SELF-REGULATION AND PRIVACY ONLINE:

A REPORT TO CONGRESS

FEDERAL TRADE COMMISSION
JULY 1999

Federal Trade Commission*

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

Bureau of Consumer Protection

Staff Authors

Martha K. Landesberg
Laura Mazzarella

* The Commission vote to issue this Report was 3-1, with Commissioner Anthony concurring in part and dissenting in part. Commissioner Anthony's statement is attached to the Report. Commissioner Swindle's concurring statement is also attached.

TABLE OF CONTENTS

I. Introduction and Background 1
A. The Growth of Electronic Commerce 1
B. Consumer Privacy Concerns 2

II. The Commission's Approach to Online Privacy 3

III. Congressional Response 5

IV. The State of Online Privacy Self-Regulation Today 6
A. Recent Assessments of Web Sites' Compliance with Fair Information Practice Principles 7
B. The Online Privacy Alliance 8
C. Seal Programs 9

V. Conclusion 12

Endnotes 15

I. INTRODUCTION AND BACKGROUND

In June 1998 the Federal Trade Commission issued *Privacy Online: A Report to Congress* ("1998 Report"), an examination of the information practices of commercial sites on the World Wide Web and of industry's efforts to implement self-regulatory programs to protect consumers' online privacy.[1] Based in part on its extensive survey of over 1400 commercial Web sites, the Commission concluded that effective self-regulation had not yet taken hold.[2] In both the 1998 Report and in subsequent testimony before Congress, the Commission raised concerns about protecting the privacy of children's personal information online and recommended that Congress pass legislation to address these concerns.[3] In its testimony, the Commission also raised concerns about the progress of industry self-regulation, but noted that industry leaders had indicated their commitment to work toward self-regulatory solutions. Accordingly, the Commission did not recommend legislative action in the area of online privacy for consumers generally, and instead urged industry to focus on developing and implementing broad-based and effective self-regulatory programs.[4]

In the ensuing year, there have been important developments both in the growth of the Internet as a commercial marketplace and in consumers' and industry's responses to the privacy issues posed by the online collection of personal information. The Commission has examined these developments and now presents its views on the progress made in self-regulation since last June, as well as its plans to encourage industry's full implementation of online privacy protections.

A. THE GROWTH OF ELECTRONIC COMMERCE

Commerce on the World Wide Web is booming. The United States Department of Commerce recently announced that online sales tripled from approximately $3 billion in 1997 to approximately $9 billion in 1998.[5] Online revenues of North American retailers in the first half of 1998 were approximately $4.4 billion.[6] Online advertising revenues have grown from $906.5 million in 1996 to $1.92 billion in 1998.[7] In 1998, revenues for Internet advertising

exceeded those for advertising on outdoor billboards.[8] It is estimated that almost 80 million adults in the United States are using the Internet.[9] They are finding a vast array of products, services, and information in a marketplace that has experienced exponential growth since its beginnings only a few years ago.

The Web is also a rich source of information about online consumers. Web sites collect much personal information both explicitly, through registration pages, survey forms, order forms, and online contests, and by using software in ways that are not obvious to online consumers. Through "cookies" and tracking software, Web site owners are able to follow consumers' online activities and gather information about their personal interests and preferences. These data have proved extremely valuable to online companies because they not only enable merchants to target market products and services that are increasingly tailored to their visitors' interests, but also permit companies to boost their revenues by selling advertising space on their Web sites.[10] In fact, an entire industry has emerged to market a variety of software products designed to assist Web sites in collecting and analyzing visitor data and in serving targeted advertising.[11]

B. Consumer Privacy Concerns

Notwithstanding the substantial benefits that consumers may derive from using the Internet, consumers still care deeply about the privacy of their personal information in the online marketplace. Eighty-seven percent of U.S. respondents in a recent survey of experienced Internet users stated that they were somewhat or very concerned about threats to their privacy online.[12] Seventy percent of the respondents in a recent national survey conducted for the National Consumers League reported that they were uncomfortable providing personal information to businesses online.[13] Consumers are particularly concerned about potential transfers to third parties of the personal information they have given to online businesses.[14] It is not surprising that only about one-quarter of Internet users go beyond merely browsing for information to actually purchasing goods and services online.[15]

II. THE COMMISSION'S APPROACH TO ONLINE PRIVACY

For almost as long as there has been an online marketplace, the Commission has been deeply involved in addressing online privacy issues.[16] The Commission's goal has been to understand this new marketplace and its information practices, to assess the impact of these practices on consumers, and to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online. The Commission's efforts have been based on the belief that greater protection of personal privacy on the Web will not only benefit consumers, but also benefit industry by increasing consumer confidence and ultimately their participation in the online marketplace.

