

**PREPARED STATEMENT OF THE  
FEDERAL TRADE COMMISSION ON**

**"INTERNET PRIVACY"**

Before the

**SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY**

of the

**HOUSE COMMITTEE ON THE JUDICIARY  
UNITED STATES HOUSE OF REPRESENTATIVES**

Washington, D.C.

March 26, 1998

---

Mr. Chairman and members of the House Judiciary Committee: I am David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the important issue of privacy on the Internet.<sup>(1)</sup>

## **I. Introduction**

### ***A. Internet Privacy***

The Internet is an exciting new marketplace for consumers. It offers not only easy access to a vast array of goods and services, but also to rich sources of information that enable consumers to make better-informed purchasing decisions.

The online consumer market is growing exponentially. In early 1997, 51 million adults were already online in the U.S. and Canada.<sup>(2)</sup> Of those people, 73% reported that they had shopped for product information on the World Wide Web ("the Web"), the interactive graphics portion of the Internet.<sup>(3)</sup> By December 1997, the number of adults online in the U.S. and Canada had climbed to 58 million, and 10 million had actually purchased a product or service online.<sup>(4)</sup> Further, analysts estimate that Internet advertising -- which totaled approximately \$301 million in 1996 -- will swell to \$4.35 billion by the year 2000.<sup>(5)</sup>

These figures suggest rapid growth of the online marketplace, but there are also indicators that consumers are wary of participating in it. Surveys have shown that increasing numbers of consumers are concerned about how their personal information is used in the electronic marketplace. This research indicates that consumers have less confidence in how online service providers and online merchants handle personal information than they have in how traditionally off-line institutions, such as hospitals and banks, handle such information.<sup>(6)</sup> In fact, 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.<sup>(7)</sup> According to the results of a *Business Week* survey released earlier this month, 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.<sup>(8)</sup> These findings suggest that consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until sufficient consumer privacy protections are implemented in the online marketplace.

### ***B. The FTC's Role***

The mission of the FTC is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission undertakes this mission by enforcing the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.<sup>(9)</sup> The Commission's responsibilities are far-reaching. With the exception of certain industries, this statute provides the Commission with broad law enforcement authority over virtually every sector in our economy.<sup>(10)</sup> Commerce on the Internet falls within the scope of this statutory mandate.

### ***C. The FTC's Approach to Online Privacy***

The Commission is taking a proactive approach to online privacy issues impacting consumers by: (1) identifying potential consumer protection issues related to online marketing and commercial transactions; (2) providing a public forum for the exchange of ideas and presentation of research and technology; and (3) encouraging self-regulation.

The Commission's first public workshop on privacy was held in April 1995. In a series of hearings held in October and November 1995, the FTC 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. A summary of the workshop testimony was published by the Commission in a December 1996 staff report entitled *Consumer Privacy on the Global Information Infrastructure*. The agency held a four-day workshop in June 1997 to explore issues raised by computerized databases that contain consumers' personal identifying information (also known as "individual reference services" or "look-up" services). This workshop also explored issues relating to unsolicited commercial e-mail, online privacy, and children's online privacy.

These FTC 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 consumer privacy

concerns in the electronic marketplace.<sup>(11)</sup> In addition, FTC staff has written opinion letters delineating what types of practices in this area might violate the Federal Trade Commission Act.<sup>(12)</sup>

## **II. Focus of FTC Privacy Activities**

Following the June 1997 workshop, the Commission focused on a number of key privacy issues impacting consumers. These issues were discussed in a July 31, 1997, letter (Attachment A) responding to a joint request from Chairman John McCain and Chairman Tom Bliley for a brief report on the Commission's findings from the workshop. The Commission's letter summarized its work and provided a plan to address concerns raised by the following issues: (1) computerized databases containing consumers' personal identifying information, *i.e.*, individual reference services or look-up services; (2) unsolicited commercial e-mail; (3) online information collection; and (4) children's privacy in the online environment. I will address each of these issues today. In addition, as set forth in the July 31 letter, the Commission intends to issue a report to Congress in June 1998 that will focus on the Commission's efforts to monitor and assess the status of self-regulatory efforts by industry members involved in the online collection and dissemination of consumer information.

