputes handled by the NAD and NARB are resolved without government intervention, resulting in greater respect for and enforcement of the law at a substantial savings to the taxpayer. Those disputes that the NAD and NARB are unable to resolve are referred to the Commission.

    The Commission also has a long record of working with industry to develop and disseminate informational materials for the public. *See, e.g.*, Notice of Opportunity to Participate and Obtain Co-Sponsorship in Agency Public Awareness Campaign re: Children's Online Privacy Protection Rule, available at <http//:www.ftc.gov/os/2000/05/index.htm#12>.

203. 5 U.S.C. § 553.

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

DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE
in *Privacy Online: Fair Information Practices in the Electronic Marketplace*
A Report to Congress

I dissent from this embarrassingly flawed Privacy Report and its conclusory — yet sweeping — legislative recommendation.[1] In an unwarranted reversal of its earlier acceptance of a self-regulatory approach, a majority of the Commission recommends that Congress require **all** consumer-oriented commercial Web sites that collect personal identifying information from consumers to adopt government-prescribed versions of all four fair information practice principles ("FIPPs"): Notice, Choice, Access, and Security.[2] The majority abandons a self-regulatory approach in favor of extensive government regulation, despite continued progress in self-regulation.

The majority recommends that Congress give rulemaking authority to an "implementing agency" (presumably the Commission) to define the proposed legislative requirements "with greater specificity," to "expand on what constitutes 'reasonable access' and 'adequate security'" and to "examine the specific contours of the Choice requirement . . ." (Privacy Report ["PR"] at 37). In some cases, the Report explains, the agency engaged in rulemaking might determine that "reasonable access" means "no access" despite the recommended statutory direction to provide access. (*Id.*). The Commission owes it to Congress — and the public — to comment more specifically on what it has in mind before it recommends legislation that requires all consumer-oriented commercial Web sites to comply with breathtakingly broad laws whose details will be filled in later during the rulemaking process.

Most disturbing, the Privacy Report is devoid of any consideration of the costs of legislation in comparison to the asserted benefits of enhancing consumer confidence and

[1]To assist readers, a list of the topics I address is appended to my dissenting statement.

[2]While this is a reversal for the Commission, Commissioner Anthony has consistently preferred a legislative approach. *See* Statement of Commissioner Sheila F. Anthony, Concurring in Part and Dissenting in Part, *Self-Regulation and Privacy Online* (July 1999), available at <http://www.ftc.gov/os/1999/9907/index.htm#13>.

allowing electronic commerce to reach its full potential. Instead, it relies on skewed descriptions of the results of the Commission's 2000 Survey and studies showing consumer concern about privacy as the basis for a remarkably broad legislative recommendation. It does not consider whether legislation will address consumer confidence problems and why legislation is preferable to alternative approaches that rely on market forces, industry efforts, and enforcement of existing laws.

In fact, the 2000 Survey demonstrates continued noteworthy growth in the display of privacy notices and, for the first time, provides a qualitative assessment of the content of privacy notices. The survey results, despite their flaws, show continued development of self-regulatory privacy policies that are, for the most part, not yet comprehensive when measured against the 2000 Survey yardstick. **Why?** As discussed below, the Privacy Report makes no attempt to answer this vital question, but instead leaps to the conclusion that legislation is needed.

The majority's Report concludes that the 2000 Survey numbers "demonstrate" that industry self-regulatory efforts are insufficient. (PR at 35). It makes no attempt to determine **why** the figures warrant changing course to advocate legislation. Instead, the Report concludes that legislation is needed because self-regulation "**cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders.**" (PR Executive Summary at ii-iii) (emphasis added). When has self-regulation ever ensured that every member of an industry will adopt industry standards? If this is the Commission's new standard for successful self-regulation, then no numbers can ever be high enough to meet it. Using such logic leads inevitably to government regulation.

To the extent that Access and Security disclosures are less prevalent than expected, the Survey results are consistent with the implementation difficulties identified by the Advisory

Committee on Access and Security in that Committee's report.[3] The Choice figures, while much higher than the Access and Security figures, also are not surprising in light of the unanticipated complexities of implementing a far more limited version of opt-out Choice required by the Gramm-Leach-Bliley ("G-L-B") Act for protecting the privacy of consumers' financial information.[4] Reports that many companies are exiting the business of providing services to children online to avoid the burdens of complying with regulations issued under the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501 *et seq.*, also should raise a red flag about the wisdom of proceeding to mandate Choice and Access for all commercial consumer-oriented Web sites.[5]

Nor did the 2000 Survey attempt to measure whether sites actually provide Access and Security; rather, it gauged only whether disclosures addressed these issues. And the 2000

[3]In 1999, the Commission established an Advisory Committee on Online Access and Security to provide advice and recommendations to the Commission regarding implementation of reasonable access and adequate security by domestic commercial Web sites. The Committee provided the final version of its report to the Commission on May 15, 2000, describing options for implementing reasonable access to, and adequate security for, personal information collected online and the costs and benefits of each option. The Advisory Committee report is appended to the Privacy Report.

[4]The Commission, along with other agencies involved in implementing the G-L-B Act's privacy provisions, has found it necessary to extend the deadline for compliance with the implementing regulations by more than seven additional months to provide sufficient time for financial institutions to establish new policies, procedures, and systems for implementing regulatory requirements. Federal Trade Commission, Final Rule, Privacy of Consumer Financial Information, available at <http://www.ftc.gov/os/2000/05/glb000512.pdf>.

[5]The COPPA regulations require detailed Notice; Access, including the ability to review, correct, and delete information maintained by the site; and a form of opt-in mandated Choice (verifiable parental consent). 16 C.F.R. §§ 312.4, 312.6(a)(1), 312.6(a)(2), 312.5(a), 312.5(b). The regulations went into effect on April 21, 2000, and already press reports state that some small online companies have stopped providing services to children because implementation of COPPA's requirements is too costly. *See, e.g.*, "New Children's Privacy Rules Pose Obstacles for Some Sites," *The Wall Street Journal* (April 24, 2000) at B-8 (reporting one attorney's estimate that it will cost her clients between $60,000 and $100,000 annually to meet COPPA standards); "New privacy act spurs Web sites to oust children," William Glanz, *The Washington Times* (April 20, 2000), available at < *See also* "COPPA Lets Steam out of Thomas," Declan McCullagh, *Wired News* (May 16, 2000), available at <wysiwyg://1/http://www.wired.com/news/politics/0,1283,36325,00.html>.

Survey certainly did not give any credit for "No Access," even though the majority indicates it might consider no access to be "reasonable Access" in some instances.

Why does the Privacy Report not analyze why the 2000 Survey figures are too low to avert legislation? Perhaps it is because the 2000 Survey results, like the Advisory Committee's report, are not really the basis for the Commission's startling legislative recommendation. The Commission has barely had time to review, much less digest, the detailed report issued by the Advisory Committee earlier this week, including the very illuminating statements of individual members of the Committee.[6] Apparently, the majority views the Committee's report as something for an implementing agency to consider **later**, when it writes regulations detailing how **all commercial, consumer-oriented Web sites** are to comply with laws requiring them to provide "reasonable access" and "reasonable security." I, on the other hand, think the Advisory Committee's report is an incredibly valuable contribution to self-regulation and urge Congress to consider it fully before enacting legislation — something the Commission has failed to do before recommending legislation. Notably, the Advisory Committee's report does **not** recommend government action.

Nor do there appear to be independent reasons supporting the majority's broad legislative recommendation. Legislation should be reserved for problems that the market cannot fix on its own and should not be adopted without consideration of the problems legislation may create by, for example, imposing costs or other unintended consequences that could severely stifle the thriving New Economy. What is the problem to be solved here? Is it abuse of privacy online

[6]Stewart Baker points out in his concurring statement that the FTC refused to share the results of the 2000 Survey with the members of the Advisory Committee because the survey results were too confidential. Nonetheless, details about the survey results and the staff recommendation for legislation leaked to The Wall Street Journal, as reported on Thursday, May 11, 2000, and confirmed by FTC spokesman Eric London, indicated that the Commission's study of online privacy ignored the lessons of the Advisory Committee's report. Concurring Statement of Stewart Baker, Steptoe & Johnson LLP, Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security (May 15, 2000). *See also* Separate Statement of Jerry Cerasale appended to Advisory Committee Report (noting that any recommendation for government access likely was determined before the Committee issued its report).

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%. (*Id.*).

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

Next, the 2000 Survey presents a unique and demanding measurement of the quality and detail of privacy disclosures based on the four FIPPs. When the 2000 Survey gives credit for "Notice," it requires a level of notice that satisfies four distinct requirements: (1) the site 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. When the 2000 Survey results refer to "Choice," it means that the site did two things: (1) it stated that it provided the consumer an option to authorize or agree to the site's use of personal information to send communications back to the consumer (or stated that it did not use personal information in this way); and (2) it stated that it provided an option to authorize or agree to the disclosure of personal identifying information to third parties (or stated that it did not disclose personal identifying information to third parties).

In partial recognition of the complexities of these issues, Access and Security were measured by simpler standards. When the 2000 Survey concludes that a site provided "Access," it means that the site stated that it did at least one of three things: it allowed consumers to review, delete, or correct at least some personal information. "Security" means that the site explicitly stated that it takes steps to provide security. As the Privacy Report acknowledges, providing security is more important than disclosing it.[7] **The 2000 Survey did not attempt to measure whether sites actually provide security (or access, for that matter), but only whether privacy disclosures addressed them in the parameters described above.**

[7]PR at 19; *see also* Advisory Committee Report at 19-20.

C. Disclosures Addressing Individual Fair Information Practice Principles Are Widespread

NOTICE: The survey results show that **55%** of sites in the Random Sample and **89%** of the Most Popular sites meet all four Notice requirements. (PR Appendix C, Table 4).

CHOICE: **82%** of the sites in the Random Sample and **98%** of the Most Popular sites provide some form of choice for either sending communications to customers or disclosing information to third parties. (PR Appendix C, Table 10). **50%** of the Random Sample sites provide both types of choice, as do **67%** of the sites in the Most Popular Group. (PR Appendix C, Table 4).

ACCESS: **43%** of the Random Sample sites and **83%** of the Most Popular Group sites provide disclosures indicating that they provide some form of access. (PR Appendix C, Table 4).

SECURITY: **55%** of the Random Sample sites and **74%** of the Most Popular Group sites display a statement that the site takes steps to provide security. (PR Appendix C, Table 4).

Thus, when looked at in terms of adherence to individual fair information practice principles, the Random Sample numbers are fairly high and the Most Popular Group figures are substantially higher.

D. Comprehensive Privacy Policies that Provide All Four Elements of FIPPs Are Less Common

When the Privacy Report combines all four of the 2000 Survey's Notice, Choice, Access, and Security measurements to determine what sites have disclosures satisfying all four fair information practice principles, however, the results are much lower: **20%** of the Random Sample Web sites and **42%** of the Most Popular Web sites. (PR Appendix C, Table 4). If the Access and Security measurements are not considered, then **41%** of the sites in the Random Sample and **60%** of the Most Popular sites provide the four-element Notice and both types of Choice. (*Id)*. These numbers rise even more when sites are credited for providing choice either for internal uses or for disclosures to third parties: **54 %** of sites in the Random Sample and **87%** in the Most Popular Group. (PR Appendix C, Table 10). Treating Choice in this

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

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 apples-to-oranges comparison, because the 1999 surveys did not define Notice, Choice, Access, and Security to include the more demanding elements required by the Privacy 2000 survey. (PR at 12 nn. 76-77).

As acknowledged in footnotes 79 and 80 of the Privacy Report, the scoring models are not identical because the surveys asked different questions. **Using the most comparable approach possible in light of this significant limitation, the 2000 Survey's full FIPPs numbers rise to 25% and 57%. This apples-to-apples comparison shows a dramatic one-year improvement.** Nonetheless, the majority's Report chooses not to highlight this more direct comparison, instead measuring the 20% of the Random Sample Web sites that implement **all of the 2000 Survey's specified elements** for Notice, Choice, Access and Security against the 1999 survey that found 10% of sites had posted disclosures addressing **at least one element** of Notice, Choice, Access, and Security. *(See* PR Executive Summary at i).

