UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

July 31, 1997

The Honorable John McCain
Chairman
Committee on Commerce, Science and Transportation
United States Senate
SD-508 Dirksen Senate Office Building
Washington, D.C. 20510-6125

Dear Mr. Chairman:

This letter responds to your letter dated July 30, 1997 requesting that the Commission provide Congress with a preliminary assessment of the Public Workshop on Consumer Privacy held on June 10-13, 1997. The Workshop addressed four major topics: computerized databases containing identifying information about consumers; unsolicited commercial e-mail; consumers' online privacy; and children's privacy in the online environment. The Workshop presentations and the extensive written commentary submitted in connection with the Workshop form a rich public record with which to examine these subjects. We welcome this opportunity to provide our preliminary findings from the Workshop and to outline some of the steps the Commission intends to undertake in the next twelve months to address consumer privacy issues.[1]

Computerized Databases

In light of widespread concern and Congressional interest, the Commission previously agreed to conduct a study of the collection, compilation, sale, and use of computerized databases that contain what consumers may perceive to be sensitive identifying information, often referred to as "look-up services," "locators," or "individual reference services." The Workshop, as well as the comments which have been and continue to be filed, will aid us in completing this ongoing study. At the Workshop, database operators, information vendors and other participants identified the types and sources of information contained in these databases. A wide variety of personal information, including social security numbers, dates of birth, unlisted phone numbers, prior addresses, and the names and ages of household members, is being collected and stored in databases. In some cases, this data is made instantly available to anyone with access to the Internet.

---

[1] The public record for the unsolicited commercial e-mail and online privacy sessions of the Workshop closed on July 14, 1997. The public record for the session on computerized databases remains open. The transcript of the Workshop and all commentary submitted has been posted on the Commission's Web page (www.ftc.gov).

Workshop participants discussed the benefits and risks associated with look-up services. Database users demonstrated the crucial role that these databases play in furthering important objectives, such as tracking down criminals, preventing fraud, finding witnesses, preparing news reports, and locating missing children. Privacy and consumer advocates expressed concerns about the privacy implications of the databases and warned of potential harm that could result from inaccurate or insecure data, as well as from the misuse of the data for criminal ends, including identity theft.

We are encouraged that the industry has stepped forward to address the serious privacy concerns raised by these databases. Key industry members came together and offered a preliminary self-regulatory proposal to limit the availability of sensitive information, to ensure the accuracy and security of this information, and to educate consumers about their practices.

Workshop participants and Commission staff have identified a number of key issues to address in the Commission's study of computerized databases. These issues include: preventing misuse of personal information; providing consumers with sufficient access to their own information to correct inaccuracies; avoiding undue chilling of the free flow of information for legitimate purposes; assessing the effectiveness of self-regulatory guidelines and enforcement mechanisms; and examining the extent to which government action, if any, may be needed.

The Commission anticipates submitting a report on the database study to the Congress by the close of 1997. We plan to continue our dialogue with industry members to help improve and broaden the reach of their self-regulatory effort.

Unsolicited Commercial E-mail

Survey research presented at the Workshop demonstrates that unsolicited commercial e-mail is strongly disfavored by almost all consumers who receive it. It imposes considerable costs (in time and money) on individual recipients and their online or Internet service providers, and the large volume of bulk e-mail solicitations burdens the infrastructure of the Internet itself. These costs are likely to escalate as e-mail solicitations become interactive and incorporate video and audio messages that further consume the Internet's capacity and use more space on recipients' computers. Furthermore, an increasing segment of unsolicited commercial e-mail involves seemingly fraudulent offering of products or services, such as get-rich-quick schemes that we commonly see in our telemarketing fraud program. In addition, in what appears to be unique to this form of direct marketing, unsolicited e-mail often involves the use of false return addresses and forged header information, practices which may also be deceptive within the meaning of Section 5 of the Federal Trade Commission Act.

We recognize, however, that interactive technology provides a unique and potentially lucrative marketing medium. It is an extremely inexpensive way for small businesses and

entrepreneurs to reach a broad audience. E-mail also holds out the promise of one-to-one marketing of bona fide products and services to consumers who truly wish to receive solicitations in this manner. Workshop participants discussed various ways to identify those consumers. For the most part, industry groups favor providing consumers with the opportunity to have their e-mail addresses removed from lists created for the purpose of sending unsolicited commercial e-mail. Another approach which some individual online marketers have found successful is the use of lists which include only individuals who have affirmatively asked to receive e-mail solicitations.

The Workshop provided both proponents and opponents of the practice of sending unsolicited commercial e-mail with the opportunity to come to one table. We are encouraged that a disparate group, including senders of unsolicited commercial e-mail, technology experts, and privacy advocates, has committed to develop a voluntary response to consumer and industry concerns and to report back to the Commission in 6 months. Staff will monitor this self-regulatory effort. In addition, staff will continue to monitor unsolicited commercial e-mail for possible violations of Section 5 of the Federal Trade Commission Act, and the Commission will bring enforcement actions, as appropriate, against senders who engage in fraudulent or deceptive practices.

