PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON

"CONSUMER PRIVACY ON THE WORLD WIDE WEB"

Before the
SUBCOMMITTEE ON TELECOMMUNICATIONS,
TRADE AND CONSUMER PROTECTION
of the
HOUSE COMMITTEE ON COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.
July 21, 1998

Mr. Chairman, I am Robert Pitofsky, Chairman of the Federal Trade Commission. I appreciate this opportunity to present the Commission's recommendations for addressing the privacy concerns raised by the wide-spread collection of personal information from consumers by commercial sites on the World Wide Web.[(1)]

I. Introduction and Background

A. FTC Law Enforcement Authority

The Commission's mission is to promote the efficient functioning of the marketplace. It does so by seeking to protect consumers from unfair or deceptive acts or practices and by promoting vigorous competition. As you know, the Commission's responsibilities are far-reaching. Its primary legislative mandate is to enforce the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(2)] With the exception of certain industries, this statute provides the Commission with broad law enforcement authority over virtually every sector of our economy.[(3)] Commerce on the Internet falls within the scope of this statutory mandate.

B. The Commission's Role in Online Privacy

The Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace and has held a series of workshops and hearings on such issues. Throughout, 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 to encourage self-regulation have included bringing industry and consumer and privacy advocates together to address online privacy issues at our workshops, and meeting with, and encouraging, industry leaders to adopt effective self-regulatory programs. These efforts have been based on (1) the understanding that personal information can be collected and

widely disseminated on the Web with unprecedented ease, and (2) the belief that greater protection of personal privacy on the Web will not only protect consumers, but also increase consumer confidence and ultimately their participation in the online marketplace.

In June, the Commission issued a comprehensive report on Internet privacy, *Privacy Online: A Report to Congress* (the "Report").[(4)] The Report sets forth widely accepted fair information practices; reports on the Commission's extensive survey of some 1400 Web sites' information practices; and assesses the effectiveness of self-regulatory efforts to date in protecting consumer privacy. The Report concludes that an effective self-regulatory system has yet to emerge and that additional incentives are required in order to ensure that self-regulation is effective and consumer privacy is protected. The Report also includes a recommendation that Congress adopt legislation that would set forth standards for the online collection of information from children. Today the Commission presents a legislative model that would address the recommended standards pertaining to children, and the broader issue of consumer privacy online.

C. The Online Marketplace

The advent of the Internet --- with its new methods of communicating through Web sites, electronic mail, news groups, chat rooms, electronic bulletin boards, and commercial online services --- is an historical development much like the introduction of television or, a few generations earlier, the telephone. Like these earlier technologies, the Internet presents consumers with extraordinary new means to purchase both innovative and traditional goods and services, to communicate more effectively, and to tap into rich sources of information that previously were difficult to access and that now can be used to make better-informed decisions. According to recent survey evidence, 76 million American adults use the Internet.[(5)] This figure represents a marked increase from figures reported in recent years.[(6)]

Children also represent a large and rapidly growing segment of online consumers.[(7)] Almost 10 million (14%) of America's 69 million children are now online, with over 4 million accessing the Internet from school and 5.7 million from home.[(8)] Children are also avid consumers and represent a large and powerful segment of the marketplace.[(9)] Their growing presence online, therefore, creates enormous opportunities for marketers to promote their products and services to an eager audience.[(10)]

1. Collection of Information Online

This unique, new medium is also very valuable to merchants because it is used to collect vast amounts of personal information about consumers. Commercial sites on the World Wide Web (the "Web") collect personal information explicitly through a variety of means, including registration pages, user surveys, online contests, application forms, and order forms. Web sites also collect personal information through means that are not obvious to consumers, such as using electronic means (*e.g.*, cookies) to track which pages a consumer views and for how long.[(11)] As a result, merchants can effectively follow consumers around their "virtual stores" as consumers do their shopping. In the Commission's recent survey of

some 1400 Web sites, the Commission found that the vast majority of sites collect personal information from consumers -- 92% in the sample representing all U.S.-based commercial sites likely to be of interest to consumers.[(12)] In addition, we found that a wide variety of detailed personal information is being collected online from and about children, often without actual notice to, or an opportunity for control by, parents. In our survey, 89% of the 212 children's sites surveyed collect personal information from children, but only 1% obtain parental permission prior to collecting such information.[(13)]