B. Measuring Success on the Basis of Full FIPPs Is Irrational

Based on the many difficulties of implementing Access and Security, discussed in detail below, the Privacy Report's use of full FIPPs as the yardstick for success is irrational. It should be noted that even in the sensitive area of protecting personal financial information, the Congress did not insist on all four FIPPs in the G-L-B Act. Once beyond sensitive financial and medical information, the importance of Access arguably diminishes. Had the 2000 Survey

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.[8] The majority has arrived at its 82% figure by adding

[8]Odyssey, *Consumers' Internet Privacy Concerns: Lip Service or Limiting Factor?* (2000) ("Odyssey Study") at 2.

the percentages of online households that strongly agreed and somewhat agreed, something that the Odyssey authors themselves did not do.

Moreover, the Odyssey survey's method of describing consumers' views is unusual and somewhat biased in favor of "agree" responses, because it gives two possible answers that use the word "agree" and only one possible answer to "disagree." (Odyssey Study at 2, Chart 1). Typically in a survey the points used in a three-point scale would be labeled something like: (1) agree; (2) neither agree nor disagree; and (3) disagree. A typical four-point scale would have labels along the lines of: (1) strongly agree; (2) somewhat agree; (3) somewhat disagree; and (4) strongly disagree. In the Odyssey survey, only one category — "strongly disagree" — is available for consumers who have only weak opinions but tend to disagree. Since they do not "strongly" disagree, such consumers might say they "somewhat agree," even though that is not an accurate portrayal of their views. The Odyssey survey method pushes consumers to "agree" categories and captures consumers in the "somewhat agree" category who may simply tend more to "somewhat disagree" (a choice not offered by the survey). In these circumstances, the Privacy Report's addition of the "strongly agree" and "somewhat agree" responses is very misleading.

b. IBM Privacy Survey Example

Regardless of the extent to which consumers are concerned about privacy online, the available data do not support the conclusion that these concerns are causing any significant lost online sales. The Report also cites the IBM Privacy Survey as support for the proposition that "surveys show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce." (PR at 2 n.14). Specifically, the Report observes 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." (PR at 15 n.84).

On its face, the IBM Privacy Survey does not demonstrate that there have been or will be a significant number of lost sales online because of privacy concerns. The survey treats as a

positive response any consumer who has **ever** been dissuaded from making **any** purchase online from the relevant type of Web site.[9] 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 *do* buy spend 21% less online than their more at-ease counterparts, leaving $2.8 billion on the table in 1999."[10] It did not explain, however, how

[9]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).

[10]Christopher M. Kelley, et al., *The Privacy Best Practice*, 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.[11] 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.**

ii. Jupiter Proactive Online Privacy Study

Even worse, the Report relies — as a basis for legislation — on a projection of "potential losses of up to $18 billion by 2002 (as compared to a projected total of $40 billion in online sales), if nothing is done to allay consumer concerns." (PR at 2). The Report cites to an overview of a study that Jupiter Research Services released in June 1999. (PR at 2 n.17).[12] **The data supporting the statements in the Jupiter Study are at least a year old and, since industry self-regulation has made significant progress since June 1999, the Jupiter lost sales projections are clearly not applicable today**.[13]

The overview on which the Privacy Report relies does state that Jupiter projects a "[l]oss of $18 billion in Commerce Revenue" due to privacy concerns. But the overview also explains that the forecast is that such revenue losses will be suffered "**unless** [Web sites] take a more proactive approach and engage in an informed dialogue to shape and allay consumers' fears" (emphasis added) and contains a heading that states "A Do-Nothing Approach Will Lead to Significant Revenue Loss."

Here, the Report makes a quantum leap in logic, misleading Congress by going beyond simply selectively citing the Jupiter Study overview. It fails to consider the complete Jupiter

[11]Conversation between my staff and Christopher M. Kelley, Forrester Research (May 17, 2000).

[12]Specifically, the Report cites a press item dated August 17, 1999, which, in turn, quotes from the Jupiter Study. The Report also cites the overview of the Jupiter Study available at Jupiter's Web site to registered users. (PR at 2 n.17).

[13]The online overview of the Jupiter Study warns purchasers of its research that "[a]ll opinions and projections are based on Jupiter's judgment at the time of the publication and are subject to change."

Study.[14] 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."[15]**

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.[16] 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."[17] **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."[18]** These figures clearly cut against the Privacy Report's recommendation for rulemaking.

---

[14]Michele Slack, Jupiter Communications, *Proactive Online Privacy, Scripting an Informed Dialogue to Allay Consumers' Fears* (June 1999).

[15]Jupiter Study at 12-13 and Figure 9 (emphasis added).

[16]*See* Jupiter Study at 16.

[17]*Id.* at 19.

[18]*Id.* at 4.

iii. Legislation Is Not Needed and in Fact May Cause Lost Sales

Assuming for the sake of argument that privacy concerns are causing some lost online sales, it is far from clear that government intervention is the appropriate response. First, some of the same consumer surveys that purport to show that privacy concerns are causing lost online sales also appear to indicate that government intervention is not needed to allay consumers' privacy concerns.[19] Moreover, government regulation of online privacy obviously will impose substantial costs on online sellers that might very well reduce their online sales or induce firms to offer fewer products for sale or go out of business entirely — an offsetting reduction in online commerce that the Report entirely ignores.

iv. "Lost" Sales Are Not Really Lost

Finally, a lost online sale is not a complete loss to the economy. Again, assuming for the sake of argument that consumers have been dissuaded from making purchases online because of privacy concerns, the most likely response of these consumers would be to purchase the same item from an offline retailer. Of course, switching to an offline retailer in this situation may not be the optimal economic outcome, because transaction costs might be lower if consumers make the purchase online. Offline retailers might be able to free-ride on the services provided by online retailers. Nevertheless, the fundamental point remains that overlooking offline sales that offset a lost online sale overstates the economic effect of the lost online sale.

v. The Meaning of Surveys Showing Consumer Unease Is Unclear

Consumer surveys often are poor predictors of consumers' actual behavior. The growth of online commerce despite growing consumer awareness and concern about online privacy

[19]For example, the Odyssey study reports that "82% of online shoppers say they would be more likely to shop at an online retailer that promised not to reveal their personal information to third parties." Odyssey Study at 3. The study notes that for such privacy promises to be credible, it is "absolutely essential" that online retailers communicate clearly to consumers what privacy policies are in place and adhere to those policies. *Id.* at 3-4. The study concludes that "it appears that the security and privacy policies of successful online retailers today are adequate to provide for continued growth in electronic commerce." *Id.* at 4. Consequently, the Odyssey study does not support the majority's position that more government regulation is needed to prevent lost sales resulting from online privacy concerns.

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.[20] 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.

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

A. The Report Does Not Adequately Credit Self-Regulatory Efforts

The Privacy Report's emphasis on seal programs overshadows other corporate efforts. **Corporate leaders** including IBM, Microsoft, Disney, Intel, Procter and Gamble, Novell, and Compaq have voluntarily committed to requiring their advertising partners to post high-quality privacy policies in order to receive advertising monies.

Microsoft has committed to developing business and consumer tools based on the Platform for Privacy Practices Protocol ("P3P"). The business tool known as the Privacy Statement Wizard is intended to enhance the ability of Web site operators to present their privacy statements both as human and as machine-readable documents. A related consumer tool, the Privacy Manager Wizard, is intended to enhance consumers' abilities to state their personal information privacy preferences. An early version of the Privacy Statement Wizard has been on the market for just over a year and has allowed over 15,000 companies to craft their own online privacy practices by answering a questionnaire.

Associations also have stepped up to the plate. On May 8, 2000, the CEOs of theglobe.com, Yahoo!, Inc., America Online, Lycos, Inktomi , Excite@Home**,** eBay, DoubleClick, Amazon.com, and EMusic.com, wrote a letter on behalf of NetCoalition.com to the CEOs of the Top 500 Web sites urging them to take the initiative to ensure that their companies establish and promote the adoption and implementation of rigorous voluntary privacy policies. NetCoalition.com led the way during the 1999 holiday shopping season, sponsoring a "Consumer Privacy Education Campaign" to empower Internet users with practical information about online privacy. The campaign included over 50 million impressions with banner ads and site impressions.

The Online Privacy Alliance ("OPA") continues to play a leading role serving as an industry coordinator and a general information resource. The OPA has taken significant strides toward alerting consumers and businesses about the value of privacy protection, as well as how to provide substantive protective measures. In December 1999, OPA disseminated a video

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 communication methods to state and local chambers to educate them about the importance 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 active involvement in educating their own members about the importance of online privacy.

In October and November 1999, the Software & Information Industry Association ("SIIA") undertook a comprehensive outreach program in which it contacted all of its member companies that did not have a privacy policy linked from the company home page. SIIA sent each company a letter encouraging them to develop fair information practices and to post a privacy policy online. In addition, SIIA provided each company with resources and information through an online "toolkit" on its web site and devoted the entire April issue of its association magazine to the issue of online privacy.

The Electronic Retailing Association ("ERA") joined 35 associations in March, 2000 to urge each of their member companies to post a simple, straightforward privacy policy. As a condition of membership, ERA member companies are required to abide by ERA's Online Marketing Guidelines.

Many other associations that have endorsed and promoted self-regulatory solutions to online privacy including the Information Technology Association of America ("ITAA"), Information Technology Industry Council ("ITI"), Business Software Alliance ("BSA"), Computer & Communications Industry Association ("CCIA"), Computer Systems Policy Project ("CSPP"), Consumer Electronics Association ("CEA"), Electronic Industries Alliance ("EIA"), Semiconductor Industry Association ("SIA"), and the Telecommunications Industry Association ("TIA").

My discussion of these organizations is by no means intended to be comprehensive, but merely to demonstrate the extent to which the majority's Privacy Report ignores ongoing, significant industry self-regulation and promotion of privacy online.

B. The Report Ignores Developments in Technology

The market for privacy protection is growing and companies are responding with a host of technological tools. In addition to P3P, which will allow consumers to communicate 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.

Technology can be one part of the solution to consumers' online privacy concerns. But the majority's Privacy Report does not consider the existence, or the likely impact of, such technological tools on consumer privacy online before recommending a legislative attempt to address consumer concerns. The market is working here: consumers are demanding tools to protect privacy and merchants are competing to provide them.

C. The Report Fails to Identify and Consider the Costs and Benefits of Proposed Legislation

The most fundamental flaw in the Privacy Report is its failure to address the costs and benefits of the legislation it proposes. While I cannot undertake a comprehensive analysis myself, a few observations are appropriate.

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."**[21]

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

[21]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.

Report at 15). Indeed, "[g]iving access to the wrong person could turn a privacy policy into an anti-privacy policy." (*Id.* at 4). In light of this, liability concerns may be preventing sites from providing Access. The Advisory Committee's report also observes that authentication of a consumer's identity before allowing that consumer Access could have considerable costs, including to the consumer's ability to remain anonymous. *(Id.)* Given the complexities and risks of Access, it is not surprising that Web sites have not implemented Access more broadly. Unlike the Commission, some may have been waiting to consider the findings of the Advisory Committee.

4. Security

As the Advisory Committee observes (and the Commission acknowledges in footnote 192 of the Privacy Report), **it is impossible to judge the adequacy of Web site security by surveying the presence or absence of security notices on Web sites.** (Advisory Committee Report at 15). Many sites may actually provide security, yet not inform consumers that they do so. The Commission majority's Report notes that security disclosures can enhance consumer confidence and are essential to informed consumer choice. (PR at 33 n.192). Indeed, "security notices are ineffective standing alone." (Advisory Committee Report at 21). Why, then, should the Privacy Survey's results measuring the frequency of security disclosures — not whether security is actually provided — be given any weight in assessing the progress of self-regulation of privacy online?