Consumer Online Privacy

The Workshop demonstrated that many consumers care deeply about the security and confidentiality of their personal information in the online environment. Consumer survey research presented at the Workshop indicates they are looking for greater protections, preferably from voluntary efforts by industry, but if necessary from government. Currently a handful of commercial sites on the World Wide Web disclose how they collect and use consumer information online and offer consumers an opportunity to exercise choice as to whether and how their information should be used. Members of the online industry are aware of the need to address consumers' concerns, and have begun to respond with self-regulatory measures.

We are delighted with the high level of interest in our efforts shown by the industry leaders who submitted commentary and chose to participate in the Workshop. Industry groups demonstrated varying approaches to protecting online privacy. Some key trade associations have well-developed policies and procedures; others are in the initial stages of policy formation; still others remain uncertain as to whether industry-wide policies, as opposed to individual company efforts, are necessary. Even when a Web site has a policy, its effectiveness depends on whether the policy is easily communicated to consumers.

The McGraw-Hill Companies, a Workshop participant whose corporate divisions sponsor sixty Web sites, is implementing a privacy policy that is one model for companies committed to protecting consumer privacy online. This policy requires: (1) that consumers be notified of the collection and intended uses of their personally identifiable information; (2) that consumers be offered the opportunity to refuse permission for distribution of their personally identifiable

information to third parties; (3) that security measures be implemented to protect the integrity and privacy of this information; (4) that consumers have access to this information and a mechanism to correct it; and (5) that measures be implemented to ensure that only authorized third parties use this information, and only for authorized purposes. The policy prohibits the distribution outside the company of "sensitive" personally-identifiable information, including medical and financial data, as well as most information about children. Consumers will also be given the ability to prevent this sensitive information from being shared even among the company's subdivisions.

The Workshop also highlighted a variety of other self-regulatory endeavors. A proprietary system requiring disclosure of member Web sites' basic information practices and third-party auditing of those practices has been launched, but has not yet been widely implemented. Its efficacy as a privacy protection will depend upon widespread industry participation. Particularly promising are efforts to create interactive technology that permits consumers to automate their preferences, and Web sites to communicate their practices, regarding the collection and use of personal information online. These technological tools, which may well provide adequate privacy protection, are in the initial stages of development. They will play a critical role in any comprehensive self-regulatory solution to online privacy concerns.

Self-regulatory approaches and emerging technological tools will be effective in protecting online privacy only to the extent that they are widely adopted by Web sites and, in the case of technology, are readily available to consumers and easy to use. Consumer and business education projects will be critical to the success of these efforts, and the Commission will assist industry and consumer groups in those endeavors.

Commission staff will monitor the World Wide Web, just as it monitors national advertising, to determine the extent to which commercial Web sites are disclosing their information practices and offering consumers choice regarding the collection and use of their personal information online. We will report our findings to Congress on or before June 1, 1998. Our recommendations, if any, will take into account whether the initial efforts demonstrated at the Workshop are translated into broader industry progress toward effective self-regulation.[2]

---

[2] We hope to find by March 1, 1998, that a substantial majority of commercial Web sites are clearly posting their information practices and privacy policies. Commission staff will also be looking to see whether Web sites are honoring consumers' privacy preferences.

Children's Online Privacy

The final focus of the Workshop was the special problems posed by the collection of information from children who use the Internet. The presentations provided valuable information regarding (1) parents' attitudes and perceptions on online information collection from children; (2) Web sites' information collection practices and policies; (3) industry initiatives; and (4) possible technological responses to address children's privacy concerns.

Consumer survey data presented at the Workshop showed that consumers generally, and particularly parents, are extremely concerned about the collection of personally-identifiable information from children. Parents are virtually unanimous (97%) in their belief that Web sites should not collect personal information from children, and sell or rent that information to others. Similarly, 72% of parents object to a Web site's asking children to provide their names and addresses when they register, even when the site uses this information only within the company; 64% object to a Web site's asking children to provide their e-mail names to gather statistics on how many children visit the site and what they do there. In addition, anecdotal evidence indicates that as many as one third of children surfing the Internet claim to have experienced problems, such as attempted password theft and inappropriate advances by adults in children's chat rooms. Information presented at the Workshop indicates that numerous Web sites are collecting a variety of personal information from children without providing effective notice to parents, although there was less information about how and in what form the data is used once collected.

Special concern was voiced at the Workshop about online activities that enable children to post or disclose their names, street addresses, or e-mail addresses in areas accessible to the public, such as chat rooms, bulletin boards, and electronic pen pal programs, creating a serious risk that the information may fall into the wrong hands. In fact, the FBI and Justice Department's "Innocent Images" investigation reveals that online services or bulletin boards are rapidly becoming one of the most prevalent sources used by predators to identify and contact children.