### ***A. Individual Reference Services***

In response to growing public and Congressional concern, the Commission examined the availability of sensitive personal identifying information through computerized database services that are used to locate, identify, or verify the identity of individuals, often referred to as individual reference services or look-up services. The Commission's study of look-up services culminated in a report to Congress in December 1997. The report summarized what the Commission had learned about the individual reference services industry; examined the benefits, risks, and potential controls associated with these services; assessed the viability of an industry self-regulatory proposal; and concluded with recommendations that address concerns left unresolved by the proposal.<sup>(13)</sup>

The Commission found that a vast amount of information about consumers is available to customers of individual reference services through the services' proprietary computer networks and increasingly over the Internet. Gleaned from various public and proprietary sources, information available through the services ranges from purely identifying information, *e.g.*, name and phone number, to much more extensive data, *e.g.*, driving records, criminal and civil court records, property records, and licensing records.<sup>(14)</sup> The Commission also learned that convenient access to this type of information confers a myriad of benefits on users of these services and on society. The look-up services enable law enforcement agencies to carry out their missions, parents to find missing children, journalists to report the news, and consumers to find lost relatives.<sup>(15)</sup> At the same time, the increasing availability of this information poses various risks of harm to consumers' privacy and financial interests, including the possibility of increasing the incidence of identity theft.<sup>(16)</sup>

At the June 1997 workshop, a group of industry members (the "Individual Reference Services Group" or "IRSG") announced its intent to address concerns associated with its industry through self-regulation. Commission staff worked with this group to encourage it to adopt an effective self-regulatory program. In December 1997, 14 companies, a substantial majority of the individual reference service industry, agreed to abide by the "IRSG Principles," a set of principles that addresses the availability of information obtained through individual reference services.

The IRSG Principles restrict access to certain information obtained from "non-public" sources contained in each signatory's database. This non-public information includes what is called "credit header" information, which is that portion of a credit report purchased from a credit reporting agency that contains an individual's name, address, aliases, Social Security number, current and prior addresses and telephone number.<sup>(17)</sup> The restrictions vary according to the category of customer. Customers that have less restricted access to non-public information are subject to greater controls. It is noteworthy that the IRSG Principles prohibit distribution to the general public -- over the Internet or otherwise -- of certain non-public information, including Social Security number, mother's maiden name, and date of birth. In addition, consumers will be able to access the non-public information maintained about them in these services and to prevent the sharing (*i.e.*, "opt out") of the non-public information distributed to the general public.<sup>(18)</sup>

The IRSG Principles show particular promise because they include a compliance assurance mechanism and are likely to influence virtually the entire individual reference services industry. First, signatories must undergo an annual compliance review by a professional third party such as an accounting firm, the results of which will be made public. Public examination of the results of compliance reviews and the possibility of liability under the FTC Act and similar state statutes should create an incentive for compliance by signatories. Second, signatories that are information suppliers (*e.g.*, the three national credit reporting agencies) are prohibited from selling information to entities whose practices are inconsistent with the Principles. Therefore, non-signatories whose practices are inconsistent with the Principles likely will be unable to obtain non-public information easily for redissemination through their services. Thus, the IRSG Principles should substantially lessen the risk that information held by these services will be misused, and they should address consumers' concerns about the privacy of their non-public information.<sup>(19)</sup>

The Commission concluded that the IRSG Principles address many of the concerns associated with the increased availability of non-public information through individual reference services while preserving important benefits conferred by this industry. However, important issues related to individual reference services remain. For example, the IRSG Principles do not give consumers access to the "public information" (*e.g.*, real estate, motor vehicle, and court records) maintained about them and disseminated by the look-up services. Accordingly, consumers will not be able to check for inaccuracies resulting from transcription or other errors occurring in the process of obtaining or compiling the public information by the look-up services. IRSG members have agreed to

revisit this issue by June 1999, and to consider whether to conduct a study quantifying the extent of any such inaccuracies. The Commission has urged the IRSG to conduct an analysis to determine whether the frequency of inaccuracies and the harm associated with them are such that consumer access to public record information or other safeguards are in fact unnecessary.<sup>(20)</sup>

In its report to Congress, the Commission also encouraged public agencies to consider the potential consequences associated with the increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices. Finally, the Commission has acknowledged and encouraged the ongoing efforts of many privacy advocates, consumer groups, government agencies, and the IRSG to educate the public about information privacy issues.<sup>(21)</sup>