Security disclosures, particularly regarding the security of credit card information, might help increase consumer confidence. Yet this is a far cry from legislatively mandating the provision of "reasonable security" by Web sites and asking regulators to decide later what security is and is not "reasonable." The honest companies will provide security to satisfy their customers; the dishonest ones will simply not comply. There was no agreement among the

Advisory Committee members that the government should mandate security standards or that the Commission should be setting security standards.[22]

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." *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 758-59 (1985) (plurality opinion); *Trans Union Corp.*, 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

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

governmental interest asserted; and (4) whether the regulation is narrowly drawn to advance the governmental interest asserted. *Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n of New York*, 447 U.S. 557, 561-63 (1980).

The Privacy Report provides no analysis of whether the governmental restrictions that it recommends would survive judicial scrutiny under the test articulated in *Central Hudson* and its progeny. It articulates no reasoned and documented basis for the conclusion that the recommended restrictions would directly and materially advance the governmental interest in protecting the privacy of consumers. Moreover, the Privacy Report presents no basis for the conclusion that the recommended restrictions are narrowly drawn to protect such privacy. Indeed, the Report does not present any information as to whether alternative legislation — for example, providing for Notice only — would protect the privacy of consumers yet impose a lesser burden on the exercise of commercial speech. In my view, we should not recommend that the Congress impose restrictions on commercial speech without conducting the necessary legal and factual analysis to state with confidence that the restrictions would survive judicial review.

7. Enforcement

It boggles the imagination to think about how the comprehensive regulatory scheme envisioned by the majority might be enforced. By enacting the broad statutory requirements recommended by the majority, Congress will create a new universe of law violators, most of whom are arguably innocent of harming consumers or other wrongdoing. Remember that **all** consumer-oriented commercial Web sites would be required to comply with the four FIPPs as implemented by government regulation.

Although a majority of the Commission suggests that self-regulation will continue to play a role in enforcement — perhaps through a mechanism like the dispute resolution and referral process of the National Advertising Division of the Council of Better Business Bureaus (PR at 36 n.202) — what is glaringly absent from the majority's recommendation is any type of safe

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.

LIST OF HEADINGS

III. WHAT DOES THE REPORT FAIL TO DO?

A. The Report Does Not Adequately Credit Self-Regulatory Efforts

B. The Report Ignores Developments in Technology

C. The Report Fails to Identify and Consider the Costs and Benefits of Proposed Legislation

1. ***Notice***
2. ***Choice***
3. ***Access***
4. ***Security***
5. ***Competitive Effects***
6. ***Constitutional Issues***
7. ***Enforcement***
8. ***Offline Privacy***

IV. WHERE DO WE GO FROM HERE?

STATEMENT OF COMMISSIONER THOMAS B. LEARY CONCURRING IN PART AND DISSENTING IN PART

Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress

Today the Federal Trade Commission recommends that Congress enact legislation to help consumers protect their privacy when transacting business on the Internet. I agree that some legislation is appropriate, but believe that the recommendation in the Report endorsed by a majority is too broad in one respect and too narrow in another. The recommendation is too broad because it suggests the need for across-the-board substantive standards when, in most cases, clear and conspicuous notice alone should be sufficient. The recommendation is too narrow because any legislation should apply to offline commerce as well.

The Report's recommendation is based, in part, on our common belief that the Internet has enormous potential to grow our economy; that this potential is inhibited to some degree by consumers' concerns about their privacy; and that it is an appropriate policy objective to address these concerns and encourage growth. So far, so good. The issue, then, is how best to address these privacy concerns in an evenhanded way. If the Internet is subjected to requirements that do not apply pro tanto to offline commerce, the regulatory imbalance could itself inhibit the growth of the Internet and undercut our common objective.

We also agree unanimously that, whatever government does or does not do, the private sector will have an important role to play. The majority looks at the 2000 Web Survey data and concludes that the private sector has failed to address privacy concerns rapidly enough. I am not convinced that the Survey supports this conclusion, but agree, for other reasons, that some legally mandated privacy protections would be appropriate.

The Survey does not necessarily demonstrate that the market has failed to respond to consumer demand. It only measures "inputs," the prevalence of privacy policies of various kinds; it does not measure "outputs," the impact that these policies have on consumer confidence and consumer behavior. The Survey numbers could be read to support alternative

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,[1] 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 (*see* 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,

[1] Jupiter Communications, *Proactive Online Privacy: Scripting An Informed Dialogue to Allay Consumers' Fears*, 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,[2] 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

---

[2] *See* 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. *See* 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.[3]

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 (*see, e.g.*, 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 privacy provisions. These are matters that Congress can and should investigate on its own, but our Report does not provide any help. It is one thing to recognize that the fair information practices (beyond adequate notice) are laudable goals and to encourage their adoption by various self-certifying industry groups. These certifying programs can make a valuable contribution by reinforcing consumers' confidence and reducing consumer costs of obtaining information. It is quite another thing to urge that the practices, in one form or another, be mandated by legislation and by rules.[4]

---

[3] This limitation may not apply to products that are hazardous to health and safety, and this is one reason why there are also affirmative disclosure requirements to deal with these risks.

[4] I acknowledge that previous Commission reports to Congress, which advocated a "wait and see" policy, have suggested that legislation could be appropriate if the fair information practices were not more broadly adopted. I would not have endorsed that aspect of the previous reports either, had I been here.

When the Commission issued the Green Guides, it expressly disclaimed any authority or intention to achieve a substantive result:

> The Commission does not have a statutory mandate to set environmental policy. It is not the Commission's goal, for example, to require that product [sic] be "recyclable." Rather, any Commission cases, rules, or guides would be designed to address how such terms may be used in a non-deceptive fashion in light of consumer understanding of the terms.[5]

These disclosure-oriented guides did have a substantive effect; later public comments indicated that they did "encourage manufacturers to improve the environmental characteristics of their products and packaging," while "allowing flexibility for manufacturers to improve the environmental attributes of their products and to communicate these improvements to consumers."[6] Better information did lead to a better market outcome. In my view, we should follow the precedent of the Green Guides, and not request the authority to issue substantive standards.

The fact that the fair information practices have been favorably regarded in the regulatory community for almost thirty years (Report at 8-9), does not justify mandatory legislation. A provenance from the 1970s is scant cause for comfort, because government regulators, here and throughout the world, had much less faith in free market institutions then than they have today.[7] Moreover, it cannot be claimed that the fair information practices are "widely-accepted" in the business community (Report at 8). Our own Survey of the Internet world demonstrates the

[5] Request for Public Comments on Issues Concerning Environmental Marketing and Advertising Claims and Pending Petitions, 56 Fed. Reg. 24,968 (1991).

[6] Guides for the Use of Environmental Marketing Claims, Final Rule, 61 Fed. Reg. 53,311, 53,313 (1996).

[7] *See, e.g.*, Daniel Yergin and Joseph Stanislaw, *The Commanding Heights: The Battle Between Government and the Marketplace that is Remaking the Modern World* (1998).

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.[8]

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 *both* an opportunity to review information *and* an opportunity to contest the data's accuracy or completeness — *i.e.,* to correct or delete the data." (Report at 32). This is an extraordinarily broad claim, which could in many cases lead to vast expense for trivial benefit and which provides an ominous portent for the content of any substantive rules.

Even "choice," which at first glance seems only a natural corollary of "notice" is a complicated subject. The Report recognizes, for example, that it may be appropriate to provide affirmative benefits if a consumer agrees to certain personal disclosures (Report at 61). If the collection of data is one thing that makes it possible for a vendor to offer lower prices, consumers who are particularly tender of privacy would otherwise be able to free ride on the value created by those who are not. (If a supermarket issues a card that offers discounts to

[8] The Commission's own Internet privacy policy, which can be readily accessed by a click on the Commission's home page, provides notice only. The Commission does protect consumer privacy. It complies with the Privacy Act of 1974, a statute that applies fair information practice principles to the federal government's collection and use of information. 5 U.S.C. §§ 552a *et seq*. However, the Commission's privacy policy does not provide information about choice, access or security measures.

people who use it, in exchange for compilation of useful data, consumer "choice" surely does not involve the right to get the discount without supplying the data.[9])

On the other hand, if the premium for permission to use information is too generous, or the penalty for refusal too severe, consumer "choice" really involves nothing more than the "choice" to refuse dealings with the vendor. The issue of what is or is not a reasonable price differential is complicated, but may be too difficult to bother with in a situation where a particular vendor competes with a number of others that have their own policies. Does this mean that reasonableness should depend on the market power of the vendor?

Other examples could be cited to illustrate the difficulties involved in fashioning substantive rules about choice, access and security, but there is no need to burden this statement further. Congress can, and should, explore these issues in detail if it takes up this aspect of the Report's legislative recommendation.

I therefore believe that any across-the-board legislative mandate should be confined to notice alone, although disclosure rules might appropriately provide that notice include information about the other categories. In some cases, involving particular kinds of information or particular uses, the risk of harm may be so great that specific substantive standards are required. This is a legislative judgment. Congress can, and already does pass industry-specific legislation to deal with these situations.[10] In addition, I believe it is entirely appropriate for the Commission to impose more specific restrictions as "fencing-in" relief in a consent settlement, in order to discipline the future behavior of business entities that have misused consumer information in the past.

---

[9] This use of an offline example is deliberate because the logic is not dependent on the mode of collection. *See* discussion, *infra* pp. 9-10.

[10] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.*; Telecommunications Act of 1996, 47 U.S.C. §§ 222 *et seq.*; Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710 *et seq.*; Cable Communications Policy Act of 1984, 47 U.S.C. §§ 551 *et seq.*; Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.*

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" (*Id.*); 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. (*See* 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

offline. The distinction between online and offline privacy is illogical, impractical and potentially harmful.[11] Let me examine each of these points in turn.

Recognition of the privacy concerns specific to e-commerce should not obscure the fact that in significant respects online privacy concerns are identical to those raised by offline commerce. The same technology that facilitates the efficient compilation and dissemination of personal information by online companies also allows offline companies to amass, analyze and transfer vast amounts of consumers' personal information.[12] Offline companies collect and compile information about consumers' purchases from grocery stores, pharmacies, retailers, and mail order companies, in particular.

It is also not possible to distinguish offline and online privacy concerns on the basis of the nature of the information collected. With the exception of online profiling, it is the same information. The Report's recommendation would require Amazon.com to comply with the fair information practice principles but not the local bookstore which can compile and disseminate the same information about the reading habits of its customers. The consumer polls, upon which the Report places such significant reliance, demonstrate that consumer concerns about the disclosure of personal information are not dependent on how the data has been collected.[13]

Moreover, it is impractical to maintain such a distinction. Businesses are likely to have a strong incentive to consolidate personal information collected, regardless of the mode of

---

[11] Chairman Pitofsky has expressed some of these views in one of his own speeches. *See* Robert Pitofsky, *Electronic Commerce and Beyond: Challenges of the New Digital Age*, Speech before the Woodrow Wilson Center, Sovereignty in the Digital Age Series, Washington, D.C. (Feb. 10, 2000).

[12] Abacus, a consortium of mail order companies, is a good example of the ability of merchants to compile and share detailed data about consumers' purchasing habits. *See In re Trans Union*, Docket No. 9255 (Feb. 10, 2000), *appeal docketed*, No. 00-1141 (D.C. Cir. Apr. 4, 2000).

[13] *See IBM Multi-National Consumer Survey, prepared by Louis Harris Associates Inc.,* at 22-24 (October 1999).

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.[14] 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.[15]

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,

---

[14] Dana James, *Synchronizing the Elements; Traditional Companies, Yearning to Catch Up on the Basics, Find Value in Merging Online, Offline Databases*, Marketing News, Feb. 14, 2000, at 15.

[15] *See supra* note 10.

followed by subsequent workshops in 1996 and 1997. Then, starting in 1998, Commission staff conducted annual surveys of Internet sites and their privacy policies to measure in a rough way the state of industry self-regulation. Each survey has been reported to Congress. The Report's legislative recommendation flows from that series of surveys. The surveys have provided a lot of useful information, and undoubtedly spurred industry attention to online privacy issues, but the scope of these particular surveys should not dictate the parameters of a legislative proposal.

