PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON "RECENT DEVELOPMENTS IN PRIVACY PROTECTIONS FOR CONSUMERS"

before the

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

of the

COMMITTEE ON COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

October 11, 2000

Mr. Chairman and members of the Subcommittee, I am Robert Pitofsky, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present an overview of the Commission's work over the past year in protecting consumers' privacy.[(1)]

I. INTRODUCTION AND BACKGROUND

As you know, the Federal Trade Commission is the federal government's primary consumer protection agency and our responsibilities are far-reaching. The Commission's legislative mandate is to enforce the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(2)] With the exception of certain industries, the FTCA provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce.[(3)] Pursuant to these responsibilities, the Commission has acquired considerable experience in addressing privacy issues in both the online and offline worlds,[(4)] and has long had particular interest in, and gained extensive experience dealing with, privacy and consumer protection issues.[(5)]

The Commission's interest and involvement in online privacy dates back to 1995. From that time forward, the Commission has held a series of public workshops on online privacy and related matters designed to educate itself and the public on the many issues involved. In addition, the Commission has been active on a number of privacy fronts. We have examined Web site practices in the collection, use, and transfer of consumers' personal information; encouraged and evaluated self-regulatory efforts and technological developments to enhance consumer privacy; developed consumer and business education materials; and have studied the role of government in protecting online information

privacy, including in particular, the online collection and use of information from and about children.[6] The Commission also has issued a series of reports to Congress regarding privacy online, including the topics of online profiling and the global aspects of Internet privacy.

II. COMMISSION INITIATIVES IN THE LAST YEAR

The past year has been a very busy one for the FTC in the area of consumer privacy.

Our efforts have included the following:

- surveying Web sites to examine their information practices and privacy statements;
- convening the Advisory Committee on Online Access and Security to study and provide recommendations pertaining to (a) consumers' access to their personal information; and (b) appropriate measures to protect the security of that information;
- issuing a report to Congress on online privacy;
- issuing a series of reports to Congress on third-party online profiling;
- issuing Rules implementing the Children's Online Privacy Protection Act (COPPA) and the Gramm-Leach-Bliley Act (GLBA);
- providing comments to other government agencies examining privacy issues; and
- bringing law enforcement actions against Web sites that violate the FTC Act.

What follows is a brief summary of our work in each of these areas.

A. 2000 Online Privacy Survey and Report to Congress

In its most recent report to Congress on online privacy, a majority of the Commission recommended legislation requiring consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online to comply with the four fair information practices: Notice, Choice, Access, and Security.[7] The Report analyzed the results of the Commission's survey of commercial Web sites' information practices, conducted in February and March 2000, and discussed the work of the Advisory Committee on Online Access and Security, which the Commission convened in December 1999.

The Advisory Committee on Online Access and Security, a group comprised of 40 e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates, provided advice and recommendations to the Commission regarding

the implementation of the fair information practice principles of Access and Security online. In a series of public meetings, the Advisory Committee discussed options, and the costs and benefits of each option, for implementation of these principles. The Advisory Committee submitted a final report to the Commission in May 2000 which highlighted the complexities of implementing Access and Security and, in light of the differing views of Committee members, developed several different options for providing Access and Security.[(8)]

The Commission's survey included two groups of sites drawn from a list of the busiest U.S. commercial sites on the World Wide Web: a census of 91 of the 100 busiest sites (the "Most Popular Group"), and a random sample of 335 sites that had at least 39,000 unique visitors per month (the "Random Sample").[(9)] The survey results showed that 88% of sites in the Random Sample and 100% of the sites in the Most Popular Group posted at least one privacy disclosure, and that 20% of Web sites in the Random Sample that collected personal identifying information, and 42% in the Most Popular Group, implemented, at least in part, all four fair information practice principles. The Commission also examined the data to determine whether Web sites were implementing Notice and Choice only. The data showed that 41% of sites in the Random Sample and 60% of sites in the Most Popular Group met the basic Notice and Choice standards.