The Commission's 1998 Report discussed the fair information practice principles 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*.[17] The 1998 Report identified the core principles of privacy protection common to the government reports, guidelines, and model codes that have emerged since 1973: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.[18]

The Notice/Awareness principle is the most fundamental: consumers must be given notice of a company's information practices before personal information is collected from them. The scope and content of the notice will vary with a company's substantive information practices, but the notice itself is essential. The other core principles have meaning only if a consumer has notice of an entity's information practices and his or her rights with respect thereto.

The other core principles are briefly summarized here. The Choice/Consent principle requires that consumers be given options with respect to whether and how personal information collected from them may be used.[19] The Access/Participation principle requires that consumers be given reasonable access to information collected about them and the ability to contest that data's accuracy and completeness.[20] The Integrity/Security principle requires that

companies take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.[21] Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of the Enforcement/Redress principle, which requires governmental and/or self-regulatory mechanisms to impose sanctions for noncompliance with fair information practices.[22]

The 1998 Report assessed existing self-regulatory efforts in light of these fair information practice principles and set out the findings of the Commission's extensive survey of commercial Web sites' information practices. The survey found that, although the vast majority of sites collected personal information from consumers – 92% in the sample representing all U.S.-based commercial sites likely to be of interest to consumers – only 14% posted any disclosure regarding their information practices, and only 2% posted a comprehensive privacy policy.[23] The results of the Commission's census of the busiest sites on the World Wide Web were more positive: while 97% collected personal information, 71% posted a disclosure and 44% posted a comprehensive privacy policy.[24] The Commission's survey of sites directed to children revealed that 89% collected personal information from children, 24% posted privacy policies and only 1% required parental consent prior to the collection or disclosure of children's information.[25]

The 1998 Report concluded that an effective self-regulatory system had yet to emerge and that additional incentives were required in order to ensure that consumer privacy would be protected. Noting its particular concern about the vulnerability of children, the Commission recommended that Congress adopt legislation setting forth standards for the online collection of information from children. Furthermore, in Congressional testimony last July, the Commission deferred judgment on the need for legislation to protect the online privacy of adult consumers, but presented a legislative model that Congress could consider if industry failed to develop and implement effective self-regulatory measures.[26]

III. CONGRESSIONAL RESPONSE

On October 21, 1998, the President signed into law the Children's Online Privacy Protection Act of 1998 ("COPPA").[27] The Act, passed by Congress just four months after the Commission's 1998 Report, 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.[28] The Act directs the Commission to adopt within one year regulations implementing these requirements.[29]

On April 20, 1999, the Commission issued a proposed Children's Online Privacy Protection Rule and is now in the midst of this rulemaking effort.[30] The proposed rule requires Web site operators to post prominent links on their Web sites to a notice of how they collect and use personal information from children under the age of 13, and sets out, among other things, standards for complying with the Act's notice, parental consent, and access requirements.[31] As required by the COPPA, the proposed rule also includes a safe harbor provision under which industry groups or others may seek Commission approval for self-regulatory guidelines. Web site operators who participate in such approved programs may be subject to the review and disciplinary procedures provided in those guidelines in lieu of formal Commission investigation and law enforcement.[32] The safe harbor would serve both as an incentive for industry self-regulation, and as a means of ensuring that the Act's protections are implemented in a

manner sensitive to industry-specific concerns and developments in technology. Commission staff is reviewing comments on the proposed rule and will hold a public workshop this month to solicit further discussion and comment on the issue of verifiable parental consent. The Commission will issue a final rule this fall.

IV. THE STATE OF ONLINE PRIVACY SELF-REGULATION TODAY

As noted in the Commission's 1998 Report, self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology. During the past year the Commission has been monitoring self-regulatory initiatives to address the privacy concerns of online consumers. In some areas, there has been much progress. The results of two new surveys of commercial Web sites suggest that online businesses are providing significantly more notice of their information practices than they were last year. In addition, several significant and promising self-regulatory programs, including privacy seal programs, are underway.

There are also major challenges for self-regulation. The new survey results show that, despite the laudable efforts of industry leaders, the vast majority of even the busiest Web sites have not implemented all four substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity. In addition, the seal programs discussed below currently encompass only a handful of all Web sites. Thus, it is too early to judge how effective these programs will ultimately be in serving as enforcement mechanisms to protect consumers' online privacy.

