Staff Report

Public Workshop on Consumer Privacy on the Global Information Infrastructure

December 1996

Table of Contents

I. THE ONLINE MARKETPLACE: CHALLENGES AND OPPORTUNITIES*

Globalization and new technologies are radically changing the contours of the late twentieth century marketplace. In the 1980's, the personal computer revolution enhanced the ability of government, industry, and consumers to capture a vast array of personal information automatically. In the 1990's, the technology underlying the Internet is making it even easier and less expensive to gather, store, analyze, transmit, and reuse personal information in ways that were unimaginable just a few years ago.

Expanded commercial use of the Internet will inevitably generate more information about more online interactions, and will make that information more readily accessible to a global community of information users. This presents both opportunity and risk. Opportunities for commercial activity online are virtually limitless. Anyone can establish a commercial site on the Internet and become a global marketer. The benefits of the free flow of information in this medium are apparent, both for consumers and for industry. Commerce may become more efficient; in the future marketers may spend fewer advertising dollars to communicate information to the consumers who are most interested in receiving it. Consumers may acquire more information about things that truly interest them, and spend less time sorting through unsolicited electronic mail.

The proliferation of readily available personal information, however, also could jeopardize personal privacy and facilitate fraud and deception. These risks may make consumers reluctant to use the Internet or participate in online transactions and therefore could prevent consumers from obtaining the benefits promised by online commerce.

The Federal Trade Commission seeks to understand these and other issues posed by the developing technology-based marketplace.[1] As part of this effort, the Bureau of Consumer

---

* This report was prepared by staff at the FTC. It does not necessarily reflect the views of the Commission or any individual Commissioner.

[1] In October and November 1995, the Commission held a lengthy series of hearings to examine the implications of globalization and technological innovation for both competition and consumer protection issues. An entire day was devoted to the newest global marketplaces — the Internet and the World Wide Web. The Commission heard testimony on the latest developments in this technology, on the new methods of marketing that the technology has made

Protection staff undertook a Consumer Privacy Initiative to examine consumer privacy issues in the online context, and to promote consumer and business education about the use of personal information online.[2] The Initiative opened an ongoing dialogue, in both traditional and electronic forums, with a wide range of interested parties — including online service providers, direct marketers, privacy advocates, information industry representatives, consumer groups, trade associations, and academics.[3]

The June 1996 Workshop that is the subject of this report was convened to continue that dialogue, and to allow the broadest possible group of interested parties to express their views on (1) privacy issues posed by the emerging online marketplace, and (2) online protections for consumer privacy. This report summarizes participants' views. It synthesizes subjects and strategies on which there was general agreement among workshop participants, records the issues upon which participants could not agree, and describes ongoing private efforts to address concerns about information privacy online. It is designed to be a resource not only for readers with an interest in privacy issues generally, but also for those who are working toward the development of policies and mechanisms for protecting consumer privacy online.

---

possible, and on emerging risks — including fraud, deception, and loss of privacy — faced by consumers who choose to engage in commerce in cyberspace.

[2] The Initiative can be traced to the Bureau's April 1995 public workshop on Consumer Protection and the Global Information Infrastructure, which explored consumer issues arising from new technologies such as the Internet. Participants at a session on privacy at that workshop sent the Commission two clear messages: first, that protecting consumer privacy online was a pressing concern, and second, that self-regulatory efforts should be given a chance to work before regulatory approaches were considered.

[3] Staff has engaged in a series of one-on-one discussions with these parties, and invited the public to take part in an online listserv devoted to information privacy issues. The listserv, whose subscribers correspond with one another electronically (although not in "real time"), has extended the dialogue on privacy issues to include a far-flung group of participants. This online discussion has complemented the series of individual meetings with Bureau staff: each has facilitated dialogue among individuals with the full range of views concerning privacy rights and responsibilities in the online commercial world.

II. ONLINE PRIVACY: GENERAL PRACTICES AND CONCERNS

The first day of the Workshop focused on current online uses of personal information, the core elements of voluntary privacy protections, new interactive technologies for enhancing notice and choice, and the Government's role in protecting consumer privacy online. Individual Workshop sessions also addressed consumer and business education strategies, the special issues posed by online uses of medical and financial information, and the potential impact of the European Union's Directive on the Protection of Personal Data on the online marketplace in the United States.[4] This part of the report draws on both the Workshop transcript and comments submitted for inclusion in the Workshop record.

A. Current Collection and Uses of Information

The Internet is a highly decentralized, global network of electronic networks. It is unique among communications media in the variety and depth of the personal information generated by its use.[5] When users browse on the World Wide Web ("the Web"), for example, they leave an

---

[4] A summary of the discussion on the European Directive is included in Appendix B.

[5] Center for Democracy and Technology (CDT) Comment at 8 (Doc. No. 5). Footnote citations are either to the printed record of the Workshop or to comments submitted after the Workshop was held. All of these materials are on file at the Federal Trade Commission. The transcript of the Workshop is available online at http://www.ftc.gov. Complete lists of Workshop participants and documents referenced in the footnotes can be found in Appendices G and H, respectively. Copies of privacy guidelines and online privacy proposals submitted for the Workshop record can be found in Appendix C.

Workshop participants differed in how they defined "personal information," for purposes of their guidelines or privacy-related proposals. The Coalition for Advertising Supported Information and Entertainment (CASIE), for example, defines "personal information" as "data not otherwise available via public sources." Goals for Privacy in Marketing on Interactive Media (1996) at ¶ 3 (Doc. No. 18). The Direct Marketing Association's (DMA) Guidelines for Personal Information Protection use a similar definition. Doc. No. 24, Attachment B at 2 ("information that is linked to an individual on a file and that is not publicly available or observable"). Other organizations employ broader definitions. The Information Industry Association (IIA)'s Fair Information Practices Guidelines refer to "personally identifiable information," defined as "information relating to an identified or identifiable individual." Doc. No. 23, Attachment, at ¶ 1 Commentary. The Center for Media Education (CME) and the Consumer Federation of America (CFA) define "personal information" very broadly, to include both "any information that is linked to or allows for the identity of individual children, their families, household members or other individuals the child knows to be determined" and such information as a child's physical or

electronic marker at each site (or on each page within a site) they visit. The series of electronic markers, or "clickstream," generated by each user's browsing activities can be aggregated, stored, and re-used.[6] Each Web site, in turn, captures certain information about users as they enter the site. A Web site can "know" users' e-mail addresses, the names of their browsers, the type of computer they are using, and the universal resource locator (URL), or Internet address, of the site from which they linked to the current site.[7]

This information-gathering capability is built into the software that makes the Internet function.[8] Indeed, the software requires clickstream data to be collected so the computer receiving the data can send the information file requested by a user (e.g., the Internet address of the next Web page that the user wants to browse) to that user's computer, rather than someone else's.[9] Clickstream data also permits Internet site owners to understand activity levels at various areas within sites,[10] in a manner analogous to a retail store's practice of checking inventory.[11]

The fact that online information-gathering is automated means it is invisible to the user and

---

psychological description, health, school, date of birth, interests and opinions, "when used in conjunction with identifying information." CME/CFA Proposal at 2 (Doc. No. 19).

[6] Goldman 13-14; CDT Comment at 8-9 (Doc. No. 5).

[7] Goldman 15-16. This scenario is drawn from the CDT online privacy demonstration, which is accessible through its Web site at www.cdt.org.

[8] Goldman 14, 16.

[9] Ingenius Comment at 3 (not paginated) (Doc. No. 29).

[10] Lieberman 316-17. Although the technology makes it possible for Web site owners to maintain logs of this "transactional" information for each visitor to the site, Goldman 14, it is currently difficult to accomplish this when more than one person uses the same computer. Ingenius Comment at 3 (not paginated) (Doc. No. 29). Participants differed on the question of whether it is currently possible to tie clickstream data to particular individuals. Some panelists argued that it is indeed possible to use the clickstream data to create a profile of individuals' preferences and usage patterns. Howard 383. See also Goldman 14; CDT Comment at 8 (Doc. No. 5). Others asserted that tracking site activity for individuals generates large, complex data files that cannot be used for profiling with current technology. Lieberman 317; O'Connell 321.

[11] Waters 407.

often takes place without the user's knowledge and consent.[12] Internet users may also voluntarily disclose personal information, including their e-mail addresses, by filling out a questionnaire at the request of an online marketer,[13] or participating in a chat room, bulletin board, or other online forum. From such activities it is possible to accumulate lists of individuals' e-mail addresses for marketing purposes.[14] Marketers, in turn, increasingly use electronic mail to reach both current and potential customers.[15] Unsolicited commercial e-mail messages, though not always unwelcome,[16] are a growing problem. Consumers incur the burden of processing such e-mail and the costs of downloading and reading it, including the time charges from their e-mail services.[17] Electronic mass mailings of online commercial solicitations also impose burdens on computers operated by online services and Internet access providers, with corresponding adverse effects for their subscribers.[18]

---

[12] Goldman 13; CDT Comment at 9 (Doc. No. 5). In certain instances, the transmittal of personally identifying information is blocked. If, for example, a user accesses the Internet through an online service provider such as America Online, Prodigy or CompuServe (as do forty-six percent of current users who access the Internet), the user's identity and e-mail address are protected by the service's proxy server, which is a computer acting as an intermediary between the sender and recipient of information. Interactive Services Association (ISA) Comment at 2 (Doc. No. 15). Web sites that the user enters will obtain the address of the proxy server (e.g., aol.com), and not the user's e-mail address. Ek 98. In this case, only the online service provider could tie clickstream data captured from the user's browsing activities directly to the user. Similarly, if a user accesses the Internet from a computer system protected by a "firewall," as is true for many corporate systems, the user's e-mail address cannot be ascertained. ISA Comment at 2 (Doc. No. 15); Goldman 16.

[13] DMA Comment at 4 (Doc. No. 24).