Here are a few examples of the kinds of information collection practices Commission staff discovered in the survey:

> A medical clinic's online doctor-referral service invites consumers to submit their name, postal address, e-mail address, insurance company, any comments concerning their medical problems, and to indicate whether they wish to receive information on any of a number of topics, including urinary incontinence, hypertension, cholesterol, prostate cancer, and diabetes. The online application for the clinic's health education membership program asks consumers to submit their name, address, telephone number, date of birth, marital status, gender, insurance company, and the date and location of their last hospitalization.
>
> An automobile dealership's Web site offers help to consumers in rebuilding their credit ratings. To take advantage of this offer, consumers are urged to provide their name, address, Social Security number, and telephone number through the Web site's online information form.
>
> A mortgage company operates an online prequalification service for home loans. The online application form requires that each potential borrower provide his or her name, Social Security number, home and business telephone numbers, e-mail address, previous address, type of loan sought, current and former employer's name and address, length of employment, income, sources of funds to be applied toward closing, and approximate total in savings. The online form also requires the borrower to provide information about his or her credit history, including credit card, car loans, child support and other indebtedness, and to state whether he or she has ever filed for bankruptcy.
>
> A child-directed site collects personal information, such as a child's full name, postal address, e-mail address, gender, and age. The Web site also asks a child extensive personal finance questions, such as whether a child has received gifts in the form of stocks, cash, savings bonds, mutual funds, or certificates of deposit; who has given a child these gifts; whether a child puts monetary gifts into mutual funds, stocks or bonds; and whether a child's parents own mutual funds. Elsewhere on the Web site, contest winners' full names, age, city, state, and zip code are posted.
>
> Another child-directed site collects personal information to register for a chat room, including a child's full name, e-mail address, city, state, gender, age, and hobbies.

> The Web site has a lotto contest that asks for a child's full name and e-mail address. Lotto contest winners' full names are posted on the site. For children who wish to find an electronic pen pal, the site offers a bulletin board service that posts messages, including children's e-mail addresses. While the Web site says it asks *children* to post messages if they are looking for a pen pal, in fact anyone of any age can visit this bulletin board and contact a child directly.[(14)]

None of these Web sites posted a privacy policy.

2. Consumer Concerns About Online Privacy

Consumers are concerned about this collection of personal data, which in turn appears to be affecting their participation in the online marketplace. While recent survey research indicates that 76 million Americans use the Internet, less than a quarter of this group, or 17.5 million people, have purchased products, services, or information online.[(15)] According to the results of a March 1998 *Business Week* survey, consumers not currently using the Internet ranked concerns about the privacy of their personal information and communications as the top reason they have stayed off the Internet.[(16)] A substantial number of online consumers would rather forego information or products available through the Web than provide a Web site personal information without knowing what the site's information practices are.[(17)] Interestingly, while 61% of all Internet users have not seen any notices describing how Web sites use personal information, 59% of those who have purchased a product or service online have seen such privacy notices, suggesting there may be a correlation between seeing such a notice and a willingness to buy products or services online.[(18)]

Consumers are even more concerned about the collection of personal information from children. These practices raise especially troubling privacy and safety concerns because of the particular vulnerability of children, the immediacy and ease with which information can be collected from them, and the ability of the online medium to circumvent the traditional gatekeeping role of the parent. Indeed, consumers strongly favor limiting the collection and use of personal information from children online. A recent survey showed that 97% of parents whose children use the Internet believe Web sites should not sell or rent personal information relating to children, and 72% object to a Web site's requesting a child's name and address when the child registers at the site, even if such information is used only internally.[(19)]