The Commission believes that there are additional steps that it can take, together with industry, and consumer and privacy groups, to build upon the progress in self-regulation to date and to work toward full implementation of effective online privacy protections. Some recent developments and plans for future work to achieve this goal are discussed below.

A. Recent Assessments of Web Sites' Compliance with Fair Information Practice Principles

Professor Mary Culnan of the McDonough School of Business at Georgetown University recently announced the results of two industry-funded surveys of commercial Web sites, conducted during the week of March 8, 1999. The Georgetown Internet Privacy Policy Survey ("GIPPS")[33] reports findings on the information practices of 361 Web sites drawn from a list of the 7,500 busiest servers on the World Wide Web.[34] Ninety-three percent of the sites in this survey collect personal information from consumers, and 66% post at least one disclosure about their information practices.[35] Forty-four percent of these sites post privacy policy notices.[36] Although differences in sampling methodology prevent direct comparisons between the GIPPS findings and the Commission's 1998 results,[37] the GIPPS Report does demonstrate the real progress industry has made in giving consumers notice of at least some information practices. On the other hand, only 10% of the sites in the GIPPS sample are implementing all four substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity.[38] The GIPPS Report findings discussed above are summarized in Figure 1.

Professor Culnan also conducted a census of the top 100 Web sites commissioned by the Online Privacy Alliance, a coalition of more than eighty online companies and trade associations that formed early in 1998 to encourage self-regulation in this area ("OPA Study").[39] As is true of the GIPPS sample, nearly all (99%) of the sites in the OPA Study collect personal information from consumers. Ninety-three percent of these sites provide at least one disclosure about their information practices, while 81% of these sites post privacy policy notices.[40] This represents continued progress since last year, when 71% of the sites in the Commission's 1998 "Most Popular" sample posted an information practice disclosure.[41] Only 22% of the sites in the OPA study address all four of the substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation and Security/Integrity, however.[42] These OPA Study findings are summarized in Figure 1.

FIGURE 1

	1999 GIPPS Report	1999 OPA Study
Number of sites in sample	361	100
Number of sites collecting personal information	337	99
Percent of sites in sample collecting personal information	93%	99%
Number of sites posting any privacy disclosure	238	93
Percent of sites in sample posting any privacy disclosure	66%	93%
Number of sites posting a privacy policy notice	157	81
Percent of sites in sample posting a privacy policy notice	44%	81%
Number of sites posting a disclosure for all four substantive fair information practice principles	36	22
Percent of sites in sample posting a disclosure for all four substantive fair information practice principles	10%	22%

The GIPPS and OPA Study results suggest that the majority of the more frequently-visited Web sites are implementing the basic Notice/Awareness principle by disclosing at least some of their information practices. The findings also indicate, however, that only a relatively small percentage of these sites is disclosing information practices that address all four substantive fair information practice principles. Both studies indicate that there has been real progress since the Commission issued its 1998 Report. Nevertheless, the low percentage of sites in both studies that address all four substantive fair information practice principles demonstrates that further improvement is required to effectively protect consumers' online privacy.

B. THE ONLINE PRIVACY ALLIANCE[43]

On June 22, 1998, the Online Privacy Alliance (OPA), a coalition of industry groups, announced its Online Privacy Guidelines, which apply to individually identifiable information

collected online from consumers.[44] Pursuant to these guidelines, OPA members agree to adopt and implement a posted privacy policy that provides comprehensive notice of their information practices. The notice includes a statement of what information is being collected from consumers and how it is being used; whether the information will be disclosed to third parties; consumers' choices regarding the collection, use and distribution of the information; data security measures; and the steps taken to ensure data quality and access to information. The OPA Guidelines also include provisions on choice, feasible consumer access to identifiable information, and data security, and call for self-enforcement mechanisms, such as online seal programs, that provide consumers with redress.

The OPA Guidelines have been used by the leading privacy seal programs, which have adapted them to fit their own program requirements. Unlike the seal programs, however, the OPA does not monitor members' compliance or provide sanctions for noncompliance. The central focus of OPA's efforts since release of its Guidelines has been business education to promote widespread adoption of online privacy policies.

C. Seal Programs

An encouraging development in the private sector's efforts toward self-regulation is the emergence of online seal programs. These programs require their licensees to abide by codes of online information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Web sites. Seal programs offer an easy way for consumers to identify Web sites that follow specified information practice principles, and for online businesses to demonstrate compliance with those principles.

