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 ana-

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

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

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

(1) Notice Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (., ., 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 (., ., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

(3) Access Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to

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

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

---

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

I. INTRODUCTION AND BACKGROUND

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

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

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

B. CONSUMER CONCERNS ABOUT ONLINE PRIVACY

With this remarkable growth in e-commerce has come increased consumer awareness that online businesses are collecting and using personal data, and increased consumer concern about the privacy of this data. Recent survey data demonstrate that 92% of consumers are concerned (67% are very concerned) about the misuse of their personal information online. Concerns about privacy online reach even those not troubled by threats to privacy in the off-line world. Thus, 76% of consumers who are not generally concerned about the misuse of their personal information fear privacy intrusions on the Internet. This apprehension likely translates into lost online sales due to lack of confidence in how personal data will be handled. Indeed, surveys show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce, [4] and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction. [5] One study estimates that privacy concerns may have resulted in as much as $2.8 billion in lost online retail sales in 1999, [6] while another suggests potential losses of up to $18 billion by 2002 (compared to a projected total of $40 billion in online sales), if nothing is done to allay consumer concerns. The level of consumer unease is reflected in the results of a recent study in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential, and 82% agreed that government should regulate how online companies use personal information. [7]

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

C. T

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

(1) Notice data collectors must disclose their information practices before collecting personal information from consumers;

(2) Choice consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;

(3) Access consumers should be able to view and contest the accuracy and completeness of data collected about them; and

(4) Security data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

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

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

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

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.[4] In a series of public meetings, the Advisory Committee discussed options, and the

Other online privacy seal programs have been announced or are in the early stages of development,[43] 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.[44]

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.[45] 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[46] by third parties.

The Survey examined Web sites that had 39,000 or more unique visitors[47] each month. These sites were drawn from a list provided by Nielsen//NetRatings based on January 2000 traffic figures. Two separate groups were drawn from this pool of sites: (1) a random sample of all of the sites (the Random Sample) and (2) the 100 busiest sites (the Most Popular Group). A detailed methodology describing the sample selection, data collection, data entry, and data analysis is included in Appendix A. Lists of the sites included in the Random Sample and the Most Popular Group are set forth in Appendix B.

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

information from consumers and (b) posts privacy disclosures.[4] Privacy disclosures were defined to include both privacy policies, (descriptions of a site s information practices located together in a paragraph or on a Web page), and information practice statements, discrete statements about particular information practices.[5] 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.[6]

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

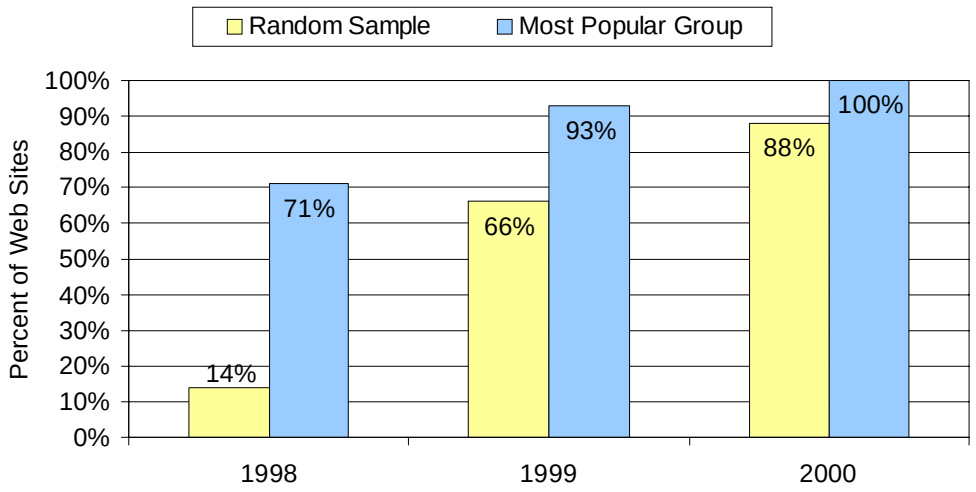
weighted analysis figure is 76%.[47] Most of the sites surveyed, therefore, are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior, or surfing behavior information they collect to personal identifying information.