Based on these results, as well as on the lack of a widely-adopted self-regulatory enforcement mechanism, a majority of the Commission recommended that Congress enact legislation to protect consumer privacy online. The proposed legislation would require Web sites to implement: (1) notice (providing clear and conspicuous notice of their information practices); (2) choice (offering consumers choices as to how their personal identifying information is used beyond the use for which the information was provided, including choice for both internal and external secondary uses of the information); (3) access (offering consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information); and (4) security (taking reasonable steps to protect the security of the information collected from consumers).[(10)]

B. Online Profiling Workshop and Reports to Congress

In November 1999, the Commission, together with the Department of Commerce, held a public workshop on "online profiling"[(11)] by third-party network advertisers, firms that place advertisements on Web sites. The workshop was designed to educate the public about this practice, as well as its privacy implications, and to examine current efforts by network advertisers to implement fair information practices. At the workshop, industry leaders announced the formation of the Network Advertising Initiative (NAI), an organization comprised of the leading Internet network advertisers, to develop a framework for self-regulation of the online profiling industry. Following the workshop, the NAI companies submitted drafts of self-regulatory principles for consideration by FTC and Department of Commerce staff. After lengthy discussions, a set of principles emerged that a majority of the Commission found to be a reasonable implementation of the fair information practice principles. The Commission discussed the NAI Principles in

Part 2 of its Report to Congress in July, 2000.[(12)]

Despite the NAI companies' commendable self-regulatory initiative, however, a majority of the Commission found that backstop legislation was still required to fully ensure that consumers' privacy is protected online. The majority reasoned that while NAI's current membership constitutes over 90% of the network advertising industry in terms of revenue and ads served, only legislation can compel the remaining 10% of the industry to comply with fair information practice principles. The majority believed that self-regulation also cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program. In addition, the majority found that there are unavoidable gaps in the network advertising companies' ability to require host Web sites to post notices about profiling, including Web sites that do not directly contract with the network advertisers, and stated that only legislation can guarantee that notice and choice are always provided in the place and at the time consumers need them. Accordingly, a majority of the Commission recommended legislation that would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites with respect to online profiling.

C. The Children's Online Privacy Protection Act

In its 1998 Report to Congress on online privacy, the Commission documented the widespread collection on the Internet of personal information from young children, and recommended that Congress enact legislation to protect this vulnerable group. In October 1998, Congress passed the Children's Online Privacy Protection Act of 1998 ("COPPA").[(13)] As required by the Act, on October 20, 1999, the Commission issued the *Children's Online Privacy Protection Rule,* which implements the Act's fair information practice standards for commercial Web sites directed to children under 13, or commercial sites that knowingly collect personal information from children under 13.[(14)] Violators of COPPA are subject to FTC law enforcement action, including civil penalties of $11,000 per violation.

There have been several press reports indicating that some Web sites directed to children have experienced difficulty in complying with COPPA, particularly in the context of children's chat rooms (online discussion groups). Staff believes that, to some extent, these concerns may have been caused by misunderstanding of the Rule's requirements or unfamiliarity with the exceptions built into the Rule. FTC staff is working hard to educate Web site operators on these issues; staff hosted a well-attended "compliance clinic" for operators in August, and has scheduled a second clinic on the West Coast in November.[(15)]

Some Web sites also have decided to discontinue children's chat rooms rather than to meet COPPA's requirements of either obtaining parental consent or monitoring chat rooms to prevent the disclosure of children's personal information. The operation of unmonitored children's chat rooms, which provide the opportunity for children to disclose personal information to third parties, has raised serious concerns about children's safety online. Those concerns contributed to the Commission's decision to recommend

that Congress enact legislation to protect children's privacy online.