The Commission has ample information available to support a broader recommendation, and Congress will have ample opportunity to develop its own legislative record. The fair information practices so frequently referenced in the Report were, after all, originally developed to address concerns regarding the collection of information *offline*. And the Commission itself has had significant exposure to offline privacy issues. For example, the Commission has enforced the Fair Credit Reporting Act since its enactment in 1970.[16] This statute addresses consumer concerns about the collection and dissemination of sensitive data by credit bureaus. Although the Act predates the advent of the fair information practices, its provisions mandate some of these same requirements.[17]

The Commission also undertook in 1997 a study of the "look-up" service industry, computerized database services that collect and sell consumers' identifying information. The workshop and subsequent report to Congress focused on the benefits of these services as well as the risks, including consumers' privacy concerns.[18] Although the Internet increased access to

---

[16] 15 U.S.C. §§ 1681 *et seq.*

[17] The Commission recently issued its decision in *In re Trans Union*, Docket No. 9255 (Feb. 10, 2000), *appeal docketed*, No. 00-1141 (D.C. Cir. Apr. 4, 2000), an enforcement action concerning the dissemination by a credit bureau of certain information to target marketers. The decision considered not only the privacy implications of this practice but also the availability of other information collected offline.

[18] *See Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997).

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.[19]

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,[20] 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

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

[20] *See FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000); *GeoCities*, 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 the most effective agents for protection of privacy, online and offline, by rewarding companies that offer the preferred levels of protection.

APPENDIX A: METHODOLOGY

I. SAMPLE SELECTION

The Survey was based on two target populations – a random sample of all Web sites with at least 39,000 monthly visitors (the "Random Sample") and the 100 most popular U.S. commercial sites (the "Most Popular Group"). Both were drawn from the January 2000 Nielsen//NetRatings data, described below. In the case of the Random Sample, the full data set was used as a "sampling frame," from which a "sampling pool" was created using a systematic sampling procedure. The Random Sample was drawn from this "sampling pool" as described below. In the case of the Most Popular Group, the Survey involved data collection for the top 100 sites, subject to the exclusions discussed below, and thus did not involve a sample.

A. CREATION OF SAMPLING FRAME

Nielsen//NetRatings provided the data from which the Random Sample and the Most Popular Group were drawn.[1] It provided a list of all ".com" domains with a projected audience of at least 39,000 unique visitors in January 2000.[2] The domains were ranked according to traffic, and each domain's unique audience was provided. A "domain" is the aggregation of all Web pages, sites, and servers using a particular domain name, defined as the word or letters immediately preceding the ".com." For example, the site "sports.yahoo.com," the page "yahoo.com/news/root.asp," and the server "www1.yahoo.com" would all be included in the domain "yahoo.com." In this study, we define "Web site" as a domain, which served as the unit of analysis for the Survey.[3]

"Unique audience" or "unique visitors" is defined as the estimate of the number of different individuals that visited a domain in a particular time period, without regard to the number of visits made to or the amount of time spent at the domain by each individual during that time period. Thus, even if a person visited a particular domain thirty times in the month of January 2000, he or she would still count as one visitor to the domain.

Nielsen//NetRatings identified all ".com" domains visited by individuals from home during the month of January 2000 and calculated the projected unique audience for each domain using

statistical methods.[4] All ".com" domains with at least 39,000 unique visitors were selected and ranked in order of audience size.[5] 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.[6] The busiest 100 sites on the Nielsen//NetRatings list (excluding certain sites, as discussed below) constituted the Most Popular Group.

B. CREATION OF SAMPLING POOL

The following systematic sampling procedure was used to create a pool of sites from the sampling frame provided by Nielsen//NetRatings.[7] First, a target size of 350 sites was established for the Random Sample. It was estimated that up to 800 sites might need to be examined to ensure a final sample size of about 350.[8] Once this target sampling-pool size was determined, a "sampling interval" was determined by dividing 5,672 (the number of sites on the Nielsen list) by 800 (the target sampling pool size) to get an interval of 7 (rounded). The sampling interval was then used to randomly select sites from the sampling frame for inclusion in the sampling pool by the following methodology. A random number was generated, and the site appearing in the random number's slot on the sampling frame list was selected for inclusion, as was each site appearing on the list at the interval of one sampling interval. The resulting sampling pool contained 811 sites.

The 811 sites were then divided into 54 replicates of 15 sites each (with one replicate having 16 sites). Dividing 811 by 54 yielded the replicate interval of 15 (rounded), which was used to apportion sites among replicates. The first site went to the first replicate, the second to the second replicate, etc. Thus the 54th site was allocated to the 54th replicate. The process was then continued with the 55th site going to the first replicate, etc., until all sites had been allocated. This allocation ensured that the final sample would be representative of the sampling frame regardless of the number of replicates used. Note that because the replicates were created from the entire sampling frame, some sites from the Most Popular Group also appeared on

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.[9] Once a replicate had been selected, all sites on that replicate were surfed.[10]

At this stage, some sites were excluded from the Survey for one of three reasons: they were "adult" (*i.e.*, pornographic) sites, they were sites primarily directed to children 12 and under,[11] or they were inaccessible.[12] 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.[13] Second, all sites primarily directed to other businesses as opposed to consumers (*i.e.*, business-to-business sites) were excluded.[14] Finally, certain duplicate sites were excluded.[15] 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	# Sites Examined	# Sites Excluded	Final Sample Size
Random	421	86	335
Most Popular	100	9	91

II. THE SURVEY

The Survey itself was divided into three separate parts: (1) a surf of all Web sites to ascertain their information collection practices and privacy disclosures; (2) a separate surf of Web sites to determine the use of third-party cookies; and (3) content analysis of the privacy disclosures found during the first surf.

A. INFORMATION COLLECTION AND PRIVACY DISCLOSURES

Sixteen Commission staff members, including attorneys, legal assistants and investigators ("surfers") surveyed the sites in the samples during a two-week period in February 2000. The surfers were not involved in designing the Survey, in the subsequent data analysis, or in drafting this report. Each surfer underwent a day's training in the technical skills of visiting and reviewing Web sites and in the use of the Survey questionnaire.[16] Surfers conducted the Survey in two rooms using computers equipped with Pentium III 500 processors and Windows 98 and connected to the Internet with a 1.5 MB SDSL link. All machines had at least the following plug-ins: RealAudio, QuickTime, and Macromedia Flash Player. Staff attorneys serving as supervisory proctors were present in the room at all times during the Survey to handle any technical difficulties and answer questions.

Surfers were randomly assigned replicates from both samples and instructed to visit each site listed on the replicate and to spend no more than twenty minutes surfing each site. Once a surfer concluded that a site qualified for inclusion in the Survey (it was not inaccessible, an "adult" site, or a site directed to children), the Survey questionnaire was completed. Surfers were instructed to determine whether the site had a privacy seal, had any information practice disclosures, and collected any personal information.[17] Surfers were instructed to print each site's home page and every page on which an information practice disclosure was located. Each site not excluded by the surfer was then examined again by a second surfer, who looked for any additional information practice disclosures.[18]

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.[19] 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 content analysis form[20] and worked in pairs. Each pair was randomly assigned ten sites at a time.[21] Each analyst in the pair independently reviewed all of the disclosures for each assigned site and completed a content analysis form. Once both members of the pair had completed their independent review, the pair met and reconciled their answers for each site on a final content

analysis form. Where their answers were the same, they simply indicated the answer on the final content analysis form. Where their answers differed, the analysts discussed the question at issue and arrived at a consensus answer.[22] All sites with at least one privacy disclosure were reviewed and analyzed by two content analysts who ultimately agreed on the answer to the questions on the content analysis form.[23]

D. DATA ENTRY AND DATA ANALYSIS

Once all of the sites had been surfed, cookie-surfed, and, in the case of sites with privacy disclosures, content analyzed, data were entered by three pairs of data-entry personnel. The data-entry teams worked in pairs, with one member of the pair reading off answers to the second member of the pair who inputted the data. These numbers were then manually checked for accuracy by the data-entry teams. A set of queries was then run on the data to ensure that the data was internally consistent, *i.e.*, that all conditional answers were answered or left blank, as appropriate. All errors were corrected prior to substantive data analysis.

Finally, the data was analyzed using Intercooled Stata 6.0 for Windows 98/95/NT, and manually reviewed for errors by several Commission attorneys involved in the preparation of the report. Two analyses were performed with the data. One analysis focuses on the performance of Web sites and seeks to estimate the proportion of sites whose privacy policies fall into various categories. This analysis was performed on both the Random Sample and the Most Popular Group. Estimates for the Random Sample are reported together with 95-percent confidence intervals, which convey the margin for error on either side of the estimates.[24] For the Most Popular Group there is no sampling error, because the results were obtained using a 100-percent sample – a census.

The second analysis performed on the data, referred to as the weighted analysis, seeks to represent consumer experiences and gives proportionally more weight to sites with more traffic.[25] This weighting scheme shifts the focus of the analysis from sites to unique site visits.[26] For example, instead of representing the proportion of sites that post a privacy policy, 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.[27]

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.[28]

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% (*i.e.*, 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 eliminated, and domain served as the unit of analysis for that survey as well. *Id.* at App. B at 5. The methodologies differ, however, in that domains with multiple servers had a greater chance of being included in the sampling pool and the sample in the Georgetown study, but not in the Commission's study, which used a list of domains as the sampling frame. *Id.* at App. B, n. iii.

4. Nielsen//NetRatings has recruited and maintained an Internet panel, a nationally representative sample of persons living in United States households with Internet access from the home. In January 2000, the month for which the data for the Commission's Survey was gathered, the panel included more than 40,000 individuals. The panel is constructed using a random digit dial, telephone recruitment process. Repeated attempts are made to identify and recruit all eligible households, in order to ensure that the Nielsen//NetRatings sample is as representative of the universe of Internet users as possible. Households receive a $50 U.S. savings bond every six months for the duration of their participation in the research.

   Proprietary tracking software is installed on the computers in all eligible, participating households. The software automatically tracks and collects information about Web pages viewed, ad banner viewing and clicking, and e-commerce activity, capturing all URLs and information about the time spent at each page, and transfers the data in real-time to Nielsen//NetRatings. The data are aggregated by Nielsen//NetRatings by property, domain, and unique site, or, for ad banner data, by advertiser, site, and banner.

   Nielsen//NetRatings also conducts monthly studies to determine the total size of the home Internet user population and demographic profile information. From this data, Nielsen//NetRatings is able to project from the panel data an estimated audience size for sites visited by the panelists. Further information about Nielsen//NetRatings is available at the company's Web site, <http://www.nielsen-netratings.com>.

5. Domains that Nielsen//NetRatings had classified in its "Adult Category" – which includes adult ISPs, adult content domains with age verification services, and sites that have explicit material in terms of language or content that should be viewed by adults only – were excluded from the list sent to the Commission. However, Nielsen//NetRatings applies its categories only to sites with a unique audience of 120,000 or

more. Therefore, some "adult" sites were included in the list provided by Nielsen// NetRatings and were excluded from the final sample, as described below.

6. There are over 7.8 million ".com" domains today, many of which receive few or no visitors. Network Solutions, *Network Solutions Surpasses 10 Million Domain Name Registrations*, available at <http://www.nsol.com/news/2000/pr_20000413.html> (Network Solutions alone has 10 million registered domains); Network Solutions, *Fun Facts About Domains*, available at <http://www.nsol.com/statistics/fun/fun.html> (as of January 2000, 78% of registered domains are ".com").

7. Because the Most Popular Group represents a census of the most popular sites, as opposed to a sample of those sites, the sampling techniques described below were used to create the Random Sample only.

8. As described below, "adult" sites, sites directed to children, and sites that were inaccessible for technical reasons were excluded at the beginning of the data collection process and did not qualify for the sample.

9. Because, as discussed below, additional sites were removed from the sample after data collection, more than the target number of sites were surfed.

10. Where a Most Popular Group site appeared on a replicate for the Random Sample, the site was not examined again, and the data gathered for the site during the surf of Most Popular sites was used in its place.