REQUENCY OF RIVACY ISCLOSURES OMPARISON WITH REVIOUS URVEYS

The results of the 1999 GIPPS Report showed a significant increase over the previous year in the percent of Web sites posting at least one privacy disclosure . . ., either a unified privacy policy or a discrete information practice statement (such as, This is a secure order form). Sixty-six percent of Web sites in the GIPPS random sample, compared with 14% of Web sites in the Commission s 1998 Comprehensive Sample had such disclosures. This year, the Commission s Survey findings demonstrate continued improvement on this front, with 88% of Web sites in the Random Sample posting at least one privacy disclosure. Of sites in the Random Sample that collect personal identifying information, 90% post at least one privacy disclosure.[48] All of the sites in the Most Popular Group post at least one privacy disclosure,[49] compared with 93% of the sites in Professor Culnan s 1999 survey of the 100 busiest sites, and 71% in the Commission s 1998 Most Popular Sample. The weighted analysis figure is 96%.[50]

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

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 、 disclosure, even if related to only one discrete information practice. Thus, a site posting only a statement such as Click here if you do not want to receive email updates from us, or This is a Secure Order Form, was given credit for having a privacy disclosure. Moreover, even the posting of a privacy policy does not necessarily mean that a site follows any or all fair information practices, as the policy might address only certain practices and not others. Accordingly, the Commission s 2000 Survey went beyond the mere counting of disclosures; it analyzed the nature and substance of these privacy disclosures in light of the fair information practice principles described in the 1998 Report.

Implementation of Notice & Choice Only

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

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

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

The Commission s Survey asked several questions designed to ascertain if sites are following the Notice principle. A site was deemed to have provided Notice if it met the following criteria: (1) it posts a privacy policy; (2) it says anything about what specific personal information it collects; (3) it says anything about how the site may use personal information internally; and (4) it says anything about whether it discloses r personal informatb*-(tionandca(4os are foll9 488.397 253.2

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

Consumer survey research shows that online consumers are also concerned about how their information is used by Web sites for marketing purposes. According to one recent study, online consumers dread junk mail : 78% of Internet users who have purchased online report being concerned that the company from which they have made a purchase will use personal information to send them unwanted email, or spam. Of those Internet users who have not made any purchases online, nearly all 94% are concerned about being spammed, and concern among both buyers and non-buyers has increased since 1998. [4] Further, over 70% of consumers identified the ability to be removed from a site s mailing list as a very important criterion in assessing a site s privacy protections. [4]

Consistent with these consumer concerns, the Cna juhn0.0421 Tw(TCon8.0-en)]Tr.00Tj/F1tall/F18 TD-0.0

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; the costs and benefits of providing access; and how to ensure adequate authentication that the person requesting access is the data subject. 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. 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 of these disclosures. In the Random

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

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

As discussed in greater detail below, the Advisory Committee also explored the meaning of adequate security and developed implementation options. There was strong agreement among Committee members that security is a process: no one static standard can assure adequate security, as threats, technology, and the Internet itself are constantly evolving. [4] 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. [5] The Advisory Committee pointed out that, while most consumers worry about security for the transmission of personal information to a site, security threats to that information once a site receives it are far more substantial and pervasive.