In sum, it is clear that consumers care deeply about the privacy and security of their own, and their children's, personal information in the online environment and are looking for greater protections. Until meaningful and effective consumer privacy protections are implemented in the online marketplace, consumers may remain wary of engaging in electronic commerce, and this new marketplace will fail to reach its full potential.[(20)]

3. Industry Self-Regulation to Protect Privacy

For the past several years, the Commission has encouraged industry to address consumer

concerns regarding online privacy through self-regulation. The Commission believes that self-regulation is preferred to a detailed legislative mandate because of the rapidly evolving nature of the Internet and computer technology. The Commission also recognizes that a private-sector response to consumer concerns that incorporates the widely-accepted fair information practices discussed in the Report and provides for effective enforcement mechanisms could afford consumers adequate privacy protection.

However, despite the Commission's considerable efforts to encourage and facilitate an effective self-regulatory system, we have not yet seen one emerge.[(21)] Our March 1998 survey of commercial Web sites and assessment of industry self-regulatory efforts revealed that, at the time of the survey, the state of self-regulation was inadequate and disappointing. Our survey found that the vast majority of Web sites fail to provide even the most basic privacy protection -- notice of what information they collect and what they do with that information. Few of the sites surveyed -- only 14% in the Commission's random sample of commercial Web sites -- provide any notice with respect to their information practices, and fewer still -- approximately 2% -- provide notice by means of a comprehensive privacy policy.

The information practices of the sites designed for children were also disappointing. While 54% of children's sites surveyed provide some form of disclosure of their information practices, few sites take any steps to provide for meaningful parental involvement in the process. Only 23% of sites even tell children to seek parental permission before providing personal information, fewer still (7%) say they will notify parents of their information practices, and less than 10% provide for parental control over the collection and/or use of information from children. For example, neither of the children's sites described earlier provided for parental notice or control.

Recently, there have been some encouraging signs that the private sector is attempting to address consumer concerns about online privacy. Within the last month, a number of industry leaders have taken steps to develop self-regulatory programs.[(22)] While the Commission is hopeful that self-regulation will achieve adequate online privacy protections for consumers, we recognize that there are considerable barriers to be surmounted for self-regulation to work. For such programs to be meaningful, an effective enforcement mechanism is crucial. Moreover, it will be difficult for self-regulatory programs to govern all or even most commercial Web sites. While some industry players may form and join self-regulatory programs, many may not. This would result in a lack of the uniform privacy protections that the Commission believes are necessary to allow electronic commerce to flourish.

Accordingly, the Commission believes that, unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional governmental authority in this area would be appropriate and necessary.[(23)] The Commission offers the following as a legislative model for consideration by the Congress. We believe that this model would bolster ongoing self-regulatory initiatives, encourage others to undertake such initiatives, and provide statutory standards

that would govern businesses that do not participate in self-regulatory programs.

II. Legislation

The proposed legislative model would set forth a basic level of privacy protection for all consumers visiting U.S. consumer-oriented commercial Web sites. Furthermore, as an incentive for continued industry participation in structuring privacy guidelines, the legislation would provide a safe harbor for industries that choose to establish their own means of providing consumers privacy protections, as long as those means are subject to governmental approval.[(24)] The agency responsible for approving such guidelines and enforcing this legislation (the "implementing agency") would be given rule-making authority under the Administrative Procedure Act.[(26)] Such authority would allow the implementing agency to promulgate both procedural mechanisms for approval of industry guidelines and substantive, sector-specific definitions of fair information practices based on general statutory guidance. The Commission's prior recommendations with respect to children's online privacy would fit within this framework and form the substantive rules governing the online collection of information from children. The basic structure of this legislative model is described in greater detail below.

A. Statutory Standards

Pursuant to the proposed model, federal privacy legislation would set out the basic standards of practice governing the collection of information online, as well as provide the implementing agency with the authority to enforce compliance with those standards. All 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 set forth in the Report. The four basic information practices required by the statute would be as follows:

> (1) notice/awareness -- Web sites would be required to provide consumers notice of their information practices, *i.e.*, what information they collect and how they use it;
>
> (2) choice/consent -- Web sites would be required to offer consumers choices as to how that information is used beyond the use for which the information was provided (*e.g.*, to consummate a transaction);
>
> (3) access/participation -- Web sites would be required to offer consumers reasonable access to that information and an opportunity to correct inaccuracies; and
>
> (4) security/integrity -- Web sites would be required to take reasonable steps to protect the security and integrity of that information.