11. Such sites' information practices are covered by the Children's Online Privacy Protection Act, 15 U.S.C. § 6501, *et seq.*, and its implementing regulations, 16 C.F.R. Part 312, available at <http://www.ftc.gov/opa/1999/9910/childfinal>.

12. This last category included sites for which there was no DNS entry, a 404 Error message was received, or which were otherwise inaccessible.

13. Sites were deemed foreign if the registrant address, as listed in the Whois database at <http://www.networksolutions.com>, listed an address outside the U.S. A total of 31 foreign sites were excluded.

14. Two Commission staff re-examined each site in the proposed sample to identify potential business-to-business sites. A group of three Commission staff then jointly decided whether each such site was in fact a business-to-business site. A total of 13 sites were excluded as business-to-business sites.

15. "Duplicate" sites occur when two separate domain names lead to the same Web page. Duplicates were identified by a staff member visiting all the sites in the proposed samples, and identifying the homepage visited. Duplicates fell into one of three categories. Where both duplicate sites were in the Most Popular Group, the higher-ranked site was retained and the lower-ranked site was deleted, resulting in a smaller final Most Popular Group. (There were 4 such duplicates deleted.) Where one of the duplicate sites was in the Most Popular Group (*i.e.*, in the top 100 sites) and the other was not, the site in the Most Popular Group was retained and its data used in place of the duplicate site in the Random Sample. Thus, such a situation did not affect sample size.

(There were four such duplicate pairs.) Where both sites were in the Random Sample, one site was randomly deleted, resulting in a smaller final Random Sample. (There were two such duplicates deleted.) A total of six sites were deleted as duplicates, and four additional duplicate pairs resulted in the substitution of data, as described above.

For the weighted analysis, the traffic for the retained site was used. Where one of the duplicates was in the Most Popular Group and one was in the Random Sample, however, the retained site (from the Most Popular Group) and its traffic was included only in the Most Popular portion of the weighted analysis; *i.e.*, the site was not counted twice in the weighted analysis.

16. Copies of the surfers' instructions and the Survey questionnaire are included in Appendix B.

17. Staff did not ascertain whether sites in the Survey used hidden electronic means to collect personal information, but instead looked to order forms, registration pages, and other places where information was requested from consumers.

18. When additional information practice disclosures resulted in a change to an answer on the Survey questionnaire, a proctor first approved the change.

19. Copies of the cookie surfers' instructions and the third-party cookie questionnaire are included in Appendix B.

20. Copies of the content analysts' instructions and the content analysis form are included in Appendix B.

21. On occasion, fewer than ten sites were assigned for scheduling reasons.

22. The content analysts' agreement rate was 92% (number of agreements/total number of questions answered).

23. The content analysts were trained to treat inconsistencies in information practice disclosures as follows. First, questions were to be answered based on a site's treatment of *any piece* of information. Thus, for example, if a site offered choice with respect to disclosure of some but not all information collected, answers regarding such choice were answered in the affirmative. If, however, a site offered differing types of choice for different kinds of information, the least privacy-protective of those choices would control. Thus, if a site offered choice with respect to the sharing of personal information with some, but not all, third parties, the site received credit for choice as it relates to third parties. If the same site offered opt-in choice with respect to some third parties and opt-out choice with respect to other third parties, the site was classified as offering opt-out choice with respect to third parties. This methodology was necessitated by the complexity of sites' information practices and information practice disclosures, and does not reflect a policy decision on the part of the Commission.

24. These confidence intervals were constructed using the binomial probability distribution, which applies when analyzing dichotomous (yes/no) variables, such as we have here.

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 as 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.

APPENDIX B: SURVEY SAMPLES, RESULTS, AND INSTRUCTIONS

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.amarillonet.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.courttv.com
www.craftassoc.com
www.crafterscommunity.com
www.creaf.com
www.crestar.com
www.crosswalk.com
www.cwsubscribe.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.holowww.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.sweepstakesonline.com
www.swiftsite.com
www.techguide.com
www.teen.com
www.teldir.com
www.theknot.com
www.themailbox.com
www.thetrip.com
www.theultimates.com
www.thomas.com
www.tir.com
www.todayssports.com
www.top-25.com
www.topps.com
www.topscreensavers.com
www.townnews.com
www.travelnow.com
www.tylenol.com
www.unitedmedia.com
www.usatoday.com
www.utrade.com
www.valic.com
www.vcall.com
www.verio.com
www.vintage-mustang.com
www.virtuallyshopping.com
www.vitaminshoppe.com
www.vrbo.com
www.warnerbros.com
www.webcom.com
www.webriot.com
www.websponsors.com
www.webvan.com
www.westlaw.com
www.whymilk.com
www.winternet.com
www.woodmagazine.com
www.worldnetdaily.com
www.wrestlingplanet.com
www.yamahausa.com
www.year2000.com
www.ym.com
www.ynot.com
www.zianet.com

Federal Trade Commission
2000 Online Privacy Survey

I D # _____

Surf Survey Form

Surfer's Name _____ **Date** _____

Assigned Domain (URL) [Random Sample Results]_____

PART 1 - SCREENING

Instructions:

(1) Are you unable to access this URL?

IF YES, STOP HERE and **RECORD** a **"U"** in the box at upper left.
Then **GO** to your next assigned URL.

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

IF YES, STOP HERE and **RECORD** an "**A**" in the box at upper left.
Then **GO** to your next assigned URL.

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

If YES, STOP HERE and **RECORD** "**K**" in the box at upper left.
Then **GO** to your next assigned URL.

If you answered NO to (1) through (3), WRITE the domain's ID Number on a folder. **PRINT** the home page, **WRITE** the domain's ID Number on it, and **PLACE** it in the folder.
Then you're ready to **GO** to **Survey Question 1.**

PART 2 - DOMAIN ATTRIBUTES

Instructions: Circle NO or YES for each question below unless instructed to skip the question.

		NO	YES
Q1	Is a **PRIVACY SEAL** posted on this domain?	**308**	**27**

Examples:

TRUSTe
CPA WebTrust
BBB*Online* Privacy
PriceWaterhouseCoopers *BetterWeb*
ESRB *Privacy Online Certified*

Other (write in): _____
(Consult a proctor before relying upon "other" to answer YES to this question.)

Q2	Is a **PRIVACY POLICY** posted on this domain?	**128**	**207**

If NO, SKIP to **Question #4**.

If YES, **PRINT** the entire Privacy Policy, **WRITE** the domain's ID Number on it, and **PLACE** it in the folder. If you cannot print the Privacy Policy, **ASK** a proctor for assistance. If the Privacy Policy cannot be printed, **COPY** it in its entirety in **Part 3** of this form (be sure to **RECORD** the URL(s) where the Privacy Policy appears).
Then **GO** to **Question #3**.

Q3	Is there a **LINK** to the Privacy Policy on this domain's home page?	**50**	**157**

Examples: icon or highlighted text

Q4	Is one or more **INFORMATION PRACTICE STATEMENT(S) (IPS)** posted on this domain?	**71**	**264**

If NO, GO to **Question #5**.

If YES, **PRINT ALL** Information Practice Statements, **WRITE** the domain's ID Number on each page you print, **HIGHLIGHT** the Information Practice Statement, and **PLACE** the page in the folder**.** If you cannot print an Information Practice Statement, **ASK** a proctor for assistance. If the Information Practice Statement cannot be printed, **COPY** it in its entirety in **Part 3** of this form (be sure to **RECORD** the URL where the Information Practice Statement(s) appears).
Then **GO** to **Question #5**.

Instructions:	**Circle NO or YES for each question below unless instructed to skip the question.**	**NO**	**YES**
Q5	Does the domain collect **EMAIL ADDRESSES**?	**15**	**320**
Q6	Does the domain collect **PERSONAL IDENTIFYING INFORMATION other than email address**?	**44**	**291**

Examples:

Name	Fax Number
Postal Address	Credit Card Number
Telephone Number	Social Security Number

Other (write in): _____
(Consult a proctor before relying upon "other" to answer YES to this question.)

Q7	Does the domain collect **NON-IDENTIFYING INFORMATION**?	**108**	**227**

Examples:

Age/Date of Birth	Occupation
Gender	Interests or hobbies
Education	Type of hardware/software using
ZIP Code, but not an address	Income

Other (write in): _____
(Consult a proctor before relying upon "other" to answer YES to this question.)

STOP

Go to your next assigned URL.

PART 3 - NOTES

Instructions: Use this space to record any privacy policy or information practice statement that cannot be printed.

URL _____

Federal Trade Commission
2000 Online Privacy Survey **I D # _____**

Third-Party Cookie Survey Form

Surfer's Name _____ **Date** _____

Assigned Domain (URL) [Random Sample Results]_____

Instructions: Circle NO or YES.

		NO	YES
Q8	Is a **THIRD PARTY** (i.e., any domain **OTHER THAN** the domain you are currently visiting) attempting to place a cookie at this domain?	**143**	**192**

IF YES, record the **URL** of the third party attempting to place the cookie:

_____

STOP

Go to your next assigned URL.

Federal Trade Commission
2000 Online Privacy Survey **I D # _____**

Content Analysis Form

Content Analyst's Name _____ **Date** _____

Content Analyst's Name _____

Assigned Domain (URL) [Random Sample Results]_____

Instructions: **Circle NO or YES for each question below unless otherwise instructed.**

PART 1 - NOTICE

		NO	YES
Q9	Does the Privacy Policy/Information Practice Statement contain a declaration that the domain does **NOT** collect any personal information from consumers? [If the Privacy Policy/Information Practice Statement contains such a declaration, answer YES. If it does not contain such a declaration, answer NO.] **If NO, GO** to **Question #10**. **If YES**, **SKIP** to **Question #24**.	**294**	**1**
Q10	Does the Privacy Policy/Information Practice Statement say **anything about what specific personal information the domain collects** from consumers?	**71**	**223**

PART 2 - INTERNAL USE: NOTICE AND CHOICE

		NO	YES
Q11	Does the Privacy Policy/ Information Practice Statement say **anything about how the domain may use** personal information it collects **for internal purposes**?	**26**	**268**
	If NO, **SKIP** to **Question #15**. **If YES, GO** to **Question #12**.		
Q12	Does the Privacy Policy/Information Practice Statement say **anything about whether** the **domain** uses personal information it collects **to send communications to the consumer?**	**13**	**255**
	If NO, SKIP to **Question #15**. **If YES, GO** to **Question #13**.		

Q13 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . .	CIRCLE ONE
says that the **domain does or may** 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)**.	**243**
says that the **domain 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)**.	**12**

IF YOU CHOSE #1 to this question, **GO** to **Question #14**.
IF YOU CHOSE #2 to this question, **SKIP** to **Question #15**.

Q14 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . .	**CIRCLE ONE**
says that the **domain** provides consumers an opportunity to **opt in** to receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question).	**55**
says that the **domain** provides consumers an opportunity to **opt out** of receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question).	**155**
says that the **domain** requires **consent or offers a choice** with respect to receiving future 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.	**9**
does not say anything about offering consumers **choice** with respect to receiving future communications from the **domain** (other than those directly related to processing an order or responding to a consumer's question).	**244**

PART 3 - DISCLOSURES TO THIRD PARTIES: NOTICE AND CHOICE

	NO	**YES**
Q15 Does the Privacy Policy/Information Practice Statement say **anything about whether** the domain **discloses personal information it collects to third parties**?	**52**	**242**

If NO, **SKIP** to **Question #18**.
If YES, GO to **Question #16**.

Q16 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**. **CIRCLE ONE**

The Privacy Policy/Information Practice Statement . . .

says that the domain **does or may** disclose **personal identifying information** to **third parties.** **169**

says that the domain **does NOT disclose personal identifying information** to **third parties**, **or** does so **only**:
(a) as required by law,
(b) as necessary to process an order, and/or
(c) in aggregate or non-identifying form. **73**

IF YOU CHOSE #1 to this question, **GO** to **Question #17**.
IF YOU CHOSE #2 to this question, **SKIP** to **Question #18**.