[14] The DMA and ISA's proposed Principles for Unsolicited Marketing E-mail provide that marketers who compile lists in this manner should give users whose names have been gathered an opportunity to have their information suppressed. Doc. No. 3 at ¶ 3; ISA Comment at 4 (Doc. No. 15).

[15] ISA Comment at 3 (Doc. No.15).

[16] Competitive Enterprise Institute (CEI) Comment at 2 (not paginated) (Doc. No. 31).

[17] See Sherman 29.

[18] ISA Comment at 3 (Doc. No. 15).

B. CONSUMERS' ATTITUDES ABOUT PRIVACY AND INTERACTIVE MEDIA

While there is much to be learned about consumers' views on the collection and use of personal information in the online environment, it is possible to discern some general trends. Survey research conducted over the last twenty years documents deep concern among Americans about how personal information is being used in the age of computers.[19] In a 1994 Harris Survey of Americans' attitudes about privacy and emerging interactive technologies, eighty-two percent of respondents stated that they are concerned about threats to their personal privacy.[20] According to the same survey, seventy-eight percent of respondents believe that consumers have lost all control over how businesses circulate and use personal information; seventy-six percent believe that businesses ask consumers for too much personal information;[21] and seventy percent have refused to give information to a business because they felt it was either unnecessary or too personal.[22]

These findings must be understood in the context of a complex array of individual consumer attitudes about privacy in traditional contexts.[23] As several Workshop participants noted, the

---

[19] Louis Harris and Associates, Inc., Interactive Services, Consumers, and Privacy (conducted for Privacy & American Business) (1994) at 70 (Doc. No. 11) [hereinafter "1994 Harris Survey"] (summarizing results of surveys conducted from 1978-94). A national study of online and Internet users' opinions on various privacy issues is currently being planned by Professor Alan Westin and Privacy & American Business. Westin 41.

[20] 1994 Harris Survey at 70 (Doc. No. 11).

[21] Id. at 73-75, 76-78.

[22] Id at 85-87.

[23] Consumers' privacy concerns should also be viewed against the backdrop of federal privacy protections. There is no overarching federal statute governing information privacy in the United States. Congress has addressed information privacy on a sectoral basis, crafting statutes that govern distinct concerns and establish targeted individual rights. The Privacy Act of 1974, for example, places limitations on the collection, use and dissemination of information about individuals by federal agencies. 5 U.S.C. § 552a. The Tax Reform Act of 1976 restricts the ability of the Internal Revenue Service to disclose personal information obtained in connection with its review of individual tax returns. 26 U.S.C. § 6103. Congress has enacted protections for individual bank records (Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401) and for personal information included in credit reports (Fair Credit Reporting Act, 15 U.S.C. § 1681). Federal statutes have also created privacy rights with respect to student records (Family

decision to divulge or not divulge personal information varies not only with the individual, but also with the context.[24] According to one panelist, survey research consistently indicates that roughly one-quarter of the American public is "intensely" concerned about privacy and that another quarter has little or no concern; the remaining fifty percent view this issue pragmatically, approaching it on a case-by-case basis.[25] These individuals consider factors such as: the nature of the benefit being offered in exchange for personal information; whether the information being collected is relevant to the benefit or socially acceptable; and whether adequate safeguards are in place to protect their information.[26]

Survey results suggest that although many individuals are willing to strike a balance between maintaining personal privacy and obtaining the information and services that new interactive technologies provide, they are concerned about potential misuse of their personal information and want meaningful and effective protection of that information.[27] In the 1994 Harris Survey, fifty-one percent of respondents stated they would be concerned if an interactive service to which they subscribed engaged in "subscriber profiling," i.e., the creation of individual profiles based upon subscribers' usage and purchasing patterns, in order to advertise to subscribers.[28] Respondents were less concerned about subscriber profiling where the interactive service provided privacy safeguards for subscribers, such as notice of when a profile would be created and how it would be used, control over the types of information to be used for advertising and

---

Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g), electronic mail and voicemail communications (Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510), video rental records (Video Privacy Protection Act of 1988, 18 U.S.C. § 2710), cable television subscriber information (Cable Communications Policy Act of 1984, 47 U.S.C. § 521), and customer information held by telecommunications carriers (Telecommunications Act of 1996, Pub.L. No. 104-104, 110 Stat. 56). Federal legal protections are complemented by state law and by self-regulatory efforts such as those described elsewhere in this report.

[24] Westin 39-40; Consumer Alert Comment at 1-2 (Doc. No. 13); CEI Comment at 1-2 (Doc. No. 31).

[25] Westin 39.

[26] Westin 39-40.

[27] Westin, A. F., "Interpretive Essay," in 1994 Harris Survey at xxv-xxvii (Doc. No. 11).

[28] 1994 Harris Survey at 93-94 (Doc. No. 11).

the types of advertising employed, and access to the information in the profile.[29]

C. PRIVACY PROTECTIONS: AREAS OF AGREEMENT AND DIVERGENT VIEWS

Workshop participants expressed a common understanding about the necessary elements of self-regulatory approaches to protecting consumer privacy online, but differed greatly on how to implement them. These elements closely track fair information practices identified by the U.S. Department of Health, Education & Welfare in 1973.[30] More recent government efforts to define privacy principles for interactive media also incorporate these practices,[31] as do policies already in use in traditional marketing media. Privacy advocates did not dispute the value of many of these measures, but argued that self-regulatory efforts are successful only against a background of legally enforceable rights to information privacy.[32]

Many businesses operating in traditional media have yet to develop privacy policies,[33] and many businesses operating online have not yet fully confronted the privacy issues posed by interactive technologies.[34] Hence, few Web sites have privacy policies or display their information practices to consumers.[35] With increasing competitive pressures to provide privacy protections, industry is recognizing the need to address this issue.[36] Indeed, the need to craft

---

[29] Id. at 96, 108-19; Westin, "Interpretive Essay," supra n. 27, at xxvi-xxvii.

[30] Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health, Education and Welfare, Records, Computers and the Rights of Citizens (July 1973) (recommending legislation establishing a federal Code of Fair Information Practice for all "automated personal data systems").

[31] U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (1995); National Telecommunications and Information Administration, U.S. Dept. of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995).

[32] Rotenberg 137-38; Smith 43-44. See Givens Comment at 3 (Doc. No. 9).

[33] See, e.g., Westin 144 (discussing the banking industry).

[34] Strenio 255-56.

[35] Id; Weitzner 115.

[36] Jaffe at 102-03.

privacy policies is implicit in information practice guidelines promulgated by various industry groups.[37]

1. Notice

Workshop participants generally agreed that notice of information practices is an essential first principle in advancing online information privacy.[38] All of the guidelines and industry statements submitted by participants call for some form of notice of information practices to consumers.[39] Participants stated that, at a minimum, notice should include the identity of the

---

[37] See, e.g. IIA Fair Information Practices Guidelines (1994) (Doc. No. 23, Attachment); CASIE Goals for Privacy in Marketing on Interactive Media (1996) (Doc. No. 18); ISA Guidelines for Online Services: The Renting of Subscriber Mailing Lists (1995) (Doc. No. 15, Attachment).

[38] See e.g., Golodner 60; CDT Comment at 2 (not paginated) (Doc. No. 22); DMA and ISA proposed Joint Statement on Online Notice and Opt-Out (1996) (Doc. No. 4); ISA Guidelines for Online Services: The Renting of Subscriber Mailing Lists (1995) (Doc. No. 15, Attachment); CASIE Goals for Privacy in Marketing on Interactive Media (1996) (Doc. No. 18); IIA Fair Information Practices Guidelines (1994) (Doc. No. 23, Attachment); DMA Guidelines for Personal Information Protection (1995) (Doc. No. 24, Attachment B).

[39] The substance of the notice varies, however. The IIA Fair Information Practices Guidelines state that members should establish a fair information practices policy and make it publicly available. Doc. No. 23, Attachment at ¶ 1. Nynex Corporation provides its customers a "Privacy Statement" detailing its information practices. Nynex Comment at 2 ¶ 2.(Doc. No. 8). The IIA Guidelines also provide for disclosure of intended uses of personal information, when the information is obtained directly from an individual. Doc. No. 23, Attachment at ¶ 3. The DMA Guidelines for Personal Information Protection state that individuals who provide personal information to marketers should be given notice of the potential rental, sale, or exchange of their personal information to third parties. Doc. No. 24, Attachment B at Art. 5. The ISA Guidelines for Online Services: The Renting of Subscriber Mailing Lists provide that subscribers are to be "clearly and actively notified" of a member service's subscriber list rental practices "proximate to sign-up." Doc. No. 15, Attachment at ¶ A.

CASIE's Goals for Privacy in Marketing on Interactive Media state that marketers seeking information through interactive media should notify consumers of potential transfers of the information to third parties. Doc. No. 18 at ¶ 4. The DMA and ISA proposed Joint Statement on Online Notice and Opt-Out provides that online marketers should make their information practices available online in a manner that is "easy to find, easy to read, and easy to understand." Doc. No. 4. ISA noted that this can easily be accomplished online. The ISA has posted such a notice on its Web page, as has the DMA. ISA Comment (Doc. No. 15 at 4); DMA Comment, Appendix C (Doc. No. 6). Users can click on an icon to read how the ISA Web site handles the

collector of the information, the intended uses of the information, and the means by which consumers may limit the disclosure of personal information.[40]

2. Consumer Choice

Panelists also agreed that consumers should be able to exercise choice with respect to whether and how their personal information is used, either by businesses with whom they have direct contact online or by third parties. Panelists disagreed, however, as to how that choice should be exercised. Industry representatives for the most part favor an "opt-out" approach, which allows personal information to be used unless consumers notify marketers that their information is not to be used in specified ways.[41] The privacy policies of America Online and CompuServe include an "opt-out" mechanism that subscribers may use to have their names removed from membership lists made available to third parties.[42] The DMA and ISA's proposed Joint Statement on Online Notice and Opt-Out follows this approach,[43] as do DMA and ISA's

---

browsing information transmitted to it. ISA Comment at 4 (Doc. No. 15).