1. TRUSTe[45]

TRUSTe, an independent, non-profit organization founded by the CommerceNet Consortium and the Electronic Frontier Foundation, was launched nearly two years ago, on June 10, 1997. The first online privacy seal program, TRUSTe currently has more than 500 licensees

representing a variety of industries.[46] Since December 1998, TRUSTe's license agreement,[47] which governs licensees' collection and use of "personally identifiable information,"[48] has taken a more comprehensive approach to privacy by requiring licensees to follow standards for notice, choice, access and security based upon the OPA Guidelines. The license agreement also requires licensees to submit to monitoring and oversight by TRUSTe, as well as a complaint resolution procedure.

The TRUSTe program includes third-party monitoring and periodic reviews of licensees' information practices to ensure compliance with program requirements. These reviews include "Web Site reviews," in which TRUSTe examines and monitors changes in licensees' privacy statements and tracks unique identifiers in licensees' databases (a practice known as "seeding") to determine whether consumers' requests to be removed from those databases are being honored; and "On-Site reviews" in which a third-party auditing firm can be called in, should TRUSTe have reason to believe that a licensee is not in compliance with the terms of the license agreement. Licensees must provide consumers with a way to submit concerns regarding their information practices, and agree to respond to all reasonable inquiries within five days. TRUSTe also plays a part in resolving consumer complaints. TRUSTe provides for public reporting of complaints, and, in appropriate circumstances, will refer complaints to the Commission.

2. BBB*ONLINE* PRIVACY SEAL PROGRAM[49]

BBB*OnLine*, a subsidiary of the Council of Better Business Bureaus, launched its privacy seal program for online businesses on March 17, 1999. Forty-two sites currently post BBB*OnLine* seals, and the program has received more than 300 applications. In order to be awarded the BBB*OnLine* Privacy Seal, applicants must post a privacy policy that comports with the program's information practice principles,[50] complete a "Compliance Assessment Questionnaire," and must agree to participate in a consumer dispute resolution system and to

submit to monitoring and review by BBB*OnLine*.[51]

The BBB*OnLine* Privacy Seal Program covers "individually identifiable information,"[52] as well as "prospect information," which is identifying, retrievable information that is collected by the company's Web site from one individual about another.[53] The BBB*OnLine* Privacy Seal Program's consumer complaint resolution procedure is bolstered by several compliance incentives, including public reporting of decisions, and suspension or revocation of the BBB*OnLine* seal, or referral to federal agencies, as sanctions for noncompliance. BBB*OnLine* has committed to adopting a third-party verification system, although this aspect of the program has not yet been implemented. The Commission looks forward to assessing BBB*OnLine*'s enforcement mechanisms when they are fully in place.

3. Other Seal Programs

Several other seal programs have been developed or are under development. One is CPA WebTrust, created by the American Institute of Certified Public Accountants ("AICPA") and the Canadian Institute of Chartered Accountants and announced in September 1997.[54] The CPA WebTrust program, which licenses the CPA WebTrust seal to qualifying certified public accountants, requires participating Web sites to disclose and adhere to stated business practices, maintain effective controls over the security and integrity of transactions, and to maintain effective controls to protect private customer information. Web sites are awarded the CPA WebTrust seal by certified public accountants who conduct quarterly audits to ensure compliance with the program's standards.

Although primarily intended to provide assurance for consumers that a site displaying the seal is a legitimate business that will process transactions and protect sensitive information like credit card numbers, CPA WebTrust also has a privacy component. The information practice requirements in the latest version of the program, introduced in May 1999, conform to the OPA Guidelines. Currently, 19 Web sites have been awarded the CPA WebTrust seal.

Industry sector-specific programs are also beginning to emerge. For example, in October

1998 the Interactive Digital Software Association ("IDSA") adopted its own fair information practice guidelines for its members' Web sites.[55] In addition, on June 1, 1999, the Entertainment Software Rating Board ("ESRB"), an independent rating system for entertainment software and interactive games established by IDSA in 1994, launched ESRB Privacy Online.[56] This online seal program requires participants to adhere to information practice standards that parallel the IDSA guidelines.[57] The program monitors compliance through a verification system that includes unannounced audits and seeding. The program also includes a consumer online hotline for reporting privacy violations and alternative dispute resolution services to resolve consumer complaints.