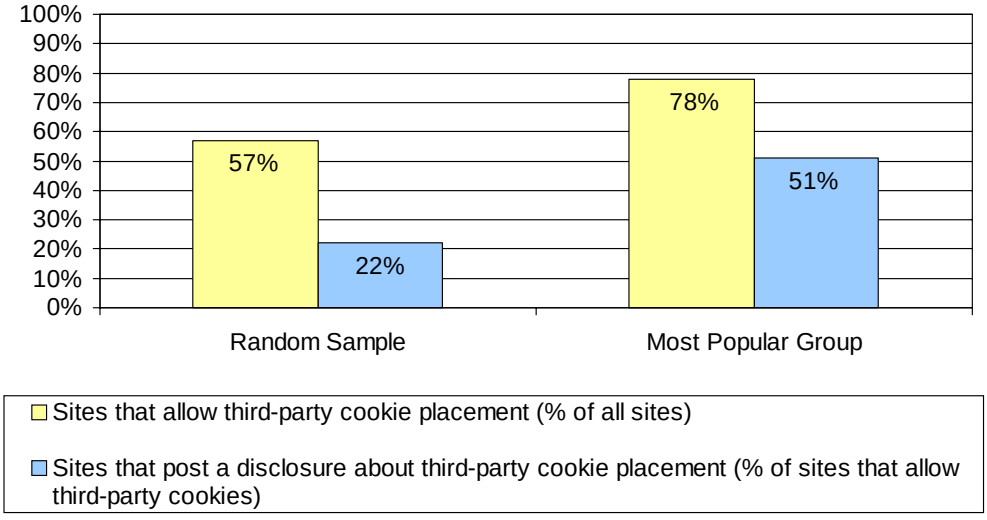
The Advisory Committee also examined whether, and to what extent, Web sites should make disclosures about security. As discussed in greater detail below, [6] the Committee agreed

HIRD- ARTY OOKIES

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. 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. The weighted analysis figure is 69%. 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.

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. The weighted analysis figure is 41%.

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. , COPE OF ONTENT NALYSIS

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

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

- With respect to

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

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

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

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

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

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

d. Best Practices

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

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

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

III. THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY

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

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

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

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

The Advisory Committee Report also evaluates whether the Access principle should apply to entities other than the original data collector. [4] Members of the Advisory Committee generally agreed that businesses should provide access to data held by their agents. [5] 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. [6] Others believed that this requirement would be too burdensome.

B. SECURITY

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

The Advisory Committee Report recommends implementation of a security approach that requires that each commercial Web site have a security program to protect personal data that it maintains, and that the program specify its elements and be appropriate to the circumstances. /[4] The elements of the security program may include conducting a risk assessment; establishing and implementing a security system; managing policies and procedures based on the risk assessment; conducting periodic training for employees; conducting audits; conducting internal reviews; and conducting periodic reassessment of risk./ The appropriateness standard, which would be defined through case-by-case adjudication, takes into account changing security needs over time as well as the particular circumstances of the Web site, including the risks it faces, the costs of protection, and the type of the data it maintains./

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

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

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

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

Indeed, as noted above, only 20% of the busiest sites on the World Wide Web implement to some extent all four fair information practices in their privacy disclosures. Even when only Notice and Choice are considered, fewer than half of the sites surveyed (41%) meet the relevant standards. These numbers fall well short of the meaningful broad-based privacy protections the Commission was seeking and that consumers want. Moreover, the enforcement mechanism so

C. LEGISLATIVE RECOMMENDATION

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

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

(1) Notice Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (., 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 (., 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

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, , 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. Cyber Dialogue, , available at < http:// www.cyberdialogue.com/resource/data/ic/index.html > (69 million users); Cyberstats, , *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. .

4. Ernst & Young/Technometrica, - *&* (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. The Gallup Organization, (Feb. 23, 2000), available at < http:// www.gallup.com/poll/releases/pr000223.asp > (48%); Business Week/Harris Poll, , available at < http://www.businessweek.com/2000/00_12/ b3673010.htm?scriptFramed. > (some results also available in B

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, / , 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., (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, *$4.6 1999* (Apr. 18, 2000), available at < http://www.iab.net/news/content/revenues.html > [hereinafter IAB 1999 Revenue Report]. This indicates that Internet advertising spending is growing faster than historical trends in other media. Internet ad revenues hit the $4 billion/year mark after just five years. . In inflation-adjusted dollars, it took six years before television ad revenues hit $4 billion/year, 13 years for cable television, and 30 years for radio. Internet Advertising Bureau, *: 1999 -* , available at < http://www.iab.net/news/content/3Q99exec.html > .