[40] CDT Comment at 2 (Doc. No. 22); DMA and ISA proposed Joint Statement on Online Notice and Opt-Out (Doc. No. 4); IIA Fair Information Practices Guidelines (Doc. No. 23, Attachment).

[41] Sherman 28 (referring to unsolicited e-mail); DMA Guidelines for Personal Information Protection Art. 5 (Doc. No. 24, Attachment B); DMA and ISA proposed Joint Statement on Online Notice and Opt-Out (Doc. No. 4); CASIE Goals for Privacy in Marketing on Interactive Media at ¶ 5 (Doc. No. 18); ISA Guidelines for Online Services: The Renting of Subscriber Mailing Lists ¶ B (Doc. No. 15, Attachment). The IIA's Fair Information Practices Guidelines do not specify the timing of notice and consumer choice. Doc. No. 23, Attachment at ¶ 3. See also Nynex Privacy Principles, at 3 (providing for customer "opt out") (Doc. No. 8); Consumer Alert Comment at 3 (not paginated) (Doc. No. 13).

[42] America Online Comment, Attachment at 12 (Doc. No. 17); CompuServe Comment, Attachment A at 8 (not paginated) (Doc. No. 25).

[43] Doc. No. 4. The ISA's Guidelines for Online Services: The Renting of Subscriber Mailing Lists do not specify the mechanism members should provide to subscribers for removing their names from mailing lists. Members may devise any scheme so long as the process is "easy and well publicized." ISA Comment, Attachment at ¶ B (Doc. No. 15).

proposed Principles for Unsolicited Marketing E-mail.[44]

Some privacy advocates believe that requiring affirmative consent prior to any collection or commercial use of a consumer's personal information is the most effective privacy protection.[45] In their view, individuals have a property interest in their personal information. This interest can be protected only through an "opt-in" regime that maintains the privacy of personal information unless an individual releases it.[46] Other privacy advocates argued that interactive technology can provide an alternative to regimes requiring only an "opt-out" or an "opt-in." In their view, software could be used to allow consumers to communicate their privacy-related preferences automatically for all of their online interactions or on a case-by-case basis.[47]

3. Data Security and Consumer Access

Panelists agreed that the security of personal information is essential if commerce in cyberspace is to flourish on the Internet.[48] Many also agreed that consumers should have access to information about them that is held by marketers and other online businesses, and that collectors of such information should maintain the information's accuracy and timeliness. IIA's Fair Information Practices Guidelines, DMA's Guidelines for Personal Information Protection,

---

[44] Doc. No. 3. The proposed Principles provide several strategies for addressing the problem of unsolicited commercial e-mail. They propose that commercial solicitations be identified as such and disclose the marketer's identity. Id. at ¶ 2. They provide that recipients of these solicitations who have no prior relationship with the marketer should be told of a mechanism through which they can instruct the marketer to send no other solicitations. Id. They also propose that marketers having an established relationship with online customers should provide them a notice and opt-out mechanism to prevent the use of their e-mail addresses in marketing lists sold, rented or exchanged for online solicitation purposes. Id.

[45] Hendricks 31; Goodman Comment at 1 (Doc. No. 26).

[46] Goodman Comment at 1 (Doc. No. 26). Consumers' views on the "opt-in" vs. "opt-out" debate are not well understood. Professor Alan Westin is planning a study that would investigate consumers' preferences in this regard. Westin 41. In a recent survey of consumer views on direct marketing generally, eighty-three percent of respondents stated that they favored legislation requiring an "opt-in" regime for including names on mailing lists used for marketing. Negus, B., "You're Not Welcome," Direct 1 (June 15, 1996).

[47] Goldman 14-15; CDT Comment at 15-23 (Doc. No. 5); CDT Comment at 4 (Doc. No. 22). See also Resnick Comment at 9-10 (Doc. No. 14).

[48] See Rotenberg 24; Krumholtz 38; Jaffe 105; Wellbery 205.

and CASIE's Goals for Privacy in Marketing on Interactive Media all call for mechanisms giving consumers access to stored information about them and a right to correct that information when necessary.[49] Privacy advocates likewise view access to personal information as an essential privacy protection.[50] Panelists also agreed that the entities holding such information must take steps to protect it from loss or misuse.[51] Both IIA and DMA call for such protections in their guidelines.[52] IIA encourages its members to require any third parties to whom they transfer personal information to extend a comparable level of protection.[53]

D. SENSITIVE DATA: MEDICAL AND FINANCIAL INFORMATION ONLINE

The first day of the Workshop focused on privacy practices and protections generally, rather than on particular categories of information being collected. One panel, however, was devoted to online uses of medical and financial information, two categories generally thought to be particularly sensitive and worthy of special protection. As one panelist noted, of all the types of information collected about individuals, the public is most troubled by the prospect of unauthorized disclosure of medical and financial information.[54] Changes in the health care and financial industries will affect how such personal information is used. As the health care

---

[49] IIA Comment, Attachment at ¶¶ 4-5 (Doc No. 23); DMA Comment, Attachment B at Arts. 3-4 (Doc. No. 24); CASIE Goals at ¶ 5 (Doc. No. 18).

[50] CDT Comment at 2-3 (Doc. No. 22); Rotenberg 159-60. See also Smith 164 (calling for screening mechanisms to ensure the accuracy of personal information prior to its transmittal via the Internet).

[51] See e.g., CDT Comment at 3 (not paginated) (Doc. No. 22). For example, the IIA's Guidelines call for "reasonable and appropriate steps" to protect personal information from loss, destruction, or unauthorized use. IIA Comment, Attachment at ¶ 2 (Doc. No. 23). DMA's Guidelines for Personal Information Protection include a similar provision. Doc. No. 24, Attachment B at Arts.7-8. ISA's Guidelines for Online Services: The Renting of Subscriber Mailing Lists provide that members should take appropriate action where they identify misuses of personal information by third parties to whom they have transferred personal information. ISA Comment, Attachment at ¶ C (2)-(3) (Doc. No. 15).

[52] IIA Comment, Attachment at ¶ 2 (Doc. No. 23); DMA Comment, Attachment B (Guidelines for Personal Information Protection) at Arts. 7-8 (Doc. No. 24)

[53] IIA Comment, Attachment at ¶ 2 (Doc. No. 23).

[54] Westin 143 (discussing the consistent findings of survey research on this question).

industry changes, there is a move toward computerization of patient records and electronic exchange of medical information.[55] In the financial world, there are growing pressures to target-market products and services to individual consumers that require the collection and use of detailed personal information.[56]

Several panelists noted the benefits of online technology in the areas of health care and financial services.[57] Electronic transmission of medical information, for example, can enhance the quality of health care by facilitating long-distance consultations between doctors[58] and by allowing doctors to use e-mail to monitor their patients' compliance with treatment regimens.[59] One panelist opined that online technology could assist consumers by making financial information that is currently available only through intermediaries, such as credit reports, instantly available to them.[60]

Concerns about online uses of medical or financial information fall into two categories. First, there is a concern about unauthorized access to sensitive medical and financial information. The confidentiality of medical records, for example, could be compromised,[61] and information misused by third parties who gain unauthorized access to it through chat rooms, bulletin boards, or by other means.[62] Second, there is concern about the commercial use of medical and financial

---

[55] Id.

[56] Westin 144; Bushey 151.

[57] Frawley 165; Hendricks 171; Strenio 177-78; Westin 146-47.

[58] Frawley 165.

[59] Id; Strenio 177-78.

[60] Westin 146-47.

[61] Frawley 166.

[62] Frawley at 166-67; Westin 147. For example, a user might participate in a chat room for AIDS or breast cancer patients. As chat rooms are essentially public places, the user's e-mail address could be obtained and archived, as could the content of the user's posted comments. See Westin 147.

One panelist argued that medical information should not be transmitted at all on the Internet, because it is an insecure medium. Goldman 175. In some panelists' view, legislation is needed in this area to fully protect individuals. Frawley 167; Goldman 174-75. One panelist argued that

information. DMA believes that medical information derived from a patient-provider relationship should never be disclosed or used for marketing purposes, unless the patient has voluntarily provided such information through questionnaires, or the information has been otherwise compiled with the patient's knowledge.[63] DMA's Guidelines for Ethical Business Practice state that financial information such as credit card numbers and checking account numbers should not be sold, rented, exchanged, or transferred to third parties where the consumer has a "reasonable expectation" that the information will be kept confidential.[64]

Representatives of the direct marketing and banking industries rejected any approach that would categorically limit online commercial uses of financial information.[65] In DMA's view, the online marketplace will not become economically viable if marketers cannot use financial information to evaluate the credit-worthiness of a potential customer.[66] In the banking industry transfers of certain personal financial information among institutions are essential to prevent fraud.[67] The American Bankers Association representative argued that privacy protections must be weighed against the industry's need for customer accountability.[68]

Many panelists agreed that a secure online medium is a prerequisite for routine online

---

no personal information should be offered for sale to third parties on the Internet. Smith 164.

[63] Sherman 160-161; DMA Comment (Doc. No. 24), Attachment B (DMA Guidelines for Ethical Business Practice (1995) at 24). DMA's Guidelines for Ethical Business Practice provide that consumers who voluntarily give medical information to marketers should be notified of potential uses of the information (such as transfer to third parties) at the time they provide the information and that they should be given an opportunity to opt out of such uses. Id.

[64] Sherman 170; DMA Comment (Doc. No. 24), Attachment B (DMA Guidelines for Ethical Business Practice at 23). According to DMA's representative, financial information such as a credit account number should be used only to complete a given transaction, absent the consumer's knowledge and consent to transfer it to third parties. Sherman 170.

[65] Sherman 169-70; Daguio 171-73.

[66] Sherman 169-70.

[67] Daguio 173.