V. CONCLUSION

The self-regulatory initiatives described above, including the guidelines adopted by the OPA and the seal programs, reflect industry leaders' substantial effort and commitment to fair information practices. They should be commended for these efforts. Enforcement mechanisms that go beyond self-assessment are also gradually being implemented by the seal programs. Only a small minority of commercial Web sites, however, have joined these programs to date. Similarly, although the results of the GIPPS and OPA studies show that many online companies now understand the business case for protecting consumer privacy, they also show that the implementation of fair information practices is not widespread among commercial Web sites.

Based on these facts, the Commission believes that legislation to address online privacy is not appropriate at this time. We also believe that industry faces some substantial challenges. Specifically, the present challenge is to educate those companies which still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.

First, industry groups must continue to encourage widespread adoption of fair information practices. Companies like IBM, Microsoft and Disney, which have recently announced,

among other things, that they will forgo advertising on sites that do not adhere to fair information practices are to be commended for their efforts, which we hope will be emulated by their colleagues. These types of business-based initiatives are critical to making self-regulation meaningful because they can extend the reach of privacy protection to small and medium-sized businesses where there is great potential for e-commerce growth.

Second, industry should focus its attention on the substance of Web site information practices, ensuring that companies adhere to the core privacy principles discussed earlier. It may also be appropriate, at some point in the future, for the FTC to examine the online privacy seal programs and report to Congress on whether these programs provide effective privacy protections for consumers.

Finally, industry must work together with government and consumer groups to educate consumers about privacy protection on the Internet. The ultimate goal of such efforts, together with effective self-regulation, will be heightened consumer acceptance and confidence. Industry should also redouble its efforts to develop effective technology to provide consumers with tools they can use to safeguard their own privacy online.

The Commission has developed an agenda to address online privacy issues throughout the coming year as a way of encouraging and, ultimately, assessing further progress in self-regulation to protect consumer online privacy:

- The Commission will hold a public workshop on "online profiling," the practice of aggregating information about consumers' preferences and interests gathered primarily by tracking their movements online, and, in some cases, combining this information with personal information collected directly from consumers or contained in other databases. The workshop, jointly sponsored by the U.S. Department of Commerce, will examine online advertising firms' use of cookies and other tracking technologies to create targeted, user profile-based advertising campaigns.

- The Commission will hold a public workshop on the privacy implications of electronic identifiers that enhance Web sites' ability to track consumers' online behavior.

- In keeping with its history of fostering dialogue on online privacy issues among all stakeholders, the Commission will convene task forces of industry representatives and privacy and consumer advocates to develop strategies for furthering the implementation of fair information practices in the online environment.

    - One task force will focus upon understanding the costs and benefits of implementing fair information practices online, with particular emphasis on defining the parameters of the principles of consumer access to data and adequate security.

    - A second task force will address how incentives can be created to encourage the development of privacy-enhancing technologies, such as the World Wide Web Consortium's Platform for Privacy Preferences (P3P).

- The Commission, in partnership with the U.S. Department of Commerce, will promote private sector business education initiatives designed to encourage new online entrepreneurs engaged in commerce on the Web to adopt fair information practices.

- Finally, the Commission believes it is important to continue to monitor the progress of self-regulation, to determine whether the self-regulatory programs discussed in this report fulfill their promise. To that end, the Commission will conduct an online survey to reassess progress in Web sites' implementation of fair information practices, and will report its findings to Congress.

In undertaking these efforts, the Commission will be better able to assess industry progress in meeting its self-regulatory responsibilities, while fostering the implementation of effective protections for online privacy in a manner that promotes a flourishing electronic marketplace.

ENDNOTES

1. The Report is available on the Commission's Web site at http://www.ftc.gov/reports/privacy3/index.htm.

2. 1998 Report at 41.

3. 1998 Report at 42; Commission testimony on *Consumer Privacy on the World Wide Web* before the House Subcommittee on Telecommunications, Trade and Consumer Protection, Committee on Commerce (July 21, 1998) at 4-5 [hereinafter "1998 Privacy Testimony"] (available at http://www.ftc.gov/os/1998/9807/privac98.htm).

4. 1998 Privacy Testimony at 4. The Commission also presented a legislative model that Congress could consider in the event that then-nascent self-regulatory efforts did not result in widespread implementation of self-regulatory protections. *Id.* at 5-7.

5. Remarks of Secretary of Commerce William M. Daley, Feb. 5, 1999 (text available at http://204.193.246.62/public.nsf/docs/commerce-ftc-online-shopping-briefing).