The implementation of these practices will vary by industry and with technological developments. For this reason, the Commission recommends that any legislation be phrased in general terms and be technologically neutral. The definitions of fair information

practices set forth in the statute should be broad enough to allow for flexibility in interpretation, in light of both reasonable consumer expectations and industry practices. Sites that collect personal identifying information from children should be subject to the additional statutory standards recommended by the Commission in its June 1998 Report.

The recommended standards pertaining to children would empower parents to make choices about when and how their children's information is collected and used on the Web. They would require commercial Web sites that collect personal identifying information from children 12 and under to provide actual notice to the parent and obtain parental consent as follows.

> (1) Where the personal identifying information would enable someone to contact a child offline or where the personal identifying information is publicly posted or disclosed to third parties, the site would be required to obtain prior parental consent (opt-in).
>
> (2) Where collection of an e-mail address is necessary for a child's participation at a site, such as to notify contest winners, and is not posted or disclosed to third parties, the site would be required to provide notice to parents and an opportunity to remove the e-mail address from the site's database (opt-out).

Where the personal identifying information is collected from children over 12, Web sites would be required to provide parents with notice of the collection of such information and an opportunity to remove the information from the site's database (opt-out).[(27)]

B. Safe Harbor

To encourage industry participation in the process and to ensure that fair information practices are implemented in a manner that is sensitive to both industry-specific concerns and technological developments, the legislative model provides that compliance with agency-certified industry guidelines would provide a safe harbor from any enforcement actions under the new statute, though not from compliance with other federal statutes, including the FTC Act's prohibition on unfair or deceptive trade practices.[(28)] In order to qualify for safe harbor protection, industry guidelines would be required to meet the basic standards of privacy protection described above.[(29)] In order to avoid any Constitutional prohibitions on delegation of government powers, and to ensure the new statute's basic requirements are met, the Commission recommends that the implementing agency be given the authority to review and certify industry guidelines as meeting the statute's standards, after public notice and comment.[(30)] Once guidelines were certified, any qualifying entity adhering to the guidelines would be deemed to be in compliance with the new law's requirements as well.[(31)]

In certifying agency guidelines pursuant to the legislative model, the implementing agency would consider the costs[(32)] and benefits, within industry-specific contexts, of implementing the core fair information practices.[(33)] For example, consumers may have varying needs, depending on the nature or sensitivity of the information collected, for

access to their information.

Industry also would be required to include compliance assurance mechanisms, enforcement mechanisms and/or provide for external compliance reviews in guidelines submitted for certification.[(34)] Such steps would enhance compliance with any certified guidelines while limiting the demands on governmental enforcement resources.

C. Rule-making

As part of the proposed legislative model, the implementing agency would be directed to undertake a rule-making under the Administrative Procedure Act. This direction would serve two important purposes. First, the agency would be authorized to issue interpretive rules defining fair information practices with greater specificity, taking into account industry-specific differences.[(35)] For example, the agency could expand on what constitutes adequate notice of a Web site's information practices, or adequate access, under various circumstances. Such interpretive rules would provide guidance for any industry seeking to qualify for safe-harbor certification as well as for any businesses that elect not to participate in an existing safe harbor program. In either event, this aspect of the rule-making authority would allow the implementing agency to apply the basic legislative prescriptions in a more refined, industry-specific manner after soliciting public comment. Second, the agency would be authorized to develop procedures to govern the approval of industry guidelines as a safe harbor from enforcement.

III. Conclusion

The Commission is committed to the goal of assuring fair information practices for consumers online, and looks forward to working with the Committee as it considers the Commission's Report and proposals for protecting online privacy.