[68] Daguio 172. According to this Workshop panelist, privacy of financial information is an especially complex issue in an environment where neither the consumer, the merchant, nor the financial institution has absolute rights to individual financial information. Daguio 173.

transmission of medical and financial information, and that special protections are necessary for such information.[69] Privacy advocates viewed ready access to an individual's own medical and financial information as an essential privacy protection.[70] For some panelists, encryption and other technologies that facilitate anonymity, such as Smart Cards,[71] are valuable means of protecting the privacy of medical and financial information.[72]

---

[69] Westin 145-47; Bushey 151; Sherman 161; Merold 169; Hendricks 170; Daguio 172; Strenio 177.

[70] See Rotenberg 159-60.

[71] A Smart Card is a stored value card bearing an implanted microprocessor. It permits its owner to enter into transactions anonymously and to transmit encrypted information via the Internet. Koehler 154-55.

[72] Westin 145; Koehler 155; Rotenberg 180. One Workshop panelist suggested that his company's practice of stripping identifying information from individuals' medical prescription information compiled for marketing and research purposes is a solution transferrable to the online context. Merold 168.

III. ENHANCING CONSUMER PRIVACY ONLINE

During the first day of the Workshop, participants discussed enhancing consumer privacy online through technological innovation, education, self-regulation, and law enforcement. They agreed that if consumers are not confident that their personal information will be protected online, they will not use the Internet for commercial purposes and the online marketplace will not thrive.[73]

A. TECHNOLOGIES TO ENHANCE NOTICE AND CONSUMER CHOICE ONLINE

The Workshop highlighted three technologies that, in the view of many participants, could enhance online privacy and at the same time satisfy the legitimate needs of online businesses for information about current or potential customers. The approaches include technology that was in use at the time of the Workshop, as well as technology that could be adapted or extended to enhance notice and consumer choice with respect to information privacy online.

1. Universal Registration Systems

A representative of Internet Profiles Corporation (I/PRO), a market research firm, demonstrated the I/CODE system, a universal World Wide Web registration system.[74] Users and Web sites register with the system. When users register, they provide I/PRO with an array of personal information, including identifying information (name, street address, e-mail address), demographic information (age, gender, marital status) and information about product and service preferences.[75] In return for this information, users receive an identifier called an I/CODE, which allows them to browse anonymously in the Web sites in the I/CODE system.[76] I/PRO aggregates the anonymous demographic information for market analysis.[77]

When a user accesses a site in the I/CODE system, only the user's I/CODE and anonymous demographic information are transmitted to the site. I/PRO uses the anonymous information

---

[73] See e.g., Rotenberg 24; Krumholtz 38; Jaffe 105; Wellbery 205.

[74] Poler 64-68.

[75] I/PRO Comment, FAQ List and Answers, at ¶ 1.3 (Doc. No. 12).

[76] Id.

[77] Id. at ¶ 5.4.

collected in this manner by the site to perform aggregate data analysis for its clients. In response to a request from the site, the user may opt to disclose his or her e-mail address, in order to receive future communications from the site, and I/PRO then forwards the user's name and street address to the site. Personally identifying information is not sent to the site without the user's explicit consent.[78] All of the personal information transmitted between I/CODE and sites registered in the I/CODE system is encrypted. I/PRO and Web sites within the I/CODE system are contractually bound not to share or sell collected personal information to entities outside the I/CODE system.[79]

Within the I/CODE system, consumers enjoy a measure of control over how their personally identifying information is used online by registered sites. The system shelters users from unsolicited e-mail from Web sites within it and allows them to browse anonymously on the Web. At the same time it allows Web sites to conduct analysis of site usage and aggregate user preferences. The I/CODE system has proven to be popular; 450,000 users registered in the first ten weeks of its operation, and about 25,000 new subscribers are joining per week.[80] The Internet Profiles Corporation representative opined that a universal registration system is preferable to a system of online disclaimers and notices, because the latter disrupts the interactivity of the online medium.[81]

2. Cookies

Before the advent of "cookies" technology, a Web site's server was unable to know whether the downloading of separate pages within the site (for example, when a user browses from page to page within an online catalogue) represented one individual's series of movements or the separate movements of many individuals.[82] Cookies were invented to enable the Web site's server to keep track of a particular user's activity within the site. Cookies technology allows the Web site's server to place information about a user's visits to the site on the user's machine in a

---

[78] Poler 67; I/PRO Comment, FAQ List and Answers at ¶ 5.2 (Doc. No. 12).

[79] I/PRO Comment, FAQ List and Answers at ¶¶ 5.5-6.2.

[80] Poler 66; I/PRO Comment at 5 (Doc. No. 12).

[81] Poler 65.

[82] Harter 71.

text file that only that Web site's server can read.[83]

Using cookies, a Web site assigns each user a unique identifier (not the actual identity of the user), so that the user may be recognized in subsequent visits to that site.[84] On each return visit, the site can call up user-specific information, which could include the user's preferences or interests, as indicated by documents the user accessed in prior visits or items the user clicked on while in the site.[85] An expiration date feature allows cookies to be set to remain on a user's machine either permanently or for a specified length of time.[86] Cookies also vary in the extent of security they provide for the information they contain.[87]

Cookies can store information that facilitates the interaction between user and Web site. As an example of how a permanent cookie functions, consider the online version of a newspaper. If a subscriber whose native language is Spanish informs the Web site that he prefers to download the Spanish edition of the newspaper, the newspaper can store that information in a cookie file on the user's hard drive. When the subscriber next enters the newspaper's Web site, the site retrieves the language preference information from the cookie and automatically sends the Spanish-language edition to the user.[88] Temporary cookies can be created during online shopping expeditions. The cookies can tag the shopper's intended purchases to facilitate the ordering process and then expire after a purchase is made.[89]

According to the representative of Netscape Communications Corporation, cookies

---

[83] Id. Although not discussed at the Workshop, there has been controversy surrounding cookies, because users initially were unaware that cookies were being created on their hard drives. The latest version of Netscape's Web browser, Navigator 3.0, includes an alarm that can be activated at the user's discretion. Once activated, the alarm sounds before a cookie is created on the hard drive. Harter 74.

[84] W. Andrews, "Sites Dip Into Cookies to Track User Info," Webweek 17 (June 3, 1996).

[85] Id.

[86] Harter 72.

[87] Harter 74. Ordinary cookies employ hypertext transfer protocol (HTTP); "secure" cookies employ secure hypertext transfer protocol (SHTTP). Id.

[88] Harter 71-73.

[89] Andrews, supra n. 84.

technology could be used by Web sites to facilitate communication of consumers' privacy preferences.[90] Once a user communicated his or her privacy preferences in response to a Web site's notice of its information practices, the site could store that information in a cookie text file on the user's hard drive. The dialogue around privacy preference, notice, and consent that initially took place between user and site would, therefore, not have to be repeated in subsequent visits to the site.[91]

3. Platform for Internet Content Selection (PICS)

The World Wide Web Consortium at the Massachusetts Institute of Technology developed its Platform for Internet Content Selection (PICS) to enable parents to block their children's access to Internet sites whose content the parents deem objectionable.[92] PICS establishes a standard for "labeling" Internet sites on the basis of their content and for creating label-reading software to block access to some sites and permit access to others based upon the labels. PICS is a set of technical specifications, a standard format for labels; it is neither software nor label, but technical language that allows software and label to work together.[93]

PICS itself is "viewpoint-neutral."[94] Anyone can develop a set of content-rating criteria (identifying "hate speech," for example, or "excessive nudity"), create a labeling vocabulary, evaluate Internet sites, and use the PICS specifications to label sites accordingly. Labels are affixed to electronic documents such as home pages on the World Wide Web by site owners or third parties -- parent groups, religious groups, consumer groups -- who can locate their labels on agreed-upon sites. Software capable of reading labels in the PICS format may be developed independently of these labels. This software automatically checks for the labels and blocks access to sites based upon the labels.[95] Thus, if a user's software has been configured to block electronic documents labeled as "excessively violent" by a site-rating service that screens Web

---

[90] Harter 73.

[91] Id.

[92] Resnick Comment at 2 (Doc. No. 14).

[93] Id. at 3; Resnick 80-81.

[94] Vezza 77, 131.

[95] Resnick Comment at 3 (Doc. No. 14).

sites for such content, it will deny access to any site to which the rating service's "excessive violence" label is affixed. The user can override the software's action only through use of a password.[96]

The use of PICS technology for content-blocking purposes is proliferating.[97] Several panelists noted that PICS technology could be adapted to enhance online privacy.[98] Industry groups, privacy advocates, and consumer groups could use existing PICS technology to create rating systems based upon the privacy-protectiveness of Web sites' information practices, and these systems could then be used to block access to sites lacking strong protections.[99] If, for example, a consumer group created an index of privacy-protective Web sites based upon a review of their information practices, a user could set her PICS-compatible browser to allow access only to sites labeled as being in the index. The label-reading software would block access to sites that were not on the list.[100]

PICS technology might be extended further to allow more sophisticated notice and choice options. The prerequisite to extending PICS technology would be a standard format for describing information practices and user preferences as to how their information should be used.[101] A user would set his preferences (e.g., "no restrictions on use" or "no transfers to third

---

[96] See Resnick Comment at 3-5 (Doc. No. 14).

[97] Software capable of reading PICS labels is currently being included in new versions of Internet browsers and in programming offered by online services. Content labeling and rating services will soon be publicly available. Vezza 77; CDT Comment at 15 (Doc. No. 5); Resnick Comment at 3 (Doc. No. 14). For a discussion of currently available PICS-compliant filtering software for children, see Appendix F.

[98] Resnick Comment at 2 (Doc. No. 14); CDT Comment at 16-23 (Doc. No. 5); Vezza 78.

[99] CDT Comment at 20 (Doc. No. 5).

[100] Id. at 21.