6. The Boston Consulting Group, *The State of Online Retailing* 7 and App. A (Nov. 1998).

7. Internet Advertising Bureau, *Advertising Revenue Report* (May 1999) (major findings available at http://www.iab.net/news/content/1998results.html).

8. *Id.*

9. Intelliquest, Inc., *Worldwide Internet/Online Tracking Service 4th Quarter 1998 Report* (results available at http://www.intelliquest.com).

10. *See* Forrester Research, Inc., *Media & Technology Strategies: Making Users Pay* at 4-6 (1998).

11. *See, e.g.,* Rivka Tadjer, *"Following the Patron Path,"* ZD Internet Magazine, Dec. 1997, at 95; Thomas E. Weber, "*Software Lets Marketers Target Web Ads,"* Wall St. J., Apr. 21, 1997, at B1.

12. Lorrie Faith Cranor, et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* at 5 (1999) [hereinafter "AT&T Study"] (available at http://www.research.att.com/projects/privacystudy).

13. Louis Harris & Associates, Inc., *National Consumers League: Consumers and the 21st Century* at 4 (1999).

14. AT&T Study at 2, 10.

15. Intelliquest, Inc., *Worldwide Internet/Online Tracking Service 1st Quarter 1999 Report* (findings summarized at http://www.intelliquest.com/press/release78.asp) (28%); Louis Harris & Associates, Inc. and Alan F. Westin, *E-Commerce & Privacy: What Net Users Want* at 1 (1998) (23%).

16. 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 issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in 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.

These efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. Further, 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* (December 1997); FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (December 1996); FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

The Commission has also brought enforcement actions under Section 5 of the Federal Trade Commission Act to address deceptive online information practices. In 1998 the Commission announced its first Internet privacy case, in which GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities on the GeoCities site. The settlement, which was made final in February 1999, prohibits GeoCities from misrepresenting the purposes for which it collects personal identifying information from or about consumers, including children. It also requires GeoCities to post a prominent privacy notice on its site, to establish a system to obtain parental consent before collecting personal information from children, and to offer individuals from whom it had previously collected personal information an opportunity to have that information deleted. GeoCities, Docket No. C-3849 (Feb. 12, 1999) (Final Decision and Order available at http://www.ftc.gov/os/1999/9902/9823015d&o.htm).

In its second Internet privacy case, the Commission recently announced for public comment a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things, that the site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. In fact, this information was maintained in identifiable form. The consent agreement would require Liberty Financial to

post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children. Liberty Financial, Case No. 9823522 (proposed consent agreement available at http://www.ftc.gov/os/1999/9905/lbtyord.htm).

17. 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).

18. 1998 Report at 7-11.

19. Although choice in this context has been traditionally thought of as either "opt-in" (prior consent for use of information) or "opt-out" (limitation upon further use of information), *id.* at 9, interactive media hold the promise of making this paradigm obsolete through developments in technology. *Id.*

20. *Id.* at 9.

21. *Id.* at 10.

22. *Id.* at 10-11.

23. *Id.* at 23, 27.

24. *Id.* at 24, 28.

25. *Id.* at 31, 35, 37.

26. 1998 Privacy Testimony at 5-7.

27. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L.105-277, 112 Stat. 2681, _____ (October 21, 1998), *reprinted at* 144 Cong. Rec. H11240-42 (Oct. 19, 1998). The goals of the Act are: (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to help protect the safety of children in online fora such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of children's personal information collected online; and (4) to limit the collection of personal information from children without parental consent. 144 Cong. Rec. S12741 (Oct. 7, 1998) (Statement of Sen. Bryan).

28. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L.105-277, 112 Stat. 2681, _____ (October 21, 1998), *reprinted at* 144 Cong. Rec. H11240-42 (Oct. 19, 1998).

29. *Id.*

30. 64 Fed. Reg. 22750 (1999) (to be codified at 16 C.F.R. pt. 312).

31. *Id.* at 22753-58 (Proposed Rule §§ 312.4-312.6).

32. *Id.* at 22759-60 (Proposed Rule § 312.10).

33. The report is available at http://www.msb.edu/faculty/culnanm/gippshome.html [hereinafter "GIPPS Report"]. The following analysis is based upon the Commission's review of the GIPPS Report itself; Commission staff did not have access to the underlying GIPPS data.

34. GIPPS Report at 1; App. B at 4. The list, a ranking of servers by number of unique visitors for the month of January 1999, was compiled by Media Metrix, a site traffic measurement company. As larger sites are more likely to have multiple servers, the largest sites on the Web had a greater chance of being selected for inclusion in the sample drawn for this survey. *See* GIPPS Report, App. A at 1; App. B at 9 n.iii.