Q17 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . . **CIRCLE ONE**

says that the domain provides consumers an opportunity to **opt in** to the disclosure of **personal identifying information** to third parties. **14**

says that the domain provides consumers an opportunity to **opt out** of the disclosure of **personal identifying information** to third parties. **274**

says that the domain requires **consent or offers a choice** with respect to the disclosure of **personal identifying information** to third parties, but **does not make clear** whether the choice is opt-in or opt-out. **37**

does not say anything about offering consumers **choice** with respect to disclosure of **personal identifying information** to third parties. **44**

PART 4 - ACCESS

		NO	YES
Q18	Does the Privacy Policy/Information Practice Statement say that the domain allows consumers to **review at least some personal information** about them?	**227**	**67**
Q19	Does the Privacy Policy/Information Practice Statement say that the domain allows consumers to **have inaccuracies corrected in at least some personal information** about them?	**174**	**120**
Q20	Does the Privacy Policy/Information Practice Statement say that it allows consumers to **have at least some personal information about them deleted** from the domain's records?	**237**	**57**

PART 5 - SECURITY

Q21	Does the Privacy Policy/Information Practice Statement say that the domain **takes any steps to provide security?** **If NO, SKIP** to **Question #24**. **If YES, GO** to **Question #22**.	**114**	**180**
Q22	Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide **security**, for personal information the domain collects, **during transmission** of the information from the consumer to the domain? Example: Secure Socket Layer Technology or SSL	**55**	**125**
Q23	Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide **security**, for personal information the domain has collected, **after the domain has received the information** (i.e., not during transmission, but after collection)?	**87**	**93**

PART 6 - COOKIES

Q24 Does the Privacy Policy/Information Practice Statement say **anything about whether the DOMAIN places cookies**?

NO	YES
142	153

If NO, SKIP to **Question #26**.
If YES, GO to **Question #25**.

Q25 Choose **ONE** of the following options **and CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . .	CIRCLE ONE
says that the domain **does or may** place cookies.	147
says that the domain **does not** place cookies.	6

Q26 Does the Privacy Policy/Information Practice Statement say **anything about whether THIRD PARTIES may place cookies** and/or collect personal information on the domain?

NO	YES
246	48

If NO, **STOP!**
Review your answers for **accuracy** and to ensure that all questions were **answered or skipped appropriately**.
Then, **Go to your next folder**.

If YES, GO to **Question #27**.

Q27 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . .	CIRCLE ONE
says that third parties **do or may** place cookies and/or collect personal information on the domain.	48
says that third parties **do not** place cookies and/or collect personal information on the domain.	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

www.webcrawler.com
www.webshots.com
www.women.com
www.wwf.com
www.xoom.com
www.yahoo.com
www.zdnet.com

Federal Trade Commission
2000 Online Privacy Survey **I D # _____**

Surf Survey Form

Surfer's Name _____ **Date** _____

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

PART 1 - SCREENING

Instructions:

(1) Are you unable to access this URL?

IF YES, STOP HERE and **RECORD** a **"U"** in the box at upper left.
Then **GO** to your next assigned URL.

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

IF YES, STOP HERE and **RECORD** an "**A**" in the box at upper left.
Then **GO** to your next assigned URL.

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

If YES, STOP HERE and **RECORD** "**K**" in the box at upper left.
Then **GO** to your next assigned URL.

If you answered NO to (1) through (3), WRITE the domain's ID Number on a folder. **PRINT** the home page, **WRITE** the domain's ID Number on it, and **PLACE** it in the folder.
Then you're ready to **GO** to **Survey Question 1.**

PART 2 - DOMAIN ATTRIBUTES

Instructions: Circle NO or YES for each question below unless instructed to skip the question.

		NO	YES
Q1	Is a **PRIVACY SEAL** posted on this domain?	**50**	**41**

Examples:

TRUSTe PriceWaterhouseCoopers *BetterWeb*
CPA WebTrust ESRB *Privacy Online Certified*
BBB*Online* Privacy

Other (write in): _____
(Consult a proctor before relying upon "other" to answer YES to this question.)

Q2	Is a **PRIVACY POLICY** posted on this domain?	**3**	**88**

If NO, SKIP to **Question #4**.

If YES, **PRINT** the entire Privacy Policy, **WRITE** the domain's ID Number on it, and **PLACE** it in the folder. If you cannot print the Privacy Policy, **ASK** a proctor for assistance. If the Privacy Policy cannot be printed, **COPY** it in its entirety in **Part 3** of this form (be sure to **RECORD** the URL(s) where the Privacy Policy appears).
Then **GO** to **Question #3**.

Q3	Is there a **LINK** to the Privacy Policy on this domain's home page?	**5**	**83**

Examples: icon or highlighted text

Q4	Is one or more **INFORMATION PRACTICE STATEMENT(S) (IPS)** posted on this domain?	**9**	**82**

If NO, GO to **Question #5**.

If YES, **PRINT ALL** Information Practice Statements, **WRITE** the domain's ID Number on each page you print, **HIGHLIGHT** the Information Practice Statement, and **PLACE** the page in the folder**.** If you cannot print an Information Practice Statement, **ASK** a proctor for assistance. If the Information Practice Statement cannot be printed, **COPY** it in its entirety in **Part 3** of this form (be sure to **RECORD** the URL where the Information Practice Statement(s) appears).
Then **GO** to **Question #5**.

Instructions: Circle NO or YES for each question below unless instructed to skip the question. **NO** **YES**

Q5 Does the domain collect **EMAIL ADDRESSES**? **1** **90**

Q6 Does the domain collect **PERSONAL IDENTIFYING INFORMATION other than email address**? **4** **87**

Examples:

Name	Fax Number
Postal Address	Credit Card Number
Telephone Number	Social Security Number

Other (write in): _____
(Consult a proctor before relying upon "other" to answer YES to this question.)

Q7 Does the domain collect **NON-IDENTIFYING INFORMATION**? **21** **70**

Examples:

Age/Date of Birth	Occupation
Gender	Interests or hobbies
Education	Type of hardware/software using
ZIP Code, but not an address	Income

Other (write in): _____
(Consult a proctor before relying upon "other" to answer YES to this question.)

STOP

Go to your next assigned URL.

PART 3 - NOTES

Instructions: Use this space to record any privacy policy or information practice statement that cannot be printed.

URL _____

Federal Trade Commission
2000 Online Privacy Survey **I D # _____**

Third-Party Cookie Survey Form

Surfer's Name _____ **Date** _____

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

Instructions: Circle NO or YES.

		NO	YES
Q8	Is a **THIRD PARTY** (i.e., any domain **OTHER THAN** the domain you are currently visiting) attempting to place a cookie at this domain?	**20**	**71**

IF YES, record the **URL** of the third party attempting to place the cookie:

_____

STOP

Go to your next assigned URL.

Federal Trade Commission
2000 Online Privacy Survey **I D # _____**

Content Analysis Form

Content Analyst's Name _____ **Date** _____

Content Analyst's Name _____

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

Instructions: **Circle NO or YES for each question below unless otherwise instructed.**

PART 1 - NOTICE

		NO	YES
Q9	Does the Privacy Policy/Information Practice Statement contain a declaration that the domain does **NOT** collect any personal information from consumers? [If the Privacy Policy/Information Practice Statement contains such a declaration, answer YES. If it does not contain such a declaration, answer NO.] **If NO, GO** to **Question #10**. **If YES**, **SKIP** to **Question #24**.	**91**	**0**
Q10	Does the Privacy Policy/Information Practice Statement say **anything about what specific personal information the domain collects** from consumers?	**9**	**82**

PART 2 - INTERNAL USE: NOTICE AND CHOICE

Q11 Does the Privacy Policy/ Information Practice Statement say **anything about how the domain may use** personal information it collects **for internal purposes**?

NO 0 **YES** 91

If NO, **SKIP** to **Question #15**.
If YES, GO to **Question #12**.

Q12 Does the Privacy Policy/Information Practice Statement say **anything about whether** the **domain** uses personal information it collects **to send communications to the consumer?**

2 **89**

If NO, SKIP to **Question #15**.
If YES, GO to **Question #13**.

Q13 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . . **CIRCLE ONE**

says that the **domain does or may** 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)**. **87**

says that the **domain 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)**. **2**

IF YOU CHOSE #1 to this question, **GO** to **Question #14**.
IF YOU CHOSE #2 to this question, **SKIP** to **Question #15**.

Q14 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . .	**CIRCLE ONE**
says that the **domain** provides consumers an opportunity to **opt in** to receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question).	**12**
says that the **domain** provides consumers an opportunity to **opt out** of receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question).	**58**
says that the **domain** requires **consent or offers a choice** with respect to receiving future 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.	**8**
does not say anything about offering consumers **choice** with respect to receiving future communications from the **domain** (other than those directly related to processing an order or responding to a consumer's question).	**9**

PART 3 - DISCLOSURES TO THIRD PARTIES: NOTICE AND CHOICE

	NO	**YES**
Q15 Does the Privacy Policy/Information Practice Statement say **anything about whether** the domain **discloses personal information it collects to third parties**?	**2**	**89**

If NO, **SKIP** to **Question #18**.
If YES, GO to **Question #16**.

Q16 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**. **CIRCLE ONE**

The Privacy Policy/Information Practice Statement . . .

says that the domain **does or may** disclose **personal identifying information** to **third parties.** **73**

says that the domain **does NOT disclose personal identifying information** to **third parties**, **or** does so **only**:
(a) as required by law,
(b) as necessary to process an order, and/or
(c) in aggregate or non-identifying form. **16**

IF YOU CHOSE #1 to this question, **GO** to **Question #17**.
IF YOU CHOSE #2 to this question, **SKIP** to **Question #18**.

Q17 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . . **CIRCLE ONE**

says that the domain provides consumers an opportunity to **opt in** to the disclosure of **personal identifying information** to third parties. **8**

says that the domain provides consumers an opportunity to **opt out** of the disclosure of **personal identifying information** to third parties. **26**

says that the domain requires **consent or offers a choice** with respect to the disclosure of **personal identifying information** to third parties, but **does not make clear** whether the choice is opt-in or opt-out. **20**

does not say anything about offering consumers **choice** with respect to disclosure of **personal identifying information** to third parties. **19**

PART 4 - ACCESS

		NO	YES
Q18	Does the Privacy Policy/Information Practice Statement say that the domain allows consumers to **review at least some personal information** about them?	**48**	**43**
Q19	Does the Privacy Policy/Information Practice Statement say that the domain allows consumers to **have inaccuracies corrected in at least some personal information** about them?	**21**	**70**
Q20	Does the Privacy Policy/Information Practice Statement say that it allows consumers to **have at least some personal information about them deleted** from the domain's records?	**63**	**28**

PART 5 - SECURITY

Q21	Does the Privacy Policy/Information Practice Statement say that the domain **takes any steps to provide security?** **If NO, SKIP** to **Question #24**. **If YES, GO** to **Question #22**.	**24**	**67**
Q22	Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide **security**, for personal information the domain collects, **during transmission** of the information from the consumer to the domain? Example: Secure Socket Layer Technology or SSL	**18**	**49**
Q23	Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide **security**, for personal information the domain has collected, **after the domain has received the information** (i.e., not during transmission, but after collection)?	**24**	**43**

PART 6 - COOKIES

Q24 Does the Privacy Policy/Information Practice Statement say **anything about whether the DOMAIN places cookies**?

NO	YES
12	79

If NO, SKIP to **Question #26**.
If YES, GO to **Question #25**.

Q25 Choose **ONE** of the following options **and CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . .	CIRCLE ONE
says that the domain **does or may** place cookies.	79
says that the domain **does not** place cookies.	0

Q26 Does the Privacy Policy/Information Practice Statement say **anything about whether THIRD PARTIES may place cookies** and/or collect personal information on the domain?

NO	YES
53	38

If NO, **STOP!**
Review your answers for **accuracy** and to ensure that all questions were **answered or skipped appropriately**.
Then, **Go to your next folder**.

If YES, GO to **Question #27**.

Q27 Choose **ONE** of the following options and **CIRCLE the number corresponding to your choice**.