---

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). The Commission also has responsibilities under approximately 40 additional statutes, *e.g.*, the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*., which establishes important privacy protections for consumers' sensitive financial information; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq*., which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et. seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 30 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

3. 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. A copy of the Report is attached as Appendix A. The Report is also available on the Commission's Web site at www.ftc.gov/reports/privacy3/index.htm.

5. Louis Harris and Associates, Inc. and Dr. Alan F. Westin, *E-Commerce & Privacy: What Net Users Want* at vi (June 1998) [hereinafter *E-Commerce & Privacy*].

6. For example, other studies show that in early 1997, approximately 51 million adults were online in the United States and Canada. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Spring '97 (March 12, 1997), reported at http://www.commerce.net/work/pilot/nielsen_96/press_97.html. By December 1997 that number had grown to 58 million adults. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Fall '97 (December 11, 1997), reported at http://www.commerce.net/news/press/121197.html.

7. Children use the Web for a wide variety of activities, including homework, informal learning, browsing, playing games, corresponding with electronic pen pals by e-mail, placing messages on electronic bulletin boards, and participating in chat rooms. *See Interactive Consumers Research Report*, Vol. 4, No. 5 at 1, 4, May 1997 (discussing results of FIND/SVP's 1997 American Internet User Survey).

8. *Id*. at 1, 2. The number of children online increased nearly five-fold from fall 1995 to spring 1997. *Id.* at 1.

9. Children are estimated to spend billions of dollars a year, and to influence the expenditure of billions more. For example, one source has estimated that, in 1997, children aged 4 through 12 spent $24.4 billion themselves; and children aged 2 through 14 may have directly influenced spending by their parents in an amount as much as $188 billion. James U. McNeal, *Tapping the Three Kids' Markets*, American Demographics, Apr. 1998, at 38, 40.

10. According to one source, most children's Web sites are targeting children ages 8 to 11. Teens tend to visit the same sites that adults visit. Robin Raskin, *What do Kids Want?*, Family PC Magazine, May 1998, at 17.

11. The Commission's survey did not track such methods of information collection.

12. Report at 23.

13. Report at 31.

14. Report at 39-40.

15. *E-Commerce & Privacy* at 2. Nevertheless, analysts estimate that Internet advertising -- which totaled approximately $301 million in 1996 -- will increase to $4.35 billion by the year 2000. Jupiter Communications, *1998 Online Advertising Report* (Aug. 22, 1997) (figure includes directory listings and classified advertisements.)

16. *Business Week/Harris Poll: Online Insecurity*, Business Week, March 16, 1998, at 102.

17. Louis Harris and Associates, Inc. and Dr. Alan F. Westin, *Commerce, Communications, and Privacy Online, A National Survey of Computer Users* at 20-21 (1997).

18. *E-Commerce & Privacy* at viii.

19. Federal Trade Commission, Public Workshop on Consumer Information Privacy, June 10-13, 1997, Transcript at 156 (testimony of Alan Westin, discussing *Commerce, Communications, and Privacy Online, A National Survey of Computer Users,* 1997).

20. The Commission recognizes that the widespread availability of consumers' personal information, and the privacy concerns raised thereby, are not unique to the Internet. The Commission has focused on online privacy for several reasons. First, interactive media make it possible to collect, store, and disseminate personal information with speed and efficiency that are unmatched in other contexts. For example, browsing an online bookstore allows a Web site to record not only a consumer's final purchase, as an offline bookstore could do if payment is made with a credit card, but also a consumer's browsing habits, including which books and topics appear to be of greatest interest. Second, the fact that the online marketplace is in its infancy makes it possible to address online privacy issues prospectively. Finally, and most important, consumers' concerns about their privacy are significantly heightened in the online environment.

21. The Commission has seen industries develop effective self-regulatory programs in other instances, such as the advertising industry's National Advertising Review Council.