9. IAB 1999 Revenue Report.

10. Internet Advertising Bureau, *1996* (Mar. 25, 1997), available at < http://www.iab.net > .

11. The exchange of personal identifying information as part of a commercial transaction or other online exchange raises special concerns. Once disclosed, such information may be subject to myriad uses, many if not all of which may be unknown to the consumer. Also, once disclosed to entities other than the data collector, the consumer may lose all control over the use and further dissemination of the information.

12. Alan F. Westin, *:* , P AC A D A E CA B E at 11 (Nov. 1999) [hereinafter Westin/PAB 1999]. - 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., (Oct. 1999), available at < http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html > (two-thirds of American and Canadian online shoppers feel insecure about exchanging personal information over the Internet).

13. IBM Privacy Survey at 73.

14. Fewer than 20% of adults who agree that the Internet threatens their privacy have placed orders online, while 54% of those who disagree that the Internet threatens pri-

vacy have placed orders. Cyber Dialogue E-Commerce Survey. IBM Privacy Survey at 96 (a majority of consumers on all but health sites have made a decision to not use or purchase from a Web site because of concerns regardit4,0/F10 ,w4,0i orumeonalot

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

22. p. 4 and accompanying notes.

23. The Commission s review of privacy has mainly focused on online issues because the Commission believes privacy is a critical component in the development of electronic commerce. However, the FTC Act and most other statutes enforced by the Commission apply equally in the offline and online worlds. Further, as described , 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. . , No. 99-WM-783 (D. Colo. filed Apr. 21, 1999); , Docket No. 9255 (Feb. 10, 2000), , No. 00-1141 (D.C. Cir. Apr. 4, 2000). This experience as well as recent concerns about the merging of online and offline databases, the blurring of distinctions between online and offline merchants, and the fact that a vast amount of personal identifying information is collected and used offline make clear that significant attention to offline privacy issues is warranted.

24. : at 7-14 (June 1998), available at < http://www.ftc.gov/reports/privacy3/index.htm > [hereinafter 1998 Report]. December 1996 Staff Report at 8-12, available at < http://www.ftc.gov/reports/privacy/privacy1.htm > (summarizing participants testimony on fair information practices).

25. 1998 Report at 7-11. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The U.S. Privacy Protection Study Commission, (1977); Organization for Economic Cooperation and Development, (1980); U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: - (1995); U.S. Dept. of Commerce, : - (1995); (1995); and the Canadian Standards Association, : (1996).

26. 1998 Report at 7-11.

27. . at 23, 27.

28. . at 42-43. In October 1998, Congress passed the Children s Online Privacy Protection Act of 1998. 15 U.S.C. §§ 6501, . The Act requires that operators of Web sites directed to children under 13 or who knowingly collect personal information from children under 13 on the Internet: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of

38. A list of current participants in the TRUSTe program is available at < http:// www.truste.org/users/users_lookup.html > .

39. A list of current BBB licensees is available at < http://www.bbbonline.org/ businesses/privacy/approved.html > .

40. A list of current CPA Webtrust licensees is available at < http://www.verisign.com/ webtrust/siteindex.html > .

41. A list of current PriceWaterhouseCoopers BetterWeb licensees is available at < http:// www.pwcbetterweb.com/betterweb/BWsitesDir/index.cfm > . Twenty-three companies have applied for the BetterWeb seal. .

42. The Entertainment Software Ratings Board (ESRB) Privacy Online seal program, designed for members of the entertainment software industry, was launched one year ago. A description of the ESRB program is available at < http://www.esrb.org > . In addition, the S.A.F.E. (Secure Assure Faith Entrusted) Dependability Seal Program was launched in October 1999. A description of this program is available at < http:// www.secureassure.org. >

43. 、 p. 20 and accompanying notes.