The Privacy Policy/Information Practice Statement . . .	CIRCLE ONE
says that third parties **do or may** place cookies and/or collect personal information on the domain.	38
says that third parties **do not** place cookies and/or collect personal information on the domain.	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 whether 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 *adult site*, **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 *adult site*, 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 *directed (or targeted) to children under the age of 13*. If the domain is *directed to children under the age of 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: As a rule, clicking on the "Print" button will print an entire Privacy Policy as a single document. Occasionally, however, sections of a Privacy Policy are configured as separate documents and must be printed separately (there may be hypertext for each section). **Please check** after printing a Privacy Policy to be sure everything you intended to print has in fact been printed. Consult a proctor if you are unsure about this. Write the domain's ID Number on every document you print.

Question 3 Is there a link to the Privacy Policy on this domain's home page?

Search the home page for an icon or highlighted text that allows a domain visitor to click to the Privacy Policy. Be sure to scroll all the way down to the bottom of the home page. Look for highlighted terms such as "Privacy Policy," "Privacy Statement," "Privacy," "Security," "Online Privacy Practices," or "Our Policies."

Note: It is possible that the page that appears when you type in an assigned URL will bear only the domain's logo. If this occurs, click on the logo. The Web page that appears after the logo is the "home page," for purposes of this question; answer this question, therefore, based upon whether an icon or highlighted text appears on this page.

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.

Because it is valuable to consumers to read Information Practice Statements in relevant contexts, we want to capture them wherever they appear on the domain. Thus, this question asks you to search the domain for Information Practice Statements **even if you have found a Privacy Policy**. You must make an effort to find all Information Practice Statements posted on the domain.

If you find an Information Practice Statement, print the page(s) on which it appears and highlight it. Write the domain's ID Number on each page you print, and place the page(s) in the domain's folder (please check to be sure everything you intended to print has printed). If, after trying the printing tips listed below, you cannot print the Information Practice Statement, copy it verbatim in Part 3 of the survey form.

Note: You are looking for all Information Practice Statements on the domain, not just one. You are likely to find Information Practice Statements in places on the domain that you will search to answer Questions 5-7 (i.e., places where personal information is collected). Therefore, don't spend an excessive amount of time trying to locate all Information Practice Statements before proceeding to Questions 5-7.

PERSONAL INFORMATION COLLECTION

Questions 5-7 ask you to determine whether the domain collects certain categories of personal information from online consumers. By "collecting information," we mean providing online consumers an opportunity to give the domain **any** personal information, whether or not the domain requires such information. To answer Questions 5-7, **follow the suggestions in the box on p. 3** for guidance as to where personal information collect may occur.

Note: If you have found either a Privacy Policy or an Information Practice Statement(s), **do not** rely upon it to answer these questions. **You must search the domain** to determine for yourself what, if any, personal information is being collected, regardless of what the Privacy Policy or Information Practice Statement might say about collection of personal information.

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 **at least one** type of personal identifying information other than an email address. If, for example, a domain collects online consumers' names, Circle YES and move on to Question 7.

If you find that a domain is collecting a type of personal identifying information that is not listed as an example, consult a proctor before Circling "YES" and writing the type of information on the line provided.

Question 7 Does the domain collect NON-IDENTIFYING INFORMATION?

As noted above, we define "non-identifying information" as information that, taken alone, cannot be used to identify or locate an individual. Examples include age/date of birth, gender, education, occupation, interests or hobbies, type of hardware or software in use, and a ZIP Code without an address. This question asks you to determine whether the site is collecting **at least one** type of non-identifying information. If, for example, a domain collects information about consumers' hobbies, Circle YES.

If you find that a domain is collecting a type of non-identifying information that is not listed as an example, consult a proctor before Circling "YES" and writing the type of information on the line provided.

When you have answered Question 7, go to your next assigned URL.

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 type Ctrl-V (or use the "Paste" button) to drop the text into a WordPerfect document. Then print. Be sure to write the URL of the page where the text appears, and the domain's ID Number, on the page.

(4) If you continue to experience difficulty, save the Web page, then open the saved file and print it (some graphics may be lost in this procedure) (see a proctor for details).

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).

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 privacy disclosures of your assigned domains. You should answer the questions in the Content Analysis Form based on a careful reading of all the privacy disclosures in your folder.

2. You should rely only on the privacy disclosures in your folder. Do not look at or rely upon the pink Survey Form in your folder to complete the Content Analysis Form. Note: When a privacy disclosure could not print, the disclosure will be written on the back of the pink Survey Form.

3. Complete the Content Analysis Form in order, and carefully follow directions regarding when to skip certain questions. Please do not skip around the Form.

4. You must work independently. Do not discuss your answers with or seek help from anybody except as explained under point #5, below.

5. Every domain's privacy disclosures will be reviewed by two content analysts you and your partner. As a team, you will be given a set of 10 folders (each containing one domain's privacy disclosures) to analyze at one time. Divide these folders between the two of you i.e., five folders each. After you have each completed analyzing 5 folders, you will remove the white Content Analysis Forms you completed and swap the folders. You will then each independently analyze the 5 folders your partner analyzed first. Once you have each analyzed all ten folders, you and your partner will meet to reconcile your answers. For each folder you reviewed, you must compare your answers to each question on the Content Analysis Form. Where your answers disagree, you must discuss the question and arrive at a single answer. Then, record your reconciled answers for all questions (including those questions that you agreed upon) on the green Content Analysis Form, sign the form, and proceed to reconcile the next folder.

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 <u>all</u> 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, <u>taken alone</u>, 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.
<u>Note</u>: Non-identifying information refers to the <u>type</u> 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."**
<u>Note</u>: 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.

STEP-BY-STEP INSTRUCTIONS

PART 1 - NOTICE

Questions 9 - 10 deal with disclosures about the collection of personal information from consumers.

Question 9 *Does the Privacy Policy/ Information Practice Statement contain a declaration that the domain does **NOT** collect any personal information from consumers?*

Answer YES: If you find an express statement that the domain does **NOT** collect any personal information from consumers.

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

Answer NO: If you do not find a statement that the domain does **NOT** collect any personal information from consumers, or if you find at least one statement that the domain **DOES** collect at least one type of personal information.

Examples: We collect your ZIP code when you provide it to get the weather forecast for your area.

We don't collect any information from you other than the information you provide to us when you register for this site.

Note: Remember, "personal information" refers to either personal identifying information or non-identifying information. Thus, if a domain says it "collects only non-identifying information" the answer to this question is NO.

Question 10 *Does the Privacy Policy/ Information Practice Statement say **anything about what specific personal information the domain collects** from consumers?*

Answer YES: If you find at least one statement about what specific personal information the domain collects or does not collect from consumers.

Examples: We collect your name and address when you register for this site.

We collect only demographic information, such as your gender, age, and ZIP code.

Answer NO: If you do not find a statement about what specific personal information the domain collects from consumers, or if the statement does not specify what personal information the domain collects from consumers.

Example: We collect information about you when you visit our site.

PART 2 INTERNAL USE: NOTICE AND CHOICE

Questions 11 - 14 deal with disclosures about how the domain may use personal information it collects from consumers for internal purposes.

"Internal purposes" include, but are not limited to, processing orders or requests for information, improving a site's performance, keeping track of which pages on a site are visited, and sending consumers future communications (such as emails, newsletters, updates, and marketing or promotional material).

Note: Internal purposes do not include the disclosure of information to third parties, for any purpose.

Question 11 *Does the Privacy Policy/ Information Practice Statement say **anything about how the domain may use** personal information it collects **for internal purposes**?*

Answer YES: If you find at least one statement about how the domain may use personal information it collects for internal purposes. Such a statement can describe how the information will be used for internal purposes, how the information will not be used for internal purposes, or offer consumers choice with respect to the use of the information for internal purposes.

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

We use your personal information to improve your experience on our site.

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.

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 *Does the Privacy Policy/ Information Practice Statement say* ***anything about whether*** *the* ***domain*** *uses personal information it collects* ***to send communications to the consumer****?*

Note: The term "communications to the consumer" includes, but is not limited to, putting the consumer on a mailing list, or sending the consumer marketing or promotional messages, newsletters, or updates. It also includes sending the consumer information about his/her order.

Answer YES: If you find at least one statement that personal information may be or is used by the domain to send communications to the consumer. These communications may be sent via email, regular postal mail, or telephone. A statement offering a consumer choice about receiving future communications is also considered such a statement. You should also answer YES to this question if you find a statement that personal

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.

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 whether the domain uses personal information it collects to send communications to the consumer, i.e., the privacy disclosures are silent with respect to whether the domain uses personal information it collects to send communications to the consumer.

Example: We use your personal information to improve your experience on our site.

Question 13 This question requires you to characterize what the domain says regarding the use of personal information to send communications to the consumer.

Circle 1 ("does or may"): If you find a statement that the domain **does or may** 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**).

Examples: 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.

Circle 2 ("does not"): If you find a statement that the domain **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**).

Example: 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.

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

Question 14 This question requires you to characterize whether or not the domain offers consumers a choice regarding the use of their personal information to send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question), and, if so, to determine the nature of that choice.

Note: We ask about two types of choice - "opt-in" and "opt-out":

- "Opt-in" choice requires an affirmative act by the consumer (such as checking a click-box or sending an email or a letter) before the information can be used in a particular manner; i.e., the default is that the information will not be used.

- "Opt-out" choice allows the consumer to take an action (such as checking a click-box or sending an email or a letter) to prevent the information from being used in a particular manner; i.e., the default is that, absent action by the

consumer, the information will be used.

Note: If the domain provides choice with respect to sending **at least some** communica tions 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.

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

We will not include you in our mailing list without first obtaining 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 receiving communications from the domain (other than those directly related to processing an order or responding to a consumer's question), i.e., the privacy disclosures are silent with respect to this issue.

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

PART 3 DISCLOSURES TO THIRD PARTIES: NOTICE AND CHOICE

Questions 15 - 17 deal with statements about whether the domain discloses personal information it collects to third parties.

Note: Questions 15, 16, and 17 are a group. All three deal with statements about the domain's disclosure of personal information to third parties. Question 15 asks if there is any statement (positive or negative) about this type of disclosure. If there is such a statement, Question 16 asks what the statement says, i.e., whether the domain says that it does or does not disclose personal information to third parties. If the domain says that it does or may disclose personal information to third parties, Question 17 asks about whether the domain says that it provides consumers with any choice with respect to this disclosure of personal information.

Note: Domains often use verbs other than "disclose." Look for statements about "sharing," "renting," "selling," "providing" or "giving" information to third parties.

Note: Remember, "third parties" include any entity other than the domain, such as advertisers, affiliates, business partners, or other companies.

Question 15 *Does the Privacy Policy/ Information Practice Statement say* ***anything about whether the domain discloses personal information it collects to third parties****?*

Answer YES: If you find at least one statement that personal information may be or is disclosed by the domain to third parties. You should also answer YES to this question

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]

We will never disclose your personal information without your consent.

Circle 2 ("does not"): If you find a statement that the domain does NOT disclose personal information to third parties, or does so only: (a) as required by law, (b) as necessary to process an order, and/or (c) in aggregate or non-identifying form.

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 only disclose personal information if required to do so by law.

We do not sell or rent your information.

Question 17 This question requires you to characterize whether or not the domain offers consumers a choice regarding the disclosure of their personal information to third parties.

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 used until the consumer takes some required action. Thus, if the consumer does not want his or her personal identifying information disclosed to third parties, he or she does not have to do anything.

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

To give your permission for us to disclose your name and address to third parties, click here.

Circle 2 ("Opt out"): If the domain will disclose personal identifying information to third parties, unless the consumer takes some required action to stop this disclosure. Thus, if the consumer does not want his or her personal identifying information disclosed to third parties, he or she must take some required action.

Examples: 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]

Please send us an email if you do not wish for us to disclose your name and address to third parties.

If you do not want to receive mailings from our business partners, click here.