In addition to the compliance clinic, the FTC has undertaken a number of initiatives designed to enhance compliance with the Rule. First, we have been active in monitoring compliance. FTC staff recently "surfed" a number of children's sites, and sent an email to those sites that seemed to have substantial compliance problems, alerting them to COPPA's requirements. Second, the Commission has begun a program of law enforcement against Rule violators. To date, we have filed suit against one Web site for COPPA violations, and we have a number of other investigations ongoing.[(16)]

Further, the FTC has undertaken a number of important and widespread educational initiatives to encourage compliance with COPPA's provisions. The Commission launched a special Web page at *www.ftc.gov/kidzprivacy* to help children, parents, and site operators understand COPPA and how it will affect them. Resources available on the Web site include guides for businesses and parents and "safe surfing" tips for kids. Staff has handled several hundred telephone and e-mail compliance inquiries since the Rule was issued in October of 1999, and has prepared a publication, entitled *COPPA FAQs*, to answer more than 50 of the most frequently asked questions about COPPA and the new Rule. FTC staff also is working with staff of the Department of Education to develop educational materials for schools about COPPA and online safety and has partnered with the private sector to help with outreach efforts.

D. The Gramm-Leach-Bliley Act

On November 12, 1999, President Clinton signed the Gramm-Leach-Bliley Act ("GLBA") into law.[(17)] Subtitle A of Title V of the GLBA ("Disclosure of Nonpublic Personal Information") requires a financial institution to disclose to all of its customers the institution's privacy policies and practices with respect to information it shares with both affiliates and nonaffiliated third parties and limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties. Specifically, it prohibits a financial institution from disclosing nonpublic personal information about consumers to nonaffiliated third parties unless the institution satisfies various disclosure and opt-out requirements and the consumer has not elected to opt out of the disclosure.

The GLBA's financial privacy provisions require the Commission, along with the federal banking agencies[(18)] and other federal regulatory authorities,[(19)] to prescribe such regulations as may be necessary to carry out the purposes of the financial privacy provisions of the GLBA. On May 24, 2000, the Commission published its GLBA Final Rule.[(20)] The Rule takes effect on November 13, 2000. In recognition of the range of financial institutions covered by the Rule and the extent of system-wide changes necessary for compliance, as well as concerns about consumer confusion, the Commission extended the deadline for full compliance by financial institutions and other persons under the Commission's jurisdiction from November 13, 2000, to July 1, 2001.[(21)]

The GLBA also obligates the Commission to promulgate a rule requiring financial institutions to safeguard their customer records and information. On September 7, 2000, the Commission issued a notice and request for comment pertaining to development of its Safeguards Rule in the Federal Register,[(22)] to garner public input concerning the safeguarding of consumer information by the wide range of financial institutions subject to the Commission's jurisdiction. After comments are received, the Commission will publish a Notice of Proposed Rulemaking, review comments received in response to that Notice, and issue a Final Rule.

E. Comments

The Commission has also shared its expertise in consumer privacy with other government agencies dealing with privacy issues through the submission of public comments. Recently, Commission staff submitted comments in response to the request for public comment by the Department of Justice, the Department of Treasury, and the Office of Management and Budget regarding their study of how a consumer's filing for bankruptcy relief affects the privacy of individual consumer information that becomes part of a bankruptcy case.[(23)] The staff comment focused on the privacy and identity theft[(24)] concerns raised by the collection and use of personal financial and other information in personal bankruptcy cases. The staff comment suggested that the agencies may wish to (a) consider the extent to which highly sensitive information must be included in public record data; (b) prohibit the commercial use by trustees of debtors' nonpublic data for purposes other than those for which the information was collected; and (c) evaluate the interplay between consumers' privacy interests and the Bankruptcy Code.[(25)]

Earlier this year, at the request of the Department of Health and Human Services ("HHS"), the Commission submitted comments on HHS' proposed Standards for Privacy of Individually Identifiable Health Information[(26)] (required by the Health Insurance Portability and Accountability Act of 1996).[(27)] The Commission strongly supported HHS' proposed "individual authorization" or "opt-in" approach to health providers' ancillary use of personally identifiable health information for purposes other than those for which the information was collected. The Commission also offered HHS suggestions it may wish to consider to improve disclosure requirements in two proposed forms that would be required by the regulations.[(28)]

F. Enforcement

The Commission has also brought three cases in the past year challenging deceptive or unfair conduct in connection with Web sites' posted privacy policies. In *FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000), the Commission settled charges that an online auction site allegedly obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business. In *FTC v. Sandra Rennert, et al.*, No. CV-S-00-0861-JBR (D. Nev. July 6, 2000), a group of individuals and Web sites involved in providing prescription drugs online collected consumers' personal medical information

through an online consultation form in addition to billing and shipping information. The Commission's complaint alleged that defendants misrepresented the security and encryption used to protect consumers' information and claimed that the defendants used the information in a manner contrary to their stated purpose.