44. In this study, we define Web site as a domain, the unit of analysis for the Survey. Appendix A at 1.

45. A cookie is a small text file placed on a consumer s computer hard drive by a Web server. The cookie transmits information back to the server that placed it, and, in general, can be read only by that server. For more information about cookies, , ., < http://www.cookiecentral.com > .

46. Unique visitors refers to an estimate of the number of different individuals that visited a Web site in a particular time period, without regard to the number of visits made to or the amount of time spent at the Web site by each individual during that time period. Appendix A at 1.

47. Adult sites, sites that were inaccessible for technical reasons, sites directed to children under the age of 18, business-to-business sites, and sites registered to companies outside the U.S. were excluded from the Survey and the results. Appendix A at 3.

48. Information practice statements include both explicit statements describing a site s information practices (., we will not share your personal information with third parties) as well as statements implicitly offering consumers choice (., click here to be on our mailing list).

49. The staff who participated in the data collection and content analysis were not involved in designing the Survey, in the subsequent data analysis, or in drafting this report.

50. There were over 5,600 such sites in January 2000, whose total unduplicated reach is 98.3%. Appendix A at n.2. That is, it was estimated that 98.3% of all active Web users visited at least one of these sites at least once in the month of January 2000. .

51. As discussed in Appendix A at 7, the weighted results are not generally representative of consumers online experiences because the population from which the Random Sample was drawn excluded sites with fewer than 39,000 unique visitors in one month. The weighted results, therefore, represent consumer experiences only on that part of the Web from which the sample was drawn.

52. Nine sites were excluded as either non-U.S. registered sites, business-to-business sites, children s sites, duplicates, or inaccessible. Appendix A at 3.

53. Sites may also collect information about consumers in ways that are less obvious to consumers, such as through cookies or through server logs that capture information about the consumer s computer. Although information collected via these passive means is usually non-identifying, it may be linked with personal identifying information. To determine whether Web sites were collecting personal information from consumers, the Commission s Survey looked for direct methods of data collection from consumers. It did not examine whether the sites surveyed placed cookies (which can be used to store a consumer s password or items selected for purchase in a shopping cart, as well as to track consumers browsing patterns), although it did ask whether sites their use of cookies. As discussed below, the Survey separately collected information on whether third parties were placing cookies at Web sites.

54. Personal identifying information includes such information as name, email, postal ad-

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

98. Appendix C, Table 4. If, under an alternative scoring model, sites were credited with Choice for providing either internal third-party choice, 82% of sites in the Random Sample that collect personal identifying information would receive Choice credit. Further, 27% of such sites would receive credit for meeting all four fair information practice principles (compared with 20%, 、 p. 12), and 54% would receive credit for meeting Notice & Choice (compared with 41%, 、 p. 13). Appendix C, Table 10.

99. Appendix C, Table 4. If sites were credited for Choice for providing either internal third-party choice, 98% of sites in the Most Popular Group that collect personal identifying information would receive Choice credit. Further, 63% of such sites would receive credit for meeting all four fair information practice principles (compared with 42%, 、 p. 12), and 87% would receive credit for meeting Notice & Choice (compared with 60%, 、 p. 13). Appendix C, Table 10.

100. Appendix C, Table 4.

101. 1998 Report at 9.

102. . 、 102. *102.*

10.

102.

1

113. Many Committee members also agreed that Access is an important framework for addressing data inaccuracies. Advisory Committee Report at 8-14 (describing four options for implementing Access, each of which takes into account the importance of correcting data inaccuracies).

114. 1998 Report at 10. Advisory Committee Report at 22-23, 26.

115. Advisory Committee Report at 19.

116. . at 26.

117. Advisory Committee Transcript of February 4, 2000, at 127 (S. Baker, Steptoe & Johnson), available at < www.ftc.gov/acoas > ; . at 128 (T. Gau, America Online, Inc.).

118. See Section III, below.

119. Advisory Committee Report at 20-21. As the Committee noted, sites that do not disclose anything about security may in fact be providing security measures. . at 20.