### ***B. Unsolicited Commercial E-mail***

At the 1997 Workshop, the Commission also gathered a considerable body of information concerning the problem of unsolicited commercial e-mail ("UCE"). Three UCE-related initiatives grew out of that workshop. First, a cross-section of interested parties, including Internet service providers, online firms, senders of UCE, and privacy advocates, formed a working group to develop a self-regulatory solution to the problems associated with UCE. This group, which has been led by the Center for Democracy and Technology, a non-profit, public interest organization involved in new technology issues, is expected to issue a report outlining proposed solutions. Second, the Commission brought enforcement actions against scam artists who make allegedly fraudulent solicitations via UCE,<sup>(22)</sup> and continues to investigate other possible frauds committed through UCE. Third, the Commission has launched an educational campaign. Staff have produced educational materials warning consumers to be suspicious of the solicitations they receive in UCE and are distributing them through channels designed to reach those who are likely to use e-mail. Staff also monitored thousands of UCE messages, identified those which appeared facially deceptive, and sent letters to over one thousand senders of these UCE messages, advising them of the legal requirements applying to their activities.

### ***C. Online Information Collection Practices***

Many consumers care deeply about the privacy and security of their personal information in the online environment and are looking for greater protections.<sup>(23)</sup> During the Commission's first privacy workshop, a consensus emerged among workshop participants regarding four important considerations that would assist in protecting online privacy. These considerations include: **notice** concerning Web sites' information practices, *i.e.*, how commercial Web sites will use personal information they collect from consumers; **choice** in how Web sites will use consumers' personal information; **access** to consumers' own information collected, maintained, or used by Web sites; and **security** of consumers' personal information maintained by Web sites from improper or unauthorized use by third parties.<sup>(24)</sup>

## **1. Commitment to Self-Regulation**

The Commission has also learned that members of the online industry are aware of the need to address consumers' concerns. Throughout the series of Commission workshops on these issues, the online industry has asserted that self-regulation is the most efficient and effective means of creating online privacy protections. Industry groups have demonstrated varying approaches to protecting online consumer privacy. As of June 1997, certain key trade associations had developed policies and procedures to protect online privacy. Others were in the initial stages of policy formation, and still others remained uncertain as to whether industry-wide policies, as opposed to individual company efforts, would be necessary. Trade association representatives committed to develop privacy policies as guidance for their members and to encourage their members to post their own information practices on their Web sites. In addition, a non-profit group called TRUSTe launched a proprietary system requiring disclosure of member Web sites' basic information practices and third-party auditing of those practices, but the system had not yet been widely implemented.<sup>(25)</sup> Its efficacy will depend upon widespread industry participation.<sup>(26)</sup>

The Commission has also learned of promising 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. At the time of the 1997 Workshop, these technological tools, which potentially could provide adequate privacy protection, were still in the initial stages of development.<sup>(27)</sup>

## **2. Online Information Collection from and about Children**

The collection of information from and about children who use the Internet deserves special attention. Internet usage by children is growing: a 1997 survey indicates that approximately 9.8 million children (under age 18) go online, which is a five-fold increase from 1995.<sup>(28)</sup> Children use the Internet for a variety of activities including homework or informal learning, playing games, browsing or for e-mail/chat rooms.<sup>(29)</sup> These young people are not shopping or banking online, but parents still have serious concerns about the online collection and use of personal information from children. A 1997 survey indicates that 97 percent of parents whose children use the Internet believe Web sites should not sell or rent personal information on children; 80 percent object to a Web site requesting a child's name and address when the child registers, even if such information is used only internally.<sup>(30)</sup>

Several workshop participants voiced concern at the 1997 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.<sup>(31)</sup> For example, anecdotal evidence indicates that many children surfing the Internet claim to have experienced problems, such as attempted password theft and inappropriate advances by adults in children's chat rooms.<sup>(32)</sup> Further, the FBI and Justice Department's "Innocent Images" investigation reveals that online services and bulletin

boards are rapidly becoming the most prevalent sources used by predators to identify and contact children.<sup>(33)</sup>

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.<sup>(34)</sup> All of the guidelines call for some form of notice and some degree of parental choice over the disclosure of personal information about children to third parties. The guidelines, however, do not always make clear what specific steps would satisfy these obligations or take into account that children may be online without parental supervision.

Overall, there was strong support at the 1997 Workshop for development of technological tools, such as filtering or browser software, to protect children's privacy. Yet, important limitations were identified, such as the ability of computer-savvy children to defeat technological protections and the fact that their widespread implementation and use may be over a year away.<sup>(35)</sup> These technologies are only now being applied to protecting privacy, and their effectiveness will depend on their widespread adoption by industry and parents.