In another recent matter, as noted earlier in note 15 *supra*, the Commission challenged a Web site's attempts to sell personal customer information gathered pursuant to a privacy policy that promised that such information would never be disclosed to a third party. *FTC v. Toysmart.com*, 00-CV-11341-RGS (D. Mass. filed July 10, 2000).[(29)]

In addition to these public enforcement actions, the Commission is currently conducting numerous nonpublic investigations of Web sites to determine if their privacy policies are deceptive or unfair.

III. CONCLUSION

The Commission is committed to the goal of ensuring privacy for consumers and will continue working to address the variety of privacy issues raised by our increasingly information-driven society. I would be pleased to answer any questions you may have.

1. My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any other Commissioner.

2. 15 U.S.C. § 45(a).

3. The Commission does not have criminal law enforcement authority. Further, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance, are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

4. The FTC Act and most other statutes enforced by the Commission apply equally in the offline and online worlds. *See, e.g., FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000) (discussed *infra*); *In re Trans Union*, Docket No. 9255 (Feb. 10, 2000), *appeal docketed*, No. 00-1141 (D.C. Cir. Apr. 4, 2000) (holding that defendants' sale of individual credit information to target marketers violated the Fair Credit Reporting Act).

5. In particular, the Commission has law enforcement responsibilities under the Fair Credit Reporting Act, which, among other things, limits disclosure of "consumer reports" by consumer reporting agencies, 15 U.S.C. §§ 1681 *et seq*., and under the Gramm-Leach-Bliley Act, which restricts the disclosure of consumers' personal financial information by certain financial institutions, 15 U.S.C. §§ 6801-6809 (Subtitle A).

6. *See, e.g., Online Profiling: A Report to Congress, Part 2 Recommendations* (July 2000); *Online Profiling: A Report to Congress* (June 2000); *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000) ("2000 Report"); *Self-Regulation and Privacy Online: A Report to Congress* (July 1999); *Privacy Online: A Report to Congress* (June 1998); *Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997); *FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996); *FTC Staff Report: Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

7. The Commission vote to issue the Report was 3-2, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part.

8. Available at http://www.ftc.gov/acoas/papers/finalreport.htm.

9. 2000 Report at Appendix A.

10. 2000 Report at 36-38. The proposed legislation would govern U.S. commercial Web sites to the extent not already covered by the Children's Online Privacy Protection Act, 15 U.S.C.§ 6501 *et seq.*

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

12. *See Online Profiling: A Report to Congress, Part 2* (July 2000). The Commission vote to issue Part 2 of the Report was 4-1, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part. Both Commissioner Swindle and Commissioner Leary commended NAI's self-regulatory program. A copy of the NAI principles is attached as an appendix to that report. The report is available at <http://www.ftc.gov/os/2000/07/onlineprofiling.htm> and the NAI principles are available at <http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf>. Among other things, the NAI Principles provide that consumers will receive notice of network advertisers' profiling activities on the Web site they are visiting (the so-called "host" or "publisher" Web site) as well as notice of their ability to choose not to participate in profiling. Where personally identifiable information is collected for profiling, a heightened level of notice, "robust" notice, will be required at the time and place such information is collected and before the personal data is entered. In addition, material changes in the information practices of a network advertising company cannot be applied to information collected prior to the changes, and previously collected non-personally identifiable data ("clickstream") cannot be linked to personally identifiable information without the affirmative (opt-in) consent of the consumer.