[101] CDT Comment at 4 (not paginated) (Doc. No. 22); Resnick 87. At this time there is no agreed-upon vocabulary for describing particular information practices as "privacy protective." However, a hypothetical application of PICS technology, using the Canadian Standards Association's (CSA) 1996 Model Code for the Protection of Personal Information as the basis for such a rating vocabulary, was demonstrated at the Workshop. In this hypothetical scenario, the user's browser is configured to locate Web sites that carry a CSA label. PICS technology gives the user the flexibility to set his preferences to reflect the degree to which he is concerned

parties") on his computer with software that employs this format.[102] Web sites would similarly give notice of their information practices (e.g., "we do not sell or rent our customer list to other companies"). The user's browser would be capable of automatically comparing his preferences with sites' practices, as the user moves around the World Wide Web. If a particular Web site's practices matched the user's preferences, notice and choice would occur "seamlessly" in the background, and the user would proceed to enter the site. If there were a mismatch, the user's software would alert him to that fact.[103] The Web site could respond by providing an explanation for the mismatch, or offering the user an opportunity to view its information policy.[104] The Web site could offer the user incentives such as discounts in exchange for the user's agreement to accept the site's information practices.[105] Finally, extended PICS technology could theoretically enable this sort of negotiation about notice and choice to be automated.[106]

4. Participants' Views on the Demonstrated Technological Approaches

Workshop panelists agreed generally that the technologies demonstrated are promising means of advancing consumer privacy.[107] There was disagreement, however, as to whether these technologies are sufficient to address the full range of online privacy concerns. For some panelists, technologies including encryption, that allow individuals to use the Internet

---

about various requirements of the CSA Code. If, for example, he is willing to access sites that comply with some but not all Code provisions, he can so indicate. If he does not want to do business with sites unless they are in full compliance with the Code, he can set his preferences accordingly and the software will block access to non-complying sites. Resnick 83-85.

[102] According to CDT, the ability to pre-set the user's preferences is more protective of privacy than a model that forces the user to decide whether to opt-out of a site's information practices on a transaction-by-transaction basis. Comment at 4 (not paginated) (Doc. No. 22).

[103] CDT Comment at 18-20 (Doc. No. 5).

[104] Id. at 20; Resnick 85; Resnick Comment at 9-10 (Doc. No. 14).

[105] Resnick Comment at 10 (Doc. No. 14).

[106] Id; Resnick 86.

[107] See, e.g., Jaffe 103; Ek 96-97; Rotenberg 99, 101-02; Weitzner 95-96; Hendricks 107; Vezza 78; Reid 121; IIA Comment at 11 (Doc. No. 23); Givens Comment at 1 (Doc. No. 9).

anonymously, offer more effective privacy protection.[108]

Participants devoted considerable time to the PICS technology, and raised several concerns. Representatives of the direct marketing and information industries viewed filtering technologies such as PICS as "blocking technologies" that give consumers a "no" vote on entire categories of information content available online. IIA opined that use of PICS to block information by category, rather than on a case-by-case basis, would unacceptably restrict commercial speech.[109] A DMA representative shared this concern and asserted that filtering technologies such as PICS should be paired with technology that allows consumers to release information alerting marketers to the kinds of products and services about which they would be willing to accept solicitations. In DMA's view, this would balance consumers' privacy with the needs of businesses whose investments are crucial to the success of the online marketplace.[110]

Others expressed concern that a PICS-based model for notice and consent would be too complicated and frustrating for consumers, especially if they were continually required to reset their privacy preferences.[111] One panelist argued that this model would unjustifiably shift the burden from industry to consumers to take affirmative steps to protect their privacy.[112] A representative of the advertising industry opined that online privacy interactions could disrupt the substantive dialogue between marketer and customer (or potential customer). According to this panelist, the timing of such interactions would be critical.[113]

PICS proponents countered that any use of the Internet requires many affirmative steps and that the additional steps consumers would take to use PICS to express privacy-related choices would not be burdensome.[114] PICS, they argued, empowers individuals to express a broad range

---

[108] Harter 74; Hendricks 107; Rotenberg 137.

[109] IIA Comment at 12 (Doc. No. 23).

[110] Reid 91-93, 121.

[111] IIA Comment at 11-12 (Doc. No. 23).

[112] Rotenberg 99.

[113] Jaffe 104-05.

[114] Weitzner 114; Goldman 126.

of preferences and enables Web sites to respond to the variations.[115] Technology like PICS, which builds an information profile, works in the background and need not interrupt the communication between the user and a Web site.[116] According to one panelist, it would therefore seem possible to create a system in which users would set their privacy preferences once, and the question of compatibility of their privacy preferences and Web sites' privacy policies would be resolved automatically through communication between computers.[117]

Privacy advocates expressed the concern that PICS technology is valuable only where a consumer is interacting directly online with an entity seeking to use his or her personal information.[118] For this type of interaction, these participants agreed that PICS provides useful tools for enhancing notice and choice.[119] These panelists argued, however, that PICS does not address the online use of a consumer's personal information by entities with whom that consumer has had no direct relationship.[120] Yet the unauthorized collection and use of personal information by third parties is, in one participant's view, so common that it is "where the action is today on the Internet."[121] In such situations, it was argued, the government has a role to play in protecting individual privacy online.[122]

The extension of PICS technology to interactions between users and Web sites around notice and choice issues is currently a theoretical construct. An extended PICS regime will require a

---

[115] Weitzner 114-15.

[116] Vezza 109.

[117] Goldman 126-27.

[118] Smith 42-43; Rotenberg 99-100.

[119] Rotenberg 101-02.

[120] Smith 42-43; Rotenberg 99-100.

[121] Rotenberg 100. Indeed, one panelist asserted that credit reports, social security numbers, arrest records and unlisted telephone numbers are currently being sold online without the data subjects' knowledge. Smith 42.

[122] Rotenberg 102.

standard vocabulary for describing Web sites' information practices and for labeling Web sites.[123] A labeling vocabulary could be based upon existing rating systems or could be developed from new criteria.[124] Panelists speculated upon the feasibility of a regime in which Web sites labeled themselves. Several panelists argued that independent entities should label and rate Web sites,[125] but others doubted whether this was realistic, given the sheer number of Web sites and the difficulty in ascertaining Web sites' information practices.[126] Web site self-labeling, coupled with third party certification of label accuracy, was said to be a more efficient approach.[127]

Ultimately, there was considerable optimism that an online notice and choice regime based upon PICS technology is attainable. The online medium is continually evolving, and several participants suggested that it can be shaped to create electronic privacy protections in relatively short order, if industry, technologists, and privacy advocates work together to that end.[128] The result could be an online environment in which users could feel safe interacting with Web sites and could choose to reveal personal data where they felt it was in their interests to do so.[129]

---

[123] Reidenberg 111; Westin 117-18; Resnick Comment at 10 (Doc. No. 14). This would be especially true, if labeling is to be done by Web sites themselves. Resnick Comment at 10 (Doc. No. 14).

[124] Resnick Comment at 10 (Doc. No. 14).

[125] Golodner 120; Ek 125. See also Reidenberg 112. It is likely that many rating entities will be created. One recent effort is eTRUST, a project of the Electronic Frontier Foundation and CommerceNet, a non-profit association of banks, telecommunications companies, Internet service providers, online services and software developers. eTRUST is developing online privacy standards and a system for rating Web sites' privacy protections that will be communicated through licensed visual symbols. Developments in this effort are posted to eTRUST's Web site at http://www.eTRUST.org.

[126] Knight 124-25; Resnick Comment at 10 (Doc. No. 14).

[127] Reidenberg 133; Resnick Comment at 11 (Doc. No. 14). The role such certification authorities would play was analogized to that of accountants who certify that business' records conform to generally accepted accounting principles. Reidenberg 133.

[128] Resnick 88; Weitzner 95-96; Vezza 109; Berman 254.

[129] Resnick Comment at 11 (Doc. No. 14).

B. CONSUMER AND BUSINESS EDUCATION

Workshop panelists agreed that consumer and business education is an indispensable component of any strategy to protect consumer privacy online and ensure the growth of the online marketplace. As several panelists pointed out, consumers generally know little about the ways in which personal information can be used online.[130] They do not understand the potential risks of divulging personal information online, and they need guidance on how to protect that information from unauthorized use.[131] This is true for both new and seasoned users of the Internet.[132] Consumers also need to understand the trade-offs in order to make an informed decision to divulge personal information online.[133] Panelists noted that business must be educated about the importance of privacy protection to the growth of the online marketplace,[134] and that smaller businesses, in particular, must be shown the benefits to their enterprise of protecting the privacy of personal information.[135]

Several panelists stated that industry, consumer groups, and government all have a role to play in educating consumers and businesses about online privacy issues.[136] Such efforts should proceed on many fronts and in many media. Panelists urged that educational efforts be creative: they should take advantage of the interactive nature of the online marketplace and include fresh approaches. Computer companies, for example, could include point-of-sale materials with each new computer.[137] Panelists also urged that consumers be involved in education efforts and that

---

[130] Jaffe 36; Givens 231; Golodner 246; Smith 259; CDT Comment at 8 (Doc. No. 5).

[131] Golodner 246.

[132] Smith 259.

[133] Cole 265.

[134] Burrington 242-43; Strenio 255-56; Smith 259-60.

[135] Burrington 242-43; Strenio 256.

[136] Burrington 239, 242; Golodner 246-47; Strenio 255; Givens Comment at 3 (Doc. No. 9); IIA Comment at 14 (Doc. No. 23).

[137] Golodner 246; Strenio 255.

such efforts be directed toward the elderly, who are increasingly active on the Internet,[138] and toward young people.[139]

Several panelists noted that the power of new electronic technologies can be harnessed to further education efforts. Individual online entities can educate their visitors simply by disclosing their information practices electronically.[140] The Privacy Rights Clearinghouse, a non-profit consumer education and research program, provides guidance for protecting information privacy online, and interacts with consumers across the country through its site on the Internet.[141] In March 1995, ISA and the National Consumers League (NCL) launched Project OPEN (the Online Public Education Network) to educate consumers on important online issues, including privacy.[142] There was a suggestion that the Commission work with ISA, NCL, DMA and other interested parties to develop a model business curriculum on online privacy issues.[143] Efforts of this sort are a necessary complement to technological approaches to protecting information privacy online.[144]

C. PARTICIPANTS' VIEWS ON SELF-REGULATION AND GOVERNMENT'S ROLE

Throughout the first day of the Workshop, participants expressed differing views of the role

---

[138] Golodner 247.