22. Two prominent self-regulatory programs have been announced. The Online Privacy Alliance, a group of thirty-nine corporations and twelve associations, has adopted a set of guidelines for online privacy policies and is currently developing enforcement mechanisms. *See* http://www.privacyalliance.org. The Council of Better Business Bureaus, Inc. has announced a plan to develop, through its BBBOnline program, a quality assurance seal that would indicate a Web site's adherence to some or all of the fair information practices discussed in the Report.

23. Currently, the Commission has limited authority to prevent abusive practices in this area. The Federal Trade Commission Act (the "FTC Act"), 15 U.S.C. §§ 41 *et seq.*, grants the Commission authority to seek relief for violations of the Act's prohibitions on unfair and deceptive practices in and affecting commerce, an authority limited in this context to ensuring that Web sites follow their stated information practices.

24. This legislative model has some structural similarities to legislation recently proposed by Subcommittee Chairman Tauzin (R-La.) and Representative Paul Gillmor (R-Oh)[(25)]

25. See Data Privacy Act of 1997, H.R. 2368, 105th Cong. (1997). - ' §

26. 5 U.S.C. § 553.

27. Parental notice raises some implementation issues. In those instances where parents and children have separate e-mail addresses, notice may be provided to parents electronically. Where parental consent is required, sites can simply direct children to download (print) the notice and consent form and have the parent return the signed form by regular mail or facsimile. The details governing implementation of parental notice are a prime example of the types of issues to be addressed in the safe harbor certification and rulemaking processes described below.

28. The implementing agency that enforces the new privacy statute would have the burden of proving non-compliance with the new law's requirements. The standards enunciated in the legislation thus would remain the benchmark against which industry's conduct would ultimately be judged. Compliance with certified guidelines, however, would serve as a safe harbor in any enforcement action under the new law. Nevertheless, the implementing agency would retain discretion to pursue enforcement under the statute if certification were obtained based on incomplete or inaccurate factual representations or if there were a substantial change in circumstances. The implementing agency will need substantial additional resources.

29. Technological standards and specifications could also qualify for safe harbor certification, to the extent they comport to the statute's requirements and operate as described. Thus, for example, technology allowing for seamless, electronic provision of notice and choice may qualify for safe harbor certification under certain circumstances.

30. A public notice and comment period would allow consumer organizations and privacy experts to contribute to the crafting of the safe harbors and ensure that small businesses' views are heard. Moreover, because certified privacy policies would be publicly available, businesses that choose not to belong to associations could inform themselves about what practices must be implemented for safe harbor protection.

31. Because application of the new law's requirements would vary by industry, guidelines would have to define the nature of businesses to which they apply. Only businesses meeting the guidelines' definition of applicable businesses would be entitled to safe harbor protection for compliance with the guidelines.

Industry would be free to revise guidelines in light of changes in technology, consumer expectations, and industry practice. Revised guidelines would be subject to the same certification process. Changes in technology and the marketplace may also call for the implementing agency to revisit guidelines after they have been approved.

32. It is likely that many of the costs of implementation of industry guidelines will be reduced as new technologies develop. Moreover, the costs of compliance to new and small businesses should be low, especially if such businesses use personal information only for the purpose of processing orders and do not maintain detailed consumer databases. Posting a privacy policy on such business' Web sites and taking basic security precautions are relatively inexpensive and should meet the statute's requirements in such circumstances. In fact, the Direct Marketing Association ("DMA") has demonstrated that it is possible to automate the creation of privacy policies. Visitors to the DMA Web Site (http://www.the-dma.org) can create their own privacy policy online at no charge.

33. Any possible anticompetitive misuse of industry self-regulation would, of course, also be considered by the implementing agency.

34. Such measures could include, for example, requiring adherence to trade association guidelines as a condition of membership; requiring independent third-party audits, as the Individual Reference Services Group has done; or providing for a referral process to federal law enforcement agencies, such as the Children's Advertising Review Unit and the National Advertising Division have done.

35. *See, e.g.*, The Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6102(a)(2) (providing that Commission shall prescribe rules defining deceptive telemarketing acts or practices); *see also* 16 C.F.R. Part 310 (defining such practices).