13. 15 U.S.C. §§ 6501 *et seq*. The Act requires that operators of Web sites directed to children under 13 or who knowingly collect personal information from children under 13 on the Internet: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

14. The rule became effective on April 21, 2000, 16 C.F.R. Part 312, and is available at <http://www.ftc.gov/opa/1999/9910/childfinal>.

15. The FTC's August compliance clinic was held at FTC headquarters and included presentations on privacy policies and parental notices, how to obtain verifiable parental consent, and safe harbor programs under the Rule. FTC staff focused in particular on how Web sites can take advantage of the Rule's exceptions for collection of an e-mail address to provide interactive content to children. The program also demonstrated ways in which sites can identify their younger visitors by asking age in a manner that minimizes their incentive to provide false information to gain entry to the site.

16. On July 21, 2000, the Commission filed an amended complaint with the U.S. District Court in Massachusetts alleging that Toysmart.com, an online toy retailer, collected personal information from children in violation of COPPA, and had offered to sell its customer list to the highest bidder

notwithstanding statements made in its privacy policy that it would never share customer information with a third party. As evidence of the COPPA violation, the Commission alleged that the site collected names, e-mail addresses, and ages of children under 13 through its Dinosaur Trivia Contest without notifying parents or obtaining parental consent. *FTC v. Toysmart.com*, 00-CV-11341-RGS (D. Mass. filed July 21, 2000).

17. Public Law 106-102, codified in part at 15 U.S.C. 6801 *et seq.*

18. Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and Secretary of the Treasury.

19. National Credit Union Administration (NCUA) and Securities and Exchange Commission (SEC).

20. 56 Fed. Reg. 33646. The Rule is codified at 16 CFR Part 313. The Federal banking agencies jointly published final regulations implementing the GLBA privacy provisions on June 1, 2000 (65 Fed. Reg. 35162). The NCUA and SEC published similar rules on May 18, 2000 (65 Fed. Reg. 31722) and June 29, 2000 (65 Fed. Reg. 40334), respectively.

21. Section 505(a)(7) of the GLBA provides that the Commission has jurisdiction over financial institutions not subject to regulation by either other federal agencies listed in footnotes 17 and 18 above or state insurance authorities. It also assigns the Commission authority to enforce the GLBA against "other persons" who receive protected consumer financial information covered by the GLBA. The broad scope of the Commission's jurisdiction is discussed in detail at the outset of the Federal Register notice (65 Fed. Reg 33646, 33647), which analyzes 16 CFR 313.1, the "Purpose and Scope" section of the Commission's rule.

22. 65 Fed. Reg. 54186. The comment period is now scheduled to close on October 24, 2000.

23. *See* Federal Register Notice Requesting Public Comment on Financial Privacy and Bankruptcy, 65 Fed. Reg. 46735 (July 31, 2000).

24. Identity theft is another privacy-related area in which the Commission has expertise. The Commission has implemented the Identity Theft and Assumption Deterrence Act of 1998, which directed the FTC to establish the federal government's centralized repository for identity theft complaints and victim assistance. For a description of the FTC's identity theft activities, *see* Statement of the Federal Trade Commission on Identity Theft, United States House of Representatives, Committee on Banking and Financial Services (Sept. 13, 2000) <http://www.ftc.gov/os/2000/09/idthefttest.htm>.

25. The staff comment is available at <http://www.ftc.gov/be/v000013.htm>.

26. 64 Fed. Reg. 59918 (November 3, 1999).

27. Pub. L. No. 104-191, 110 Stat. 1936 (August 21, 1996).

28. The Commission's comments are available at <http://www.ftc.gov/be/v000001.htm>.

29. These cases follow in the footsteps of two the Commission brought in 1999. In *Liberty Financial Companies, Inc.*, FTC Dkt. No. C-3891 (Aug. 12, 1999) the Commission challenged the allegedly false representations by the operator of a "Young Investors" Web site that information collected from children in an online survey would remain anonymous. In *GeoCities*, FTC Dkt. No. C-3849 (Feb. 12, 1999), the FTC settled charges that the Web site misrepresented the purpose for which it was collecting personal identifying information from children and adults.