[139] Id; Givens 234-35.

[140] See Givens 231-32; Burrington 242. World Wide Web sites operated by DMA, ISA and CDT currently disclose their information-gathering practices in this manner. Heatley 263; ISA Comment (Doc. No. 15, Attachment); Goldman 15-16. These sites are located at http://www.the-dma.org; http://www.isa.net; and http://www.cdt.org, respectively. Panelists asserted that interactive regimes for notice and consumer choice are useful in educating consumers about online privacy issues. Givens 231-32; Burrington 242.

[141] Givens Comment, Attachment at 1 (Doc No. 9). The Internet address is http://pwa.acusd.edu:80/~prc/. Privacy Rights Clearinghouse's Fact Sheet devoted to protecting individual privacy in cyberspace may be found at http://pwa.acusd.edu:80/~prc/fs/fs18-cyb.html.

[142] Burrington 241; ISA Comment at 2 (Doc. No. 15). Project OPEN's site on the World Wide Web is http://www.isa.net/project-open.

[143] Burrington 242.

[144] Burrington 239.

government should play in the area of online information privacy. Industry representatives and trade associations took the position that it would be both inappropriate and counterproductive to mandate particular privacy protections. According to these participants, regulation would stifle the creativity and innovation that have marked the development of interactive media to date,[145] could infringe important First Amendment rights,[146] and might force marketers off the Internet entirely.[147] Government should step back, it was argued, and permit industry to develop privacy protection models.[148]

According to these panelists, market pressures will define the best privacy protections,[149] as consumers increasingly make known their preferences regarding information privacy online.[150] In their view, it is critical that government permit the development of a healthy market in online privacy protections.[151] Moreover, according to several panelists, regulation is an insufficiently precise method of shaping information policy online. Given the rapid pace of technological development in interactive media, government regulations tied to particular technologies would quickly become obsolete.[152]

---

[145] CASIE Comment at 2 (Doc. No. 18); ISA Comment at 2 (Doc. No. 15). This view was echoed by the representative of the National Telecommunications and Information Administration, U.S. Department of Commerce. Wellbery 205.

[146] IIA Comment at 10 (Doc. No. 23).

[147] Krumholtz 38.

[148] Krause 46.

[149] IIA Comment at 5-6 (Doc. No. 23); Jaffe 36.

[150] Jaffe 36; Consumer Alert Comment at 4-5 (not paginated) (Doc. No. 13).

[151] Westin 40-41. See also Sherman 26-27.

[152] Poler 54; Ek 98; Cochetti 209; Vezza 227. Industry participants and some public interest groups generally viewed self-regulatory efforts as a necessary complement to technological innovations designed to enhance online information privacy. Reid 90; IIA Comment at 11 (Doc No. 23). See also Consumer Alert Comment at 5 (not paginated) (Doc. No. 13) (arguing that self regulation and market-driven technological innovation are efficient alternatives to regulation in this area). Participants noted that self-regulatory efforts developed for traditional marketing media are applicable to the online environment. Efforts are currently underway, for example, to adapt the DMA's Fair Information Practices Manual to take into account the unique qualities of

Panelists strongly disagreed about whether emerging technologies would obviate the need for governmental regulation to protect online privacy. ISA's representative saw PICS as an especially important alternative to government regulation in the global online marketplace. Regulation is limited by the geographic boundaries of the regulating jurisdiction; but PICS can operate globally to benefit both industry and consumers.[153] Privacy advocates argued that the technologies demonstrated during the Workshop are not a substitute for an enforceable code of fair information practices, and that they are not likely to flourish without government enforcement of privacy rights.[154] One panelist urged the Commission not to assume that these technologies can solve all abuses related to information privacy online.[155]

Panelists offered various opinions on the role the Commission should play in protecting individual privacy online. Some privacy advocates argued that the Commission should intervene promptly to protect online privacy. In their view, purely self-regulatory approaches to protecting privacy have failed.[156] Self-regulation will not be effective, according to these participants, unless regulation operates in the background to deter bad actors. Otherwise, companies that abide by self-regulatory guidelines will be at a competitive disadvantage.[157]

Some participants suggested that the Commission should undertake research on issues related to information privacy online. Several panelists urged, for example, that the Commission conduct focus groups with users of online services and with consumers generally, to obtain an

---

interactive media, including the Internet. Reid 91. Consumer choice mechanisms such as the DMA's Mail Preference Service, for example, could be expanded to the online environment, giving consumers the choice to "opt-out" of particular online uses of their personal information by participating member Web sites. Reid 91-92. One participant argued that the Mail Preference Service is ineffective, because it is voluntary. Givens Comment at 2 (Doc. No. 9).

[153] Ek 97-99.

[154] Rotenberg 137; Givens Comment at 1 (Doc. No. 9).

[155] Givens Comment at 1-2 (Doc. No. 9).

[156] See, e.g., Rotenberg 21; Hendricks 32. One panelist urged the Commission to establish standards against which self-regulatory efforts would be measured, and to impose time limits for compliance with those standards. In the absence of timely compliance, the Commission should impose a regulatory scheme. Givens Comment at 3 (Doc. No. 9).

[157] Rotenberg 23.

understanding of their expectations and experiences regarding online privacy and to assess issues such as consumers' willingness (or lack thereof) to divulge personal information in return for customized products and services.[158]

Finally, several panelists stated that the Commission has the authority to step in where online information collection and use are shown to be fraudulent or deceptive, in violation of the Federal Trade Commission Act.[159] Law enforcement was said to be appropriate where, for example, a company misrepresents the nature of its online information practices or fails to adhere to the practices it has announced.[160]

---

[158] Burrington 238; Golodner 245; Strenio 254-55. See Givens Comment at 3 (Doc. No. 9).

[159] Plesser 50; Sherman 51; Jaffe 104; Reidenberg 112; IIA Comment at 5, 8, 10 (Doc. No. 23).

[160] Jaffe 104; Reidenberg 112.

IV. CHILDREN AND PRIVACY ONLINE

The second morning of the Workshop was devoted to the particular issues presented by the online collection of information from and about children. Children are avid consumers, and represent a large and powerful segment of the marketplace. They spend billions of dollars a year, and influence the expenditure of billions more.[161] At the same time, children have generally been treated as a special, vulnerable group for public policy purposes.

During the Workshop, industry representatives were generally optimistic about the possibilities flowing from children's interaction with the Internet, but also recognized the potential for abuse. Consumer and privacy advocates focused on the special needs and vulnerabilities of children and the unique threats to their privacy posed by the online medium. This section of the report draws on both the Workshop record and a staff survey of Web sites targeted to children. It describes the traditional law and policy approach to children, the current state of online information collection from and about children, and the specific concerns and possible solutions that were identified during the Workshop.

A. TRADITIONAL LAW AND POLICY

In law and policy, children are usually treated as a special, vulnerable class. This status is premised on the belief that children lack the analytical abilities and judgment of adults.[162] It is evidenced by an array of federal and state laws, including those that ban sales of tobacco and

---

[161] One source has estimated that, in 1995, children ages 4 through 12 had a direct influence on $170 billion in sales of products and services, and indirectly influenced twice that amount. This figure is growing by about 20 percent each year. In the toy and game category alone, children spent $4.5 billion of their own money and directly influenced around $17 billion of their parents' purchases. (Figures reported to staff by Dr. James McNeal, a leading children's marketing expert at Texas A&M University.)

[162] The Commission Deception Policy Statement recognizes that children can be unfairly exploited due to their age and lack of experience. (Deception Policy Statement, appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 179 n.30 (1984), citing Ideal Toy, 64 F.T.C. 297, 310 (1964). The Commission's actions regarding the marketing of pay-per-call 900 services to children also recognizes children as a vulnerable group in the marketplace. See Audio Communications, Inc., 114 F.T.C. 414 (1991) (consent order); Teleline, Inc., 114 F.T.C. 399 (1991) (consent order); Phone Programs, Inc., 115 F.T.C. 977 (1992) (consent order); Fone Telecommunications, Inc., Docket No. C-3432, (June 14, 1993) (consent order).

alcohol to minors, prohibit child pornography, require parental consent for medical procedures,[163] and make contracts with children voidable.[164] In the specific arenas of marketing and privacy rights, moreover, several federal statutes and regulations recognize the need for special protections for children as well as the special role that parents have in implementing these protections.[165]

Marketers have traditionally employed a variety of methods to collect information from and about children, including contests, subscription forms, box tops, magazine surveys, and letters to publications.[166] While parents may be aware of the collection of such information, it is not clear

---

[163] Except in emergencies, parental consent continues to be required for nearly all types of medical care. See 59 Am. Jur. 2d Parent and Child § 48 (1987).

[164] The so-called infancy doctrine allows the minor to avoid or disaffirm contracts except where the goods or services contracted for are "necessaries," needed for a child's support. See 2 S. Williston, Williston on Contracts § 223 (3d ed. 1959) (disaffirmance cases) and 42 Am. Jur. 2d Infants §§ 58-68 (1987).

In addition, the Constitution has been interpreted as affording parents certain rights when it comes to child rearing. While no constitutional provision defines a parent's legal rights, the courts have emphasized the existence and constitutional context of parental rights. See, e.g., Ginsberg v. New York, 390 U.S. 629, 639 (1968) ("[C]onstitutional interpretation has consistently recognized that the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society").

[165] The Federal Educational Rights and Privacy Act of 1974 (FERPA), gives parents of minor students the right to inspect, correct, amend, and control the disclosure of information in education records. 20 U.S.C. § 1232g (1988). The Department of Health and Human Services Policy for Protection of Human Research requires parental/guardian written consent for all DHHS-funded research that involves children as subjects. 45 C.F.R. §§ 46.401-46.409 (1995). The Telephone Disclosure and Dispute Resolution Act of 1992 expressly prohibits advertising of pay-per-call (e.g., 900) services to children under 12 unless they are bona fide educational services. 15 U.S.C. § 5701 (Supp. IV 1992). The Children's Television Act of 1990, among other things, requires television stations and cable operators to limit the amount of advertising during children's television programming. 47 U.S.C. § 303a(b) (Supp. V 1994).

[166] A Consumers Union's 1990 study, "Selling America's Kids: Commercial Pressures on Kids of the 90's," describes a number of examples of offline marketing to children, including kids' clubs. The study indicates that such clubs sell membership lists to direct mail advertisers, and that the ad messages may come disguised as club benefits. Consumers Union Comment, Attachment (Doc. No. 30).

whether parents know how such information is being used and whether it is being sold to third parties when it is collected in traditional media.[167]

Industry groups have established various self-regulatory frameworks to promote responsible marketing aimed at children in traditional media.[168] Existing guidelines for children's advertising do not generally cover collection and use of information about children,[169] however, two recently proposed industry privacy guides do specifically address information practices as they relate to

---

[167] CME/Consumer Federation of America (CFA) Comment Appendix A-58 is a listing of 15 offline solicitations, all of which required a mailing (envelope and stamp), implying parental involvement and consent. Eleven of them also required a check or money order, a clear sign of parental agreement. CME/CFA cited these examples as demonstrating the norm in traditional media. CME/CFA Comment at 21-22 (Doc. No. 20) and Fise at 326-27.

Similarly, Professor Mary Culnan of the Georgetown University School of Business noted in a written comment that direct marketing to children is not a new phenomenon and listed some of the children's mailing lists that are currently available from commercial list brokers (Professor Mary J. Culnan Comment at 2 (Doc. No. 1).) She explained that responsible list brokers require sample mail pieces before selling or renting their lists, seed their lists with decoy names to ensure the list is not being used for other purposes, and do not provide access to individual names, reducing the risk to personal safety. Professor Culnan observed, however, that based on her research, it is unlikely that most parents were informed that the names of their children were to be disclosed or given an opportunity to object.

[168] In 1974, for example, the advertising industry established the Children's Advertising Review Unit of the Council of Better Business Bureaus (CARU). CARU's Guidelines recognize that children are less experienced than adults in evaluating advertising and making purchase decisions and are, therefore, more easily misled, and call upon advertisers to act accordingly. In addition to CARU's Guidelines, each of the major television networks has adopted guidelines that include provisions governing advertising to children. The networks screen for ads that over-glamorize, exaggerate, or misrepresent the characteristics or performance of products or services advertised to children. The network guides prohibit high pressure sales techniques, such as telling children to ask a parent to buy a product, and, like CARU guides, they also prohibit "host selling," use of personalities or characters both as program hosts and in ads placed within or immediately adjacent to the program.

[169] See, e.g., Guidelines for Personal Information Protection and Guidelines for Ethical Business Practice submitted by DMA as part of their comment for the Workshop record. DMA Comment (Doc. No 24). These guidelines are also included in Appendix C.

children.[170]

B. COLLECTING CHILDREN'S INFORMATION ONLINE

Although traditional offline media offer a useful reference for defining online privacy issues regarding children, the Internet makes it comparatively easy to collect information without any parental involvement or awareness.[171] Young children sitting at a computer terminal can easily disclose significant amounts of information about themselves and their families, or establish an ongoing relationship with someone thousands of miles away without a parent's knowledge.[172]

Several participants noted that the unique qualities of the Internet make it a particularly intrusive medium for children.[173] The medium capitalizes on "one to one marketing" and permits the site to develop a personal relationship with the user.[174] For example, with more detailed collection of data on a child, future e-mail solicitations may come from an animated character appearing on a child's computer screen, addressing him by name and urging him to purchase a specific product[175] -- perhaps the product over which the child lingered the last time he visited the site. The safeguards of traditional broadcast media, which bar "host selling" and require separation between program, editorial, and advertising, do not currently exist online.[176]

---

[170] The DMA and ISA have proposed a Joint Statement on Children's Marketing Issues. Doc. No. 2 [hereinafter "DMA and ISA's proposed Children's Marketing Statement"]. The Ingenius Group, consisting of Ingenius, I/PRO, and Yahoo, submitted its Self-Regulation Proposal for Children's Internet Industry. Ingenius Group Comment (Doc. No. 29). See Appendix C for copies of both proposals.

[171] Montgomery 307-8, 416.

[172] Lascoutx 342; See Appendix E, which describes a sampling of children's Web sites and the types of information collected online. In addition, one participant recited an incident where an adult had harvested his daughter's name from a chat room and sent her e-mail. Awerdick 429.

[173] Dr. Michael Brody of the American Academy of Child and Adolescent Psychiatry referred to the Batman Forever Web site in which a cartoon character asks kids to enter information about their family. Brody 345. See also Baecher 362; Blanke 357-58; Fise 326; Hendricks 411-13; Montgomery 416; Smith 348-49.

[174] Montgomery 334; O'Connell 319-21.

[175] Montgomery 336.

[176] Montgomery 306-7.

Industry representatives focused on the benefits to children of the Internet's interactive nature. Unlike traditional advertising media, the Internet facilitates interaction with users of their products and services much like conducting offline focus groups and offering consumers 800 numbers.[177] It was suggested that feedback from consumers via this two-way medium allows marketers to provide more personalized services.[178] Several industry representatives highlighted the benefits of information collection in designing entertaining and educational program content for the Internet, customizing the interaction to improve user experience, and providing useful information to help consumers find the best products or services at the best price.[179]

1. Current Practices

Staff surveyed numerous Internet sites targeted to children to determine how the industry is collecting and using online information.[180] Many of the sites sampled collected individually identifying information about visitors, including children. Staff discovered a variety of information collection techniques, including correspondence with fictitious characters, signing a site's "guest book," registering with the site for updates and information, and offers of incentives for completing surveys or polls. Other sites collect information in connection with contests, bulletin boards, chat rooms, pen-pal services ("keypals"), or to complete sales online. Some site operators informed staff that they use prizes or other incentives to encourage visitors to divulge their information.

The survey and Workshop also revealed a wide variety of uses of this information.[181] Many site operators gather information to determine the aggregate demographic profile of site users and

---

[177] Clark 294.

[178] O'Connell 319.

[179] O'Connell 320-21; Zimmermann 299-301; Jaffe 366-67; Ingenius Group Comment at 2-3,6-7 (not paginated) (Doc. No. 29); CEI Comment at 2 (Doc. No. 31.).

[180] For a detailed presentation of the results of this survey, see Appendix E. Downloaded pages from Web sites are on file at the Federal Trade Commission. Given the large and growing number of sites on the Web, it is difficult to determine how representative staff's survey sample is of the universe of Web sites.

[181] Staff also had informal discussions with a number of Web site operators about how they used information.

to evaluate and improve the site.[182] Operators also collect names and e-mail addresses to permit customization and visitor screening. This tracking facilitates multi-participant games, prize fulfillment, research experiments at multiple locations (e.g., at a consortium of schools), keypal programs, chat rooms, and bulletin boards, and can help to identify and screen site visitors.[183] Some site operators collect full names and postal addresses from all contestants so they can deliver prizes to winners. Others collect e-mail addresses but only contact winners to request their full name and address.[184] Sites also gather information for market research purposes.[185] Some sites used detailed questionnaires, soliciting information about visitors' ages, gender, geographic location, interests and preferences. Web operators asserted that, in general, such information is turned over to clients only as anonymous, aggregated data. Other sites collect e-mail addresses to facilitate information exchange and communication back to the child, establishing a more personal relationship. Sites collect shipping addresses, phone numbers and e-mail addresses to facilitate post-sale communication to determine consumer satisfaction.[186] Finally, although marketers assert they are not currently using data collected online for micro-targeting,[187] they maintain that they should be permitted to micro-target children.[188]

2. Concerns

The issues raised in discussing children and privacy online largely parallel those identified on the first day of the Workshop -- notice of, and control over, information collection and use; access to, and correction of, information; and security of information from unauthorized

---

[182] Clark 294; Zimmermann 299; Faley 322-23; DMA Comment at 6-7 (Doc. No. 24).

[183] Zimmerman 299; Clark 373. As an example, such screening allows the operator of a children's site to identify and prevent visits from adults or children who have behaved inappropriately.

[184] Appendix E n.7.

[185] Ek 304; Waters 406-7.

[186] O'Connell 322; DMA Comment at 4, 6-7 (Doc. 24).

[187] O'Connell 321-22.

[188] See Ingenius Group Comment at 6 (stating that " 'microtargeting' is preferable to the 'mass marketing' model that tosses every child into one big lump.") (not paginated) (Doc. No. 29). See also CEI Comment at 1-4 (not paginated) (Doc. No. 31).

access. At the same time, the discussion reflected that these concerns become more complicated when the Internet user is a child. The particular immediacy and attractiveness of the online medium for children and the ease with which parental knowledge and control can be circumvented was seen by some as contributing especially to the potential for abuse.

A consensus seemed to emerge among Workshop participants that: (1) children are a special audience; (2) information collection from children raises special concerns; (3) there is a need for some degree of notice to parents of Web sites' information practices; and (4) parents need to have some level of control over the collection of their children's information. As one industry participant observed, virtually all Workshop participants had essentially agreed that "Knowledge, Notice and No" are the paradigms to address information collection issues.[189] However, participants' views varied as to how and when to provide notice or obtain parental consent.

a. Parental Consent

Workshop participants voiced concern that online collection practices bypass parents, who have traditionally protected children from marketing abuses. A number of participants pointed out that children cannot meaningfully consent to release of personal information,[190] since, as one panelist observed, children possess neither the developmental capacity nor the moral judgment to determine whether it is appropriate to provide personal information to a third party.[191] This inability is often exacerbated when the child is offered an incentive for releasing personal information, or when the request to release information comes from a favored fictional character whom the child may regard as authoritative.[192] Participants argued, therefore, that information should not be collected without consent from parents, who have traditionally fulfilled a gatekeeping function with regard to information requests directed at their children:[193]

---

[189] Kamp 325.

[190] Weitzner 353, 361; Hendricks 355; Brody 344; Fise 327

[191] Brody 344-45; see also Brody Comment at 1, 2 (Doc. No. 27).

[192] Id.; Montgomery 333. Appendix E supports the observation that children often are provided with incentives for revealing personal information, whether it be entry into a contest, or the ability to engage in site activities.

[193] Fise 327; Montgomery 416; Rafel 422-23.

> As parents we are used to schools asking us for permission to do surveys with our children, asking us for permission to provide family life and human development education. We would never want our pediatricians or our public libraries or our government or our banks to ask our children for information in the kind of detail that we may be talking about asking children on these sites.[194]

Some child-targeted Web sites already contain notices about parental consent. One site, for example, warns: "But kids, before you register, remember that your online safety is really important to us. Make sure you don't give out personal information about yourself unless you first have your parent's permission."[195] More often, however, sites collecting information contain no such instruction,[196] and staff has identified only one site that ensures it has received parental consent before collecting information online.[197]

In addition to the basic question of whether parental consent ought to be obtained, panelists discussed the appropriate age for triggering parental consent, whether a visitor's age can be accurately determined, and whether parental consent can, in fact, be obtained and verified.

Child advocates would require parental consent for collection of information from children under the age of 16.[198] Other participants argued that teenage children have the right and need to control information themselves, and that, in any event, it is difficult for parents to supervise children meaningfully with regard to information flow once they are over the age of 13.[199] One organization suggested that parents are best able to determine the age at which their children are capable of independently engaging in activities online, noting that parental empowerment tools, such as those discussed in Section IV.C.1., provide a flexible and preferable alternative to age-

---

[194] Rafel 373; see also Culnan Comment at 1 (Doc. No. 1).

[195] Appendix E, Site 20.

[196] Appendix E, Site 13; Site 18.

[197] Stevens 313. This marketing research site recruits parents first, in order to obtain permission to interview their children. Id.

[198] CME/CFA Proposal at 1 (Doc. No.19).

[199] Westin 337-38.

based rules.[200]

Several participants noted that it is difficult to determine whether a site visitor is a child, let alone the child's age.[201] Child advocates countered that some sites appear, in light of their imagery and content, to be clearly targeted to children.[202] They also noted, however, and staff's research confirms, that many sites request visitors' ages.[203]

Finally, some participants contended that it may be difficult for sites to verify that they have, in fact, obtained parental consent.[204] One noted that, in the future, "digital signature" systems may serve as a consent mechanism,[205] while another suggested that verified certificates or encrypted identification could serve as parental consent mechanisms in the future.[206] Privacy advocates were concerned, however, that such mechanisms might require a central repository of names and ages, which would further compromise consumers' privacy.[207]

b. Notice

As noted in Section II.C.1., Workshop participants generally agree that Web sites should provide notice of their information practices, including the identity of the information collector, and how the information will be used.[208] While a few sites currently give notice, some panelists

---

[200] CDT Response to CME/CFA Proposal at 3 (Doc. No. 21).

[201] Westin 339; Weitzner 350; Jaffe 363.

[202] Montgomery 335. Some children's Web sites, however, may also attract a number of adult visitors.

[203] Montgomery 359. Many of the sites in Appendix E collect age, including sites 1, 5, 6, 8, 10, 11, 13, 16-21, 23, 25, 29, 35, and 36.

[204] Jaffe 363-64; CDT Response to CME/CFA Proposal at 4 (Doc. No. 21).

[205] CME/CFA Proposal at 7 n.11 (Doc. No. 19).

[206] Harter 310.

[207] Weitzner 350; Hendricks 356; CDT Comment at 25 (Doc. No. 5).

[208] DMA Comment at 6 (Doc. No. 6); CME/CFA Proposal at 4-5 (Doc. No. 19); CDT Response to CME/CFA Proposal at 2 (Doc. No. 21); CDT Additional Comments at 1-3 (not paginated) (Doc. No. 22); Ingenius Group Comment at 4 (not paginated) (Doc. No. 29).

found it to be inadequate,[209] and one participant argued that notice given directly to children younger than 12, "just doesn't mean anything."[210]

Notice of the identity of the information collector is not always simple. While most sites surveyed by staff identify their sponsor, others are operated by a Web developer or other agency, and, as a result, the identity of the entity for whom the site ultimately collects data may not be revealed. The copyright notice generally featured at the bottom of a site's first page, which identifies and provides a direct link to the Internet site of the Web developer, is often inconspicuous. One online service provider's privacy policy warns members that some of the services they may encounter are operated by independent entities that may not adhere to the provider's policies.[211]

The uses of the information being collected were rarely identified in the surveyed sites. Children, for example, may be unaware that they are providing information for marketing purposes, when the format of the site leads them to believe that they are simply playing a game or entering a contest. Even when parents supervise children at the computer and are aware that information is being collected, they are unlikely to be able to determine in what manner the information will be used. And while a minority of sites expressly describe the intended use of collected information,[212] this disclosure may be far from the page where information is collected.[213]

---

[209] Montgomery 336; CME/CFA Comment at 8-10 (Doc. No. 20); CDT Additional Comments at 1-2 (not paginated) (Doc. No. 22).

[210] Weitzner 361.

[211] AOL Comment, Attachment A at 10 (Doc. No. 17).

[212] See generally, the sites described in Appendix E. Site 12, for example, contains a statement, immediately below the collection vehicle, that "Guest book entries may be used for advertising purposes." Site 13, which requires full name and e-mail addresses, states that first and last names are used for internal purposes only and that registration is used to help them monitor the live online activities.

[213] One site, for example, states that information disclosed to the marketer "is ours to use without restriction" but the disclosure appears on a legal page unrelated to the collection page. Appendix E, Site 5. Another site that collects substantial children's information in connection with a keypal program states in a Business Statement located far from the collection page that it engages in market research, and that its Web site is designed to "facilitate our information-

Disclosure of children's information to third parties without parental notice and consent was also widely discussed. While a number of participants objected to this practice,[214] DMA stated that it did not know of any DMA members that currently provide data collected online to a third party,[215] and no marketer at the Workshop indicated that children's names were collected for the purpose of preparing mailing lists or selling the information to list brokers.

c. Access and Data Security

Workshop privacy advocates suggested that parents should have access to information collected about their children and the right to insist on its correction or deletion.[216] Sites in staff's survey do not generally provide that opportunity. One site staff reviewed contains a link to permit consumers to signal that the site delete their e-mail address from its mailing list.[217] Some sites will, upon a parent's request, delete information entered by a child, but sites do not typically provide notice of this fact. To the contrary, many have notices that "any information you provide becomes the property of [the site owner]."[218] Finally, it is often unclear where the data reside. When a site is operated by a Web developer or other agent on behalf of a marketer, both entities may have possession of the data. Although a marketer may honor the parent's request to delete a child's name and address from a mailing list, the Web developer may retain and continue to use the information.

Most of the discussion about unauthorized access to children's data,[219] and the need to protect data from loss or misuse, occurred in the context of general consumer privacy.[220] One participant stated that when collecting data from children, her firm secures that data from unauthorized or

---

gathering with children in this age group." Appendix E, Site 16.

[214] Blanke 417; Fise 405; Montgomery 416.

[215] DMA Comment at 7 (Doc. No. 24).

[216] Fise 405.

[217] Appendix E, Site 3.

[218] E.g., Appendix E, Site 18.

[219] CME/CFA Comment at 16 (Doc. No. 20).

[220] See Section II.C.3.

unintended access by other parties.[221] The DMA and ISA's proposed Children's Marketing Statement specifically included a provision calling on marketers to implement strict security measures to ensure against unauthorized access, alteration, or dissemination of children's data.[222]

C. PROTECTING CHILDREN'S INFORMATION ONLINE

1. Technological Responses

A number of software manufacturers participating in the second day of the Workshop demonstrated software designed to give parents the ability to monitor, filter, and prevent the disclosure of information by their children.[223] They demonstrated how their software, which initially had been designed to enable parents to block access to objectionable content, could be adapted to address privacy concerns.[224]

- Cyber Patrol allows parents to manage access, set time limits, and block access to inappropriate sites.[225] The new 3.0 version includes ChatGard, which permits parents to identify the information they do not want released, e.g., name, address, school, e-mail address.[226] AOL, CompuServe, and Prodigy initially provide Cyber Patrol to their members gratis; however, monthly updates are obtained through subscriptions.
- *PrivNet* allows users to block the creation of "cookies" by any site not specifically selected by the user.[227]

---

[221] Clark 296.

[222] DMA/ISA Comment at 2 (Doc. No. 2).

[223] Demonstrators included Microsystems Software Inc. (Cyber Patrol) at 375-76; PrivNet at 381; TROVE Investment Corporation (Net Nanny) at 383-84; New View, Inc. (Specs for Kids) at 391-92, and SafeSurf at 395-96. The demonstrators indicated that these programs are PICS compatible.

[224] A description of the filtering software is found in Appendix F.

[225] Getgood 376; Microsystems Software Inc. Comment (Doc. No. 16).

[226] Parents enter words or character strings onto a ChatGard list. Then, when the child types these words or characters, they are replaced by XXXX. All settings are password controlled so only the parent can make modifications. Microsystems Software Inc. Comment at 4. (Doc. No. 16).

[227] Howard 381-82.

- *Net Nanny* provides a complete audit trail of sites accessed. Parents