Finally, the information presented at the 1997 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 providing information to Web sites. Commission staff is developing additional educational materials for parents and children regarding privacy protections for children online and, most importantly, looking for ways to work with affected industries, consumer groups, and educators to develop educational initiatives.<sup>(36)</sup>

### **3. Encouraging Self-Regulation**

The Commission has encouraged industry to address consumer concerns through self-regulation. In the Commission's view, self-regulation in the first instance generally is more prompt, flexible, and effective than government regulation. Further, self-regulation can bring the accumulated judgment and experience of industry to bear on issues that may be difficult for the government to define with bright-line rules. Industry and consumers are well-situated to know what is needed and where immediate concerns lie. The IRSG Principles provide one promising model for self-regulation.

Commission staff has recently issued some guidance that should strengthen self-regulatory efforts to protect consumers' privacy both online and off-line. The Commission staff recently responded to a request from the Direct Marketing Association ("DMA") for an advisory opinion concerning whether the antitrust laws would permit it to require three things of its members: (1) to use the DMA's Mail Preference and Telephone Preference Services to honor consumers' requests to not be contacted by direct marketers; (2) to disclose to consumers how members sell or otherwise transfer personal information about those consumers to others; and (3) to honor consumers' requests that the members not sell or transfer their personal information. FTC Bureau of Competition

staff advised the DMA of its conclusion that these requirements, as the DMA described them, would not harm competition or violate the FTC Act.<sup>(37)</sup>

#### **4. Monitoring Self-Regulation**

The Commission continues to monitor the online collection and use of information from consumers, including children. Last October, Commission staff conducted a "Kids Privacy Surf Day," designed as a "quick snapshot" -- not a comprehensive survey -- of children's Web sites' privacy practices. Staff found that more than 80 percent of the over 100 sites surveyed were collecting personal identifying information from children, most without seeking parental permission or allowing parents to control the collection and use of the information. Commission staff sent the surveyed Web sites e-mail messages notifying them of potential law violations in connection with their information collection practices.

This month, the Commission is conducting a survey of commercial Web sites, including sites directed to children, to determine the extent to which they are disclosing their information practices and offering consumers choice regarding the online collection and use of their personal information. The survey covers approximately 1200 Web sites: 100 of the most frequently visited Web sites; roughly 900 sites drawn from a database of commercial Web sites maintained by Dun & Bradstreet, including subsamples representing the retail, health, and financial sectors; and roughly 200 children's sites drawn from Yahoo!igans' online directory of sites of interest to children. In particular, the Commission is looking at whether sites display privacy policies or discrete statements about their information practices and whether such disclosures (1) include notice to consumers as to whether their information will be transferred to third parties; (2) provide consumers with choice over the use of their information; (3) allow consumers to access the information that is maintained about them; and (4) inform consumers that security precautions will be taken to protect their information after it has been transferred. Further, the Commission is assessing whether the policies are easy to find. As to sites directed to children, the Commission is also determining whether individual sites allow parents to have control over the collection, disclosure, and use of their children's information.

### **III. Report to Congress: Assessing Staff's Findings**

As mentioned above, the Commission's upcoming report to Congress will focus on the effectiveness of self-regulation as a means of protecting consumer privacy online. The Commission will summarize and assess its findings from this month's comprehensive survey of commercial Web sites. The report will also include the Commission's analysis of existing industry guidelines and principles on the online collection and use of consumers' personal information. Toward that end, the Commission issued a *Federal Register* notice on March 5, 1998, requesting that interested trade associations and industry groups submit copies of their information practice guidelines and principles for inclusion in the Commission's report.



## IV. Conclusion

The Commission recognizes the importance of the development of the Internet as a viable and safe marketplace for consumers. In order for the online marketplace to grow, sufficient privacy protections must be in place. The Commission supports technological innovation and also encourages industry self-regulation so long as self-regulation proves meaningful and effective. The upcoming June report describing the results of the staff's Web survey will shed light on how much progress self-regulation has made in achieving effective online privacy protection for consumers. If such progress is inadequate, appropriate alternatives may need to be explored.