120. . at 20.

121. . at 20-21.

122. Business Week/Harris Poll. Eighty percent of Internet users stated that they would be encouraged to use the Internet more in general, 69% to register at a site, and 73% to

136. Appendix C, Table15a.

137. .

138. To determine whether third-party cookies observed during the online phase of data collection for the Survey were sent by network advertising companies engaged in profiling, Commission staff reviewed the completed Third-Party Cookie Survey Forms, Appendix B, and visited the Web sites associated with the domains of the observed cookies. Only companies whose Web sites explicitly stated that the company targeted banner ads on the basis of consumer characteristics were classified as profilers. Appendix A. The vast majority of these companies are members of the Network Advertising Initiative (NAI), an industry group that has been working to create a self-regulatory program for network advertising companies that collect information about consumers. As noted above, the Commission will soon address online profiling in a separate report to Congress.

139. Appendix C, Table 15b.

140. .

141. , B E WEE , Mar. 20, 2000, at 86-87; CNET News; T E I D S A DA D, Mar. 13, 2000, at 208-09; *!*, C E RE , May 2000, at 43, 47.

142. Jupiter Communications, Inc., *: 64* - (Aug. 17, 1999), press release available at < http://www.jupitercommunications.com > .

143. Such pre-checked boxes were deemed to provide opt-out choice, as they require an affirmative act by the consumer unchecking the box in order to prevent the further use of the information.

144. Notice of Establishment of the Federal Trade Commission Advisory Committee on Online and Access and Security and Request for Nominations, 64 Fed. Reg. 71,457 (1999), available at < http://www.ftc.gov/acoas > [hereinafter Establishment and Nomination Notice]. The FACA applies to groups, such as this one, established by a government agency that include non-federal members, involve deliberation among the group s members, and provide advice or recommendations as a group to the agency. 5 U.S.C. App. § 3; 16 C.F.R. § 16.2; , . . , 997 F.2d 898, 913-14 (D.C. Cir. 1993).

145. Charter of the Federal Trade Commission Advisory Committee on Online Access and Security, available at < http://www.ftc.gov/acoas/acoascharter.htm > [hereinafter Charter].

146. Establishment and Nomination Notice at 71,459; Charter.

147. Establishment and Nomination Notice. The Commission received approximately 190 nominations from highly qualified individuals. The complete list of nominees is available at < http://www.ftc.gov/acoas/nominations/index.htm > .

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

149. Shortly after each meeting, a complete transcript of the meeting was posted on the 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. . at 6-8.

153. . at 15-18.

154. . at 4-14.

155. . at 4.

156. . at 5.

157. . at 9.

158. . at 13-14.

159. . at 9.

160. . 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). . at 6.

161. . at 9.

162. . at 10.

163. .

164. .

165. .

166. .

167. . at 11.

168. .

169. . at 11-12.

170. . at 12.

171. .

172. . at 13.

173. . at 14.

174. . at 6-8.

175. . at 7.

176. .

177. .

178. . at 16.

179. . at 15.

180. .

181. . at 21-26.

182. .

183. . at 19.

184. Advisory Committee Transcript of February 4, 2000, at 127 (S. Baker, Steptoe & Johnson), available at < www.ftc.gov/acoas > ; . at 128 (T. Gau, America Online, Inc.).

185. Advisory Committee Report at 26. The Advisory Committee presents five options before making its recommendation. These options are 1) rely on existing remedies; 2) require that Web sites maintain a security program; 3) rely on industry-specific security standards; 4) require security procedures that are appropriate under the circumstances; and 5) establish a sliding scale of security standards. . at 21-26.

186. . at 26.

187. . at 25.

188. Section II.B.4 .

189. Advisory Committee Report at 19. The Report also states that notice is important in triggering one of the few available enforcement mechanisms for ensuring adequate security online an FTC action for deceptive trade practices. . at 20.

190. . at 20.

191. .

192. . at 20-21.

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