35. GIPPS Report, App. A at 3, 5.

36. GIPPS Report, App. A at 5.

37. The Commission's 1998 Comprehensive Sample was drawn at random from all U.S., ".com" sites in the Dun & Bradstreet Electronic Commerce Registry, with the exception of insurance industry sites. 1998 Report, App. A at 2. Unlike the Media Metrix list used in the GIPPS sample, the Dun & Bradstreet Registry does not rank sites on the basis of user traffic.

38. The GIPPS results show that thirty-six sites in the sample (or 10%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. GIPPS Report at 10. Thirty-two of these sites (or 8.9%) also posted contact information. *Id.* and App. A at 12. Professor Culnan also reports the number of sites posting disclosures for the four substantive fair information practice principles and for contact information in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (9.5%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (13.6%). GIPPS Report, App. A at 12 (Table 8C).

39. Online Privacy Alliance, *Privacy and the Top 100 Sites: A Report to the Federal Trade Commission* (1999) (available at http://www.msb.edu/faculty/culnanm/gippshome.html). The following analysis is based upon the Commission's review of the OPA Study report itself; Commission staff did not have access to the underlying OPA Study data.

40. OPA Study at 3, 5, and 8.

41. 1998 Report at 28.

42. Twenty-two sites in the OPA Study (or 22%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. OPA Study at 9-10 and App. A at 10 (Table 6C). Nineteen of these sites (or 19%) also posted contact information. *Id.* Professor Culnan also reports the number of sites posting disclosures for the four substantive fair information practice principles in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (22.2%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (23.7%). OPA Study, App. A at 10 (Table 6C).

43. The information included in this section is drawn from the OPA Web site (http://www.privacyalliance.org) and OPA members' testimony before the Senate Judiciary Committee's Hearing on *Privacy in the Digital Age: Discussion of Issues Surrounding the Internet* on April 21, 1999. The testimony is available on the OPA Web site, and at http://www.senate.gov/~judiciary/42199kb.htm.

44. The Guidelines are available at http://www.privacyalliance.org/resources/ppguidelines.shtml.

45. The information in this section is taken from materials posted on TRUSTe's Web site, http://www.truste.org, and from public statements by TRUSTe staff.

46. Several hundred additional companies have joined the TRUSTe program but are not yet fully licensed. *See* "*TRUSTe Testifies Before House Judiciary Committee*," May 27, 1999 (press release available at http://www.truste.org/about/about_committee.html).

47. Not all of TRUSTe's current licensees are subject to the latest version of the license agreement.

48. "Personally identifiable information" is defined as any information that can be used to identify, contact, or locate a person, including information that may be linked with identifiable information from other sources, or from which other personally identifiable information can easily be derived.

49. The information in this section is taken from materials posted on the BBB*Online* Web site, located at http://www.bbbonline.com, and from other public documents and statements by BBB*OnLine* staff.

50. The BBB*OnLine* Privacy Seal Program establishes requirements for notice, choice, access, and security. Comprehensive notice disclosures are required. Consumers must be allowed to prohibit unrelated uses of individually identifiable information not disclosed in the site's privacy policy and disclosure to third parties for marketing purposes. Consumers must also be permitted access to information about them to correct inaccuracies.

51. License fees to display the BBB*OnLine* Privacy logo are determined by a sliding scale according to the participant's revenues. Currently, the annual license fee ranges from $150 for companies with under $1 million in sales, to $3,000 for companies with sales over $2 billion.

52. "Individually identifiable information" is defined as information that (1) can be used to identify an individual, (2) is elicited by the company's Web site through active or passive means from the individual, and (3) is retrievable by the company in the ordinary course of business.

53. "Prospect information" would be collected when, for example, a visitor to a site orders a gift for another person and supplies that person's mailing address.

    It is not clear whether demographic information about a consumer that is collected at a site and tied to an identifier is covered by the BBB*Online* program, although licensees are required to provide notice if they merge or enhance individually identifiable information with data from third parties for the purposes of marketing products or services to the consumer.

54. Information about CPA WebTrust is available at http://www.cpawebtrust.org.

55. *Privacy in the Digital Age: Discussion of Issues Surrounding the Internet*, before the Senate Judiciary Comm., 106th Cong., April 21, 1999 (prepared statement of Gregory Fischbach).