At the Workshop, participating industry groups stated their commitment to effective self-regulation. Industry guidelines on the collection and use of children's information were presented by the Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus and by the Direct Marketing Association, among others. These guides, however, have only recently been released, and industry is just beginning its efforts to educate Web site operators and seek compliance. In general, the recent issuance of industry guidelines in the children's area demonstrates the industry's commitment to addressing this problem. Nonetheless, there were concerns about the sufficiency of the guidelines. While all of the guidelines call for some form of notice and some degree of choice over the disclosure of personal information about children to third parties, the guidelines do not make clear what specific steps would satisfy these obligations. The extent and speed of industry compliance with the new guidelines will be important to evaluating whether action by government is needed.

Overall, there was strong support at the Workshop for development of technological tools to protect children's privacy. The testimony also identified important limitations on the ability of current products to protect children's privacy. First, computer-savvy children can easily defeat them.[3] Second, although, 85% of parents say they would use filters if they were inexpensive and easy to operate, only 25% of parents said they were currently using them.[4] Third, while newer, interactive technologies to enhance children's online privacy were also demonstrated, their widespread implementation is at least one or more years away. For example, a new technical standard is being developed that would allow parents to set privacy preferences for their children automatically. In addition, other technologies such as digital certificates and biometric technology were presented as possible means of obtaining verifiable parental consent in the future. These technologies are only now being applied to protecting privacy, and their effectiveness will depend on their widespread adoption by industry and parents.

The staff is taking a number of steps to address the important issues raised by the online collection of information from and about children. First, in response to a petition to the Commission from the Center for Media Education (CME), the staff of the Bureau of Consumer Protection recently issued the attached letter denying the petition. The letter also provides the industry with initial staff guidance with respect to online information practices that could be deemed deceptive or unfair under Section 5 of the FTC Act.

Second, having provided initial staff guidance in the CME letter, the staff will continue to review the online collection and use of information from children by commercial Web sites and will recommend that the Commission initiate enforcement actions where appropriate. We believe that carefully selected enforcement actions will help support effective industry self-regulation.

Third, Commission staff will continue to support self-regulatory efforts, as well as technological responses to this issue. We will include our assessment of the industry's self-regulatory efforts in our June 1998 report to Congress. In preparing this report, we will assess the percentage of sites providing notice to parents, whether the notice meets the criteria set forth in the staff's response letter to CME, what information is being collected from children, and how Web sites are using this information.

Fourth, the staff will continue to pursue a dialogue with industry about the desirability of FTC guidelines in the area of children's online privacy. The Workshop revealed uncertainty in the

---

[3] Some of the filters do not screen for disguised names -- even simply separating a first and last name with a period can bypass a filter programmed to block the first and last name of a child. In addition, none of the filters reportedly guard against a child giving up information via check boxes, multiple choice menus, or as an e-mail attachment.

[4] For this reason, it appears that these filters may be widely used only if they are incorporated into Web browsers, rather than left to individual parents to obtain.

business community about what constitutes an unfair or deceptive practice in the context of online information collection from children. The CME letter and any future enforcement actions may provide adequate guidance, but we will also continue to explore the possibility of guides that would further clarify what information practices would constitute an unfair or deceptive practice under Section 5.

Finally, the information presented at the Workshop demonstrated the need to educate parents about privacy issues concerning their children's use of the Internet and the need for parents to establish clear rules for children on information disclosure to Web sites.[5] Commission staff will develop additional educational materials for parents and children regarding privacy protections for children online and, most importantly, look for ways to work with affected industries, consumer groups, and educators to develop educational initiatives.

---

[5] For example, one industry effort offers the following online safety rule: "I will not give out personal information such as my address, telephone number, parents' work address/ telephone number, or the name and location of my school without my parents' permission." Child Safety on the Information Highway, National Center for Missing and Exploited Children and the Interactive Services Association (1994).

Conclusion

The Workshop proved to be an invaluable source of information to assist our consumer privacy efforts. In sum, these efforts include the following steps. We expect to report to Congress on the database study by the end of 1997. We plan to monitor industry's self-regulatory efforts in connection with unsolicited commercial e-mail and to bring enforcement actions, as appropriate, against senders whose practices violate the Federal Trade Commission Act. We also will monitor the information practices of commercial sites on the World Wide Web, and we will report our findings on the effectiveness of self-regulation to Congress by June 1, 1998. With regard to children's online privacy, we will monitor industry's implementation of its guidelines, review online information collection practices by commercial Web sites, take enforcement action, where appropriate, and report our findings to Congress. We will continue to educate consumers and industry about information privacy issues in all these areas.

We appreciate your continued interest in, and support of, our work in this area.

By direction of the Commission.

Donald S. Clark
Secretary