---

### Endnotes:

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 one Commissioner.
2. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Spring '97 (March 12, 1997) (defining adults as individuals over 16 years old) (reported at <[http://www.commerce.net/work/pilot/nielsen\\_96/press\\_97.html](http://www.commerce.net/work/pilot/nielsen_96/press_97.html)>) [hereafter *CommerceNet/Nielsen Demographic Study*, Spring '97]; IntelliQuest Communications, Inc., Worldwide Internet/Online Tracking Service (WWITS™): Second Quarter 1997 Study Sept. 4, 1997) (reported at <<http://www.intellicquest.com/about/release32.htm>>).
3. *CommerceNet/Nielsen Demographic Study*, Spring '97.
4. 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>>) [hereafter *CommerceNet/Nielsen Demographic Study*, Fall '97]. See also Yankelovich Partners, *1997 Cybercitizen Report* (Mar. 27, 1997) (reported at <<http://www.yankelovich.com/pr/970327.HTM>>) (finding that 23% of users ordered and paid for a product over the Internet, *i.e.*, "transacted" business online).
5. Jupiter Communications, *1998 Online Advertising Report* (Aug. 22, 1997) (figure includes directory listings and classified advertisements).
6. *Commerce, Communication, and Privacy Online, A National Survey of Computer Users*, by Louis Harris & Associates and Dr. Alan F. Westin (1997) (hereinafter referred to as "Westin Survey") at ix.
7. *Id.* at 20-21.
8. "Business Week/Harris Poll: Online Insecurity," *Business Week*, March 16, 1998.
9. 15 U.S.C. § 45(a). The Commission also has responsibilities under approximately thirty 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 35 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.

10. 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).

11. *E.g.*, FTC Report to Congress: *Individual Reference Services*, 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. In addition, the Commission presented testimony on September 18, 1997, on the Implications of Emerging Electronic Payment Systems on Individual Privacy before the House Subcommittee on Financial Institutions and Consumer Credit, Committee on Banking and Financial Services.

12. *E.g.*, Letter from Bureau of Consumer Protection Director to Center for Media Education, July 15, 1997.

13. FTC Report to Congress: *Individual Reference Services*, December 1997.

14. *Id.* at 4-5.

15. *Id.* at 9-11.

16. *Id.* at 13-16.

17. *Id.* at 5-6 and n. 42. Non-public information on an individual's financial status, employment background, credit history, and medical records can be found in a credit report, but the dissemination of that information by a credit reporting agency is strictly regulated under the Fair Credit Reporting Act, 15 U.S.C. § § 1681-1681u (1997).

18. *Id.* at 25-28.

19. *Id.* at 28-30.

20. *Id.* at 31-32.

21. *Id.* at 32-33.

22. *See FTC v. Maher*, Case No. WMN-98-495 (D. Md. filed Feb. 19, 1998) (unsolicited commercial e-mail promoting allegedly bogus business opportunity); *FTC v. Cooley*, CIV-98-0373-PHX-RGS (D. Ariz. filed Mar. 4, 1998) (unsolicited commercial e-mail promoting allegedly fraudulent credit repair services).

23. *Privacy & American Business Report*, Vol. 4, No. 3 (1997) (reporting on Louis Harris Associates and Alan F. Westin's *National Survey of Computer Users*).

24. FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996.

25. *See* Transcript from FTC Public Workshop on Consumer Information Privacy, June 11, 1997 at 108-

112.

26. As noted on page 17 *infra*, the Commission has recently requested information practice guidelines and principles from trade associations and industry groups to determine the current status of these efforts.

27. *See* Transcript from FTC Public Workshop on Consumer Information Privacy, June 13, 1997 at 81-82.

28. *Interactive Consumers Research Report*, Vol. 4, No. 5 at 1, May 1997 (discussing results of FIND/SVP's 1997 American Internet User Survey).

29. *Id.*

30. *See* Transcript from FTC Public Workshop on Consumer Information Privacy, June 12, 1997, at 156 (citing Westin Survey at 74).

31. *Id.* at 230.

32. *Id.* at 192-93.

33. *Id.*

34. *Id.* at 132-78 (June 13, 1997).

35. *Id.* at 25-26.

36. In response to a petition from the Center for Media Education concerning the information collection practices of "KidsCom," a web site directed to children, the Commission staff issued an opinion letter addressing potential Section 5 violations involved in the collection of personally-identifiable information directly from young children. Letter from Bureau Director Jodie Bernstein to Center for Media Education, July 15, 1997.

37. Letter from Bureau of Competition Assistant Director to Counsel for the DMA, Sept. 9, 1997.