56. Information regarding the ESRB privacy seal program is available at http://www.esrb.org.

57. The program guidelines include standards for notice and disclosure; choice; limiting data collection and retention; data integrity/security; data access; and enforcement and accountability.

SEPARATE STATEMENT OF COMMISSIONER ORSON SWINDLE

I have voted to submit "Self-Regulation and Privacy Online: A Report" (the "Report") to Congress, although I have done so with great reluctance. I have voted to submit the Report because we promised the Congress last summer that we would make a recommendation regarding the need for legislation addressing online privacy. *I also have voted to submit the Report because it ultimately reaches the correct and obvious conclusion:* ***no legislative action is necessary at this time.***

I must add, however, that I do not believe the Report accurately reflects reality. First, the dated and unfavorable results of the 1998 FTC Study are prominently described in the first seven pages of the Report, while the current and favorable results of the 1999 Georgetown survey are relegated to a brief discussion in the middle of the Report. Thus, the Report does not present a clear and complete picture of the substantial progress industry has made in the past year.

Second, the Report overemphasizes the failure of industry to sufficiently implement all elements of comprehensive "fair information practices." The Commission first articulated the elements of these four practices in detail just one year ago. Given the recent vintage of these elements, I believe industry has made substantial progress on them as well.

Third, the Report only sparingly mentions the leadership on privacy issues that IBM, Microsoft, Disney, AOL, The Direct Marketing Association, privacy seal organizations, and many others in the private sector have continuously demonstrated. Faint praises tend to be damning. Industry's leadership in achieving progress should be lauded not buried.

Because the Report provides an inaccurate assessment of the current state of online privacy and of the substantial progress attributable to industry self-regulation, it is perhaps not too surprising that the no legislative action recommendation appears at the very end of the Report, almost as if the recommendation is some trivial afterthought. The Report instead should have emphasized "front and center" that cooperative and creative efforts by a public-private partnership have achieved and will achieve progress far more quickly than more laws and regulations, which, while they may have a "feel good" quality to them, likely will have adverse unintended consequences.

In summary, I think significant progress has been made, but continued vigilance is needed because we are not where we want to be. The way to get where we want to be is not through more laws and regulation. Rather, industry, privacy and consumer advocates, and the Commission should be able to make further progress by continuing to work hard and work together. In the event that our joint efforts do not produce results, I would caution industry that there are many eager and willing to regulate. If industry wants to have the freedom to adopt privacy policies in response to market incentives and not government regulation, I encourage industry to continue to lead the way.

STATEMENT OF COMMISSIONER SHEILA F. ANTHONY
CONCURRING IN PART AND DISSENTING IN PART

I support the Commission's 1999 Report to Congress on Self-Regulation and Privacy ("Report"). The Report commends the seal programs and the few responsible industry leaders that have undertaken significant efforts to protect online privacy by adopting fair information practices in their online dealings with consumers. I agree with the Report's conclusions that industry leaders must continue to encourage widespread adoption of fair information practices; focus attention on the substance of web site information practices; and work together with government and consumer groups to educate consumers about privacy protection on the Internet. I also support the Commission's agenda to address the public's strong concern about online privacy.

I am dismayed, however, with the results of the two studies cited in the Report. According to the studies, there is an enormous gap between the online collection of individually identifiable information and the protection of that information by the web site owners' implementation of fair information practices of notice, consent, access, and security. While 93 to 99 percent of the surveyed sites collect personal information from consumers, only 10 to 20 percent of these sites have privacy disclosures implementing the four basic substantive fair information practices.[1] It is not hard to see why surveys show that the vast majority of Americans are concerned about threats to their privacy online.[2]

I disagree with the majority's opinion that "legislation to address online privacy is not appropriate at this time."[3] As a whole, industry progress has been far too slow since the Commission first began encouraging the adoption of voluntary fair information practices in 1996.[4] Notice, while an essential first step, is not enough if the privacy practices themselves are toothless. I believe that the time may be right for federal legislation to establish at least baseline minimum standards. I note that bipartisan bills are pending in both the House and the Senate and could provide a good starting point for crafting balanced protective legislation. I am concerned that the absence of effective privacy protections will undermine consumer confidence and hinder the advancement of electronic commerce and trade.

---

[1] *See* Report at 8 - 9.

[2] *See* Report at 2 - 3.

[3] *See* Report at 15.

[4] "Staff Report, Public Workshop on Consumer Privacy on the Global Information Infrastructure," (December 1996).

WWW.FTC.GOV