Circle 3 ("consent or choice, but unclear what type"): If a domain states that it requires the consumer's consent to, or that it offers a choice with respect to, the disclosure of personal identifying information to third parties, but does not make clear whether

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 *Does the Privacy Policy/ Information Practice Statement say that the domain allows consumers to* ***review at least some personal information*** *about them?*

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 *Does the Privacy Policy/ Information Practice Statement say that the domain allows consumers to* ***have inaccuracies corrected in at least some personal information*** *about them?*

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 *Does the Privacy Policy/ Information Practice Statement say that it allows consumers to* ***have at least some personal information about them deleted*** *from the domain's records?*

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.

PART 5 SECURITY

Questions 21 - 23 deal with the steps the domain takes to provide security for personal information the domain collects.

Note: In answering these questions, be especially careful to check all the print-outs in your folder; sometimes information about security is included in its own section, often called "Security" or "About Security."

Note: These questions ask about the steps taken by domains to provide security. Statements about a domain's efforts to provide security are sufficient, even if the domain does not guarantee security. Thus, terms such as "best efforts," "attempt," "make an effort," "strive" and "try" — when used to describe a domain's security efforts — all qualify as statements regarding steps taken by domains with respect to providing security.

Question 21 *Does the Privacy Policy/ Information Practice Statement say that the domain **takes any steps to provide security**?*

Answer YES: If you find any statement that the domain takes steps to provide security, regardless of whether the statement relates to security during transmission of information, after the domain has received the information, or just security in general.

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 use SSL to protect your credit card information.

We encrypt your information when you send it to us.

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 (i.e., the privacy disclosures are silent on this issue), or if you find a statement that the domain does not take any steps to provide security.

Question 22 *Does the Privacy Policy/ Information Practice Statement say that the domain takes steps to provide **security**, for personal information the domain collects, **during transmission** of the information from the consumer to the domain?*

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 *Does the Privacy Policy/ Information Practice Statement say that the domain takes steps to provide **security**, for personal information the domain has collected, **after the domain has received the information** (i.e., not during transmission, but after collection)?*

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 after the domain has received the information, 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 use SSL to protect your credit card information.

We encrypt your information when you send it to us.

PART 6 COOKIES

Questions 24 - 27 deal with "cookies."

Question 24 *Does the Privacy Policy/ Information Practice Statement say **anything about whether the DOMAIN places cookies**?*

Answer YES: If you find a statement that the domain places cookies. Also answer YES if you find a statement that the domain does not place cookies.

Examples: We use cookies on this site.

We also collect certain information through cookies.

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 *Does the Privacy Policy/ Information Practice Statement say **anything about whether THIRD PARTIES may place cookies** and/or collect personal information on the domain?*

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.

APPENDIX C:
DATA TABLES

TABLE 1

Percent of Web Sites That Collect Personal Information[1]

	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 (*e.g.*, name, postal address, email address, telephone number); and non-identifying information, including demographic information (*e.g.*, age, gender, education level, income) and preference information (*e.g.*, 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 2a

Percent of Web Sites With a Privacy Disclosure[1]

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Post at Least One Privacy Disclosure:	88% (83.4%-91.1%)[2]	294/335	100%[3]	91/91	96% (+/- 1.6%)[4]
Post a Privacy Policy:	62% (56.4%-67.0%)	207/335	97%	88/91	82% (+/- 5.2%)
Post an Information Practice Statement:	79% (74.0%-83.1%)	264/335	90%	82/91	87% (+/- 3.3%)

TABLE 2b

Of Those Web Sites With a Privacy Policy, Percent That Link to the Privacy Policy From the Home Page

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Link From the Home Page:	76% (69.4%-81.5%)	157/207	94%	83/88	90% (+/- 3.6%)

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 3

Of Those Web Sites That Collect Personal Identifying Information, Percent With a Privacy Disclosure[1]

	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:	81% (76.5%-85.3%)	263/324	91%	82/90	87% (+/- 4.1%)

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, Percent That Implement Fair Information Practice Principles to Some Extent

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Notice:[1]	55% (49.3%-60.4%)[2]	178/324	89%[3]	80/90	77% (+/- 5.4%)[4]
Choice:[5]	50% (44.1%-55.3%)	161/324	67%	60/90	61% (+/-5.9%)
Access:[6]	43% (37.7%-48.8%)	140/324	83%	75/90	68% (+/-5.8%)
Security:[7]	55% (49.7%-60.7%)	179/324	74%	67/90	65% (+/- 6.1%)
Implement Notice, Choice, Access & Security to Some Extent:[8]	20% (15.8%-24.8%)	65/324	42%	38/90	32% (+/- 4.2%)
Implement Notice & Choice to Some Extent:	41% (36.0%-46.7%)	134/324	60%	54/90	58% (+/- 5.9%)

1. "Notice" means (1) posting a Privacy Policy, and saying anything about (2) what specific personal information is collected, (3) how the site may use personal information for internal purposes, and (4) whether the site discloses personal identifying information to third parties. (See Appendix B, Surf Survey Form, Q2; Content Analysis Form, Q10, 11 & 15).
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.
5. "Choice" means providing choice with respect to (1) the site's use of personal information to send communications (other than those related to processing an order or responding to a consumer's question) back to consumers (or stating that the site **does not** use personal information in this way) and (2) the site's disclosure of personal identifying information to third parties (or stating that the site **does not** disclose personal identifying information to third parties). (See Appendix B, Content Analysis Form, Q12-14; Q15-17).
6. "Access" means either allowing consumers to (1) review or (2) have inaccuracies corrected or (3) have information deleted from the site's records, with respect to at least some personal information. (See Appendix B, Content Analysis Form, Q18-20).
7. "Security" means making a statement that the site takes any steps to provide security. (See Appendix B, Content Analysis Form, Q21).
8. This figure represents the number of sites that implement Notice, Choice, Access **and** Security; thus it cannot be any larger than the number that implement any one of these principles.

TABLE 5

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

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Post a Privacy Policy:	64% (58.1%-68.8%)[1]	206/324	97%[2]	87/90	78% (+/- 6.6%)[3]
Say Anything about What Personal Information is Collected:	69% (63.2%-73.5%)	222/324	91%	88/90	86% (+/- 4.1%)
Say Anything about How Personal Information is Used Internally:	82% (77.8%-86.4%)	267/324	100%	90/90	93% (+/- 3.4%)
Say Anything about Whether Personal Identifying Information is Disclosed to Third Parties:	74% (69.3%-79.0%)	241/324	98%	88/90	87% (+/- 4.3%)

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 6

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

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Say That Site Uses Cookies:	44% (38.5%-49.4%)[1]	147/335	87%[2]	79/91	72% (+/- 5.6%)[3]
Say That Site Does Not Use Cookies:	2% (0.7%-3.9%)	6/335	0%	0/91	1% (+/- 1.4%)
Silent About Site's Use of Cookies:	54% (48.8%-59.8%)	182/335	13%	12/91	27% (+/- 5.5%)

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 7

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

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Provide Choice for the Use of, or Say They Do Not Use, Personal Information to Send Communications to Consumers:[1]	71% (65.7%-75.9%)[2]	230/324	88%[3]	79/90	83% (+/- 4.8%)[4]
Provide Choice for the Disclosure of, or Say They Do Not Disclose, Personal Identifying Information to Third Parties:[5]	61% (55.3%-66.2%)	197/324	77%	69/90	69% (+/-5.6%)

1. "Communications to consumers" include any communications other than those directly related to processing an order or responding to a consumer's question.
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.
5. "Third party" was defined as "[a]ny entity other than the assigned domain. Examples: advertisers, affiliates, subsidiaries, business partners, or other companies."

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

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Say Anything About Whether Domain Uses Personal Information to Send Communications:	78% (73.5%-82.8%)[1]	254/324	98%[2]	88/90	89% (+/- 4.5%)[3]
Say Do or May Use Personal Information to Send Communications:	75% (69.6%-79.3%)	242/324	96%	86/90	89% (+/- 3.7%)
Say Do Not Use Personal Information to Send Communications:	4% (1.9%-6.4%)	12/324	2%	2/90	2% (+/- 0.8%)

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 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]

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Opt-In:[2]	25% (19.6%-31.5%)[3]	55/218	16%[4]	12/77	17% (+/- 4.9%)[5]
Opt-Out:[6]	71% (64.1%-76.6%)	154/218	75%	58/77	76% (+/- 5.3%)
Unclear if Opt-In or Opt-Out:	4% (1.9%-7.7%)	9/218	9%	7/77	8% (+/- 2.6%)

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 checking a click-box or sending an email or a letter) before the information can be used in a particular manner; *i.e.*, the default is that the information will not be used. (See Appendix B, 2000 Online Privacy Survey: Instructions for Content Analysis Form at 7).
3. Figures in parentheses represent the 95% binomial confidence interval for each calculated percentage.
4. There is no sampling error for Most Popular Group data, because the results were obtained using a census as opposed to a sample.
5. Figures in parentheses represent 95% confidence intervals calculated using the Normal distribution.
6. "Opt-out" is defined as choice that allows the consumer to take an action (such as checking a click-box or sending an email or a letter) to prevent the information from being used in a particular manner; *i.e.*, the default is that, absent action by the consumer, the information will be used. (See Appendix B, 2000 Online Privacy Survey: Instructions for Content Analysis Form at 7-8).

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
	Percent	Number	Percent	Number	Percent
Say Do or May Disclose Personal Identifying Information to Third Parties:	52% (46.3%-57.4%)[1]	168/324	80%[2]	72/90	68% (+/- 6.8%)[3]

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[4]

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Opt-In:	11% (6.3%-18.2%)	14/124	15%	8/53	16% (+/- 5.3%)
Opt-Out:	59% (49.7%-67.6)	73/124	49%	26/53	58% (+/- 7.7%)
Unclear if Opt-In or Opt-Out:	30% (22.0%-38.7%)	37/124	36%	19/53	26% (+/- 5.3%)

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, Modified Choice, Access, and Security to Some Extent)

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Provide Choice for Either Sending Communications to Consumers or Disclosure to Third Parties ("Modified Choice"):	82% (77.5%-86.1%)[1]	266/324	98%[2]	88/90	89% (+/- 4.5%)[3]
Implement Notice, Modified Choice, Access, and Security to Some Extent:	27% (22.1%-32.0%)	87/324	63%	57/90	40% (+/- 6.6%)
Address Notice & Modified Choice to Some Extent:	54% (48.4%-59.5%)	175/324	87%	78/90	72% (+/- 6.8%)

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 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 and Correct or Delete at Least Some Personal Information the Site Has Collected ("Modified Access"):	18% (13.9%-22.5%)[1]	58/324	47%[2]	42/90	31% (+/- 4.7%)[3]
Implement Notice, Choice, Modified Access, and Security to Some Extent:	11% (7.6%-14.7%)	35/324	27%	24/90	20% (+/-2.9%)

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
	Percent	Number	Percent	Number	Percent
Say Take Any Steps to Provide Security:	55% (49.7%-60.7%)[1]	179/324	74%[2]	67/90	65% (+/-6.1%)[3]
Say Take Steps to Provide Security During Transmission:	39% (33.2%-44.1%)	125/324	54%	49/90	49% (+/- 5.6%)
Say Take Steps to Provide Security After Receipt:	29% (23.8%-34.0%)	93/324	48%	43/90	40% (+/- 4.8%)

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.

TABLE 15a

Percent of All Web Sites Where Third Parties[1] Attempt to Place Cookie

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Third-Party Cookie:	57% (51.8%-62.7%)[2]	192/335	78%[3]	71/91	69% (+/- 4.7%)[4]

TABLE 15b

Of Those Web Sites Where Third Parties Attempt to Place Cookie, Percent that Disclose That Third Parties May Place Cookies

	Random Sample		Most Popular Group		Weighted Analysis
	Percent	Number	Percent	Number	Percent
Disclose That Third Parties May Place Cookies/Collect Information on Site:	22% (16.2%-28.4%)	42/192	51%	36/71	41% (+/- 7.3%)
No Disclosure:	78% (71.6%-83.8%)	150/192	49%	35/71	59% (+/- 7.3%)

1. A "third party" means any domain other than the site surveyed.
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.

Federal Trade Commission	Toll-free 1-877-FTC-HELP
www.ftc.gov	For the Consumer