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

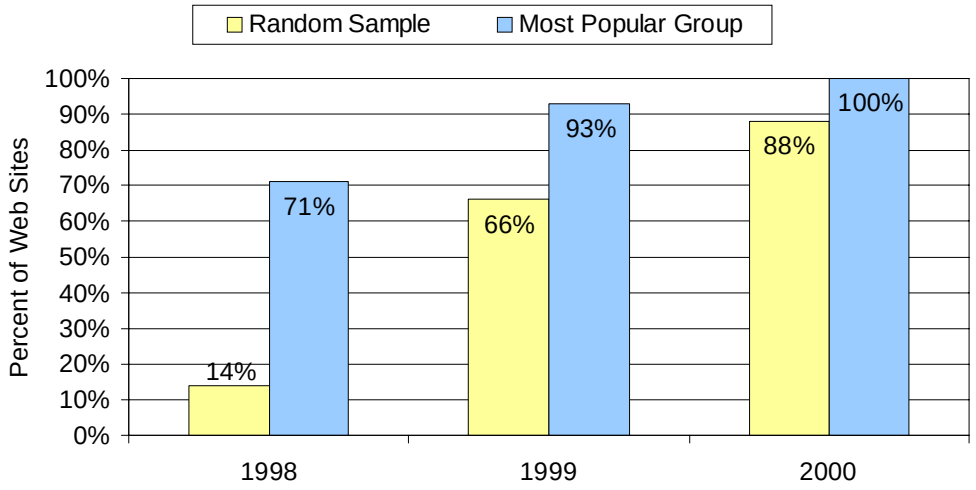
weighted analysis figure is 76%.[58] Most of the sites surveyed, therefore, are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior, or surfing behavior[59] information they collect to personal identifying information.

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.

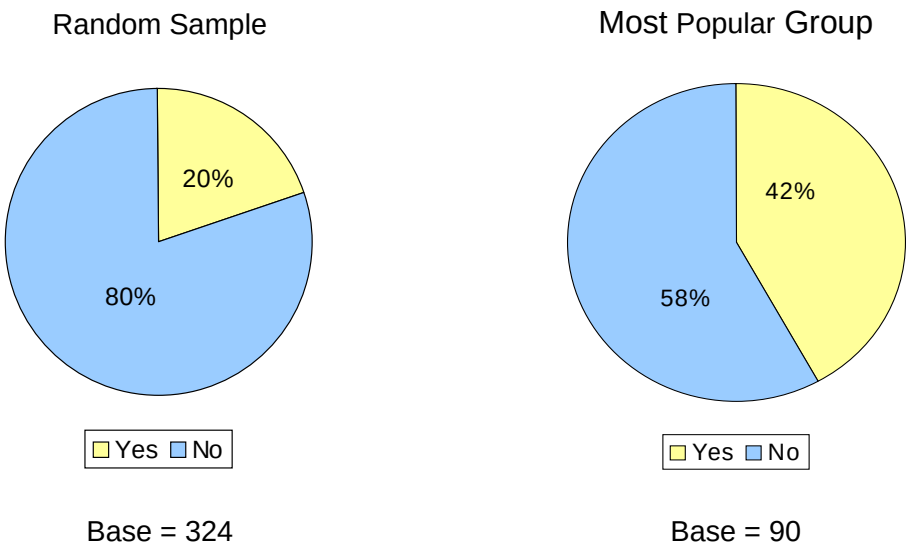
4. CONTENT OF PRIVACY DISCLOSURES: COMPARISON WITH FAIR INFORMATION PRACTICE PRINCIPLES

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

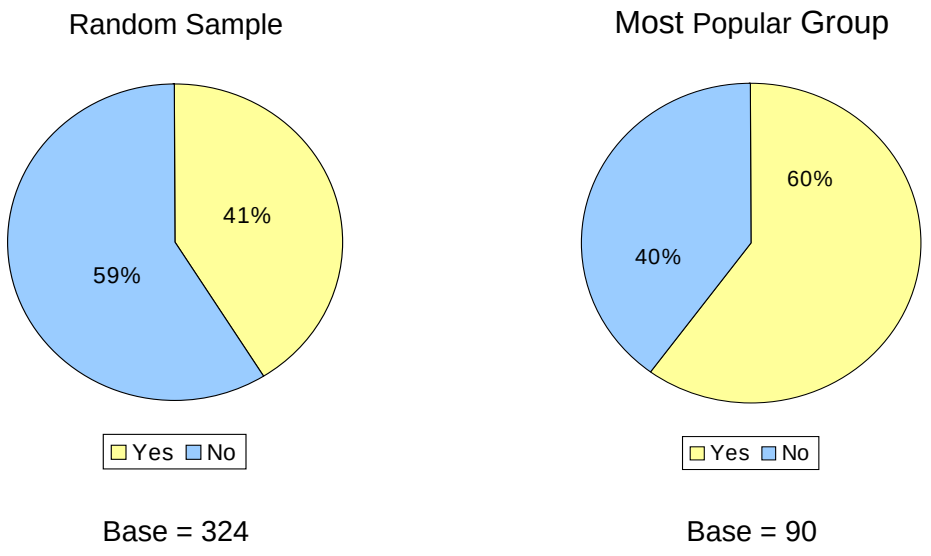


Source: Appendix C, Table 4.

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.

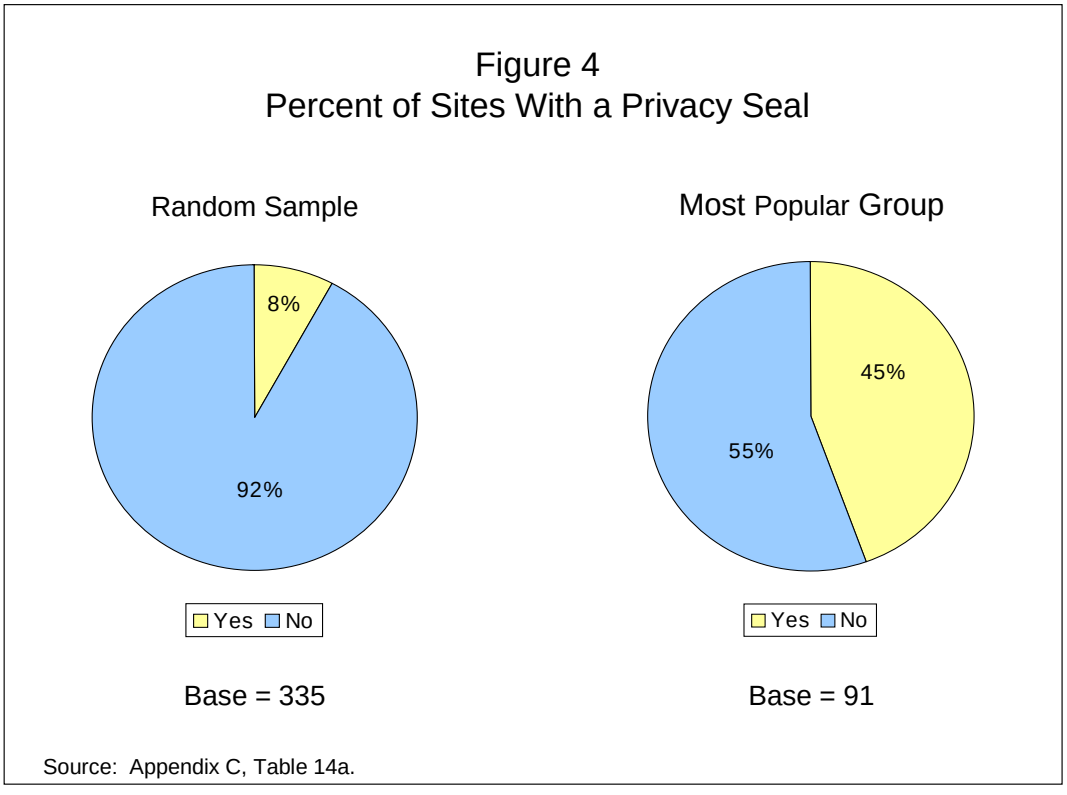
The Commission's Survey asked whether sites disclose that they (1) take any steps to provide security,[123] and if so, whether they (2) take any steps to provide security for information during transmission, or (3) take any steps to provide security for information after receipt.[124] A site was awarded 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



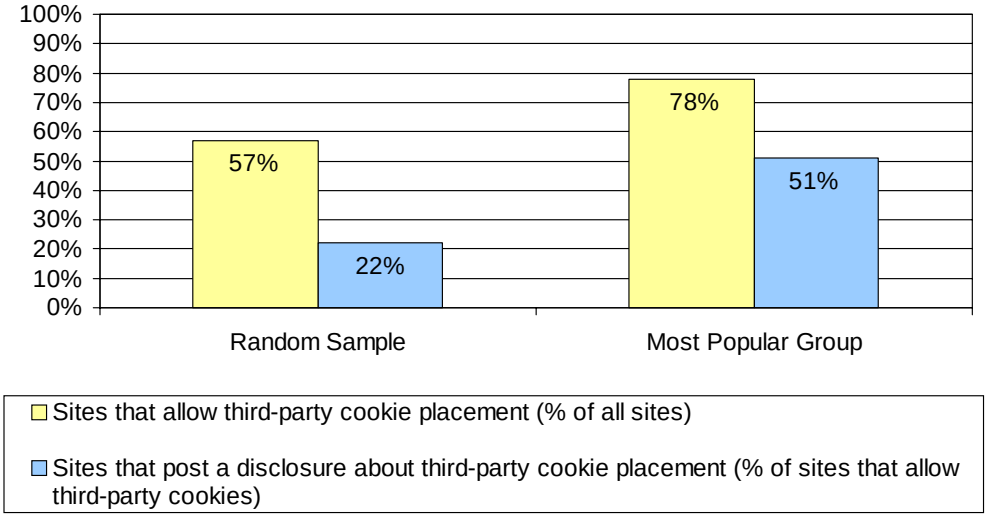
Source: Appendix C, Table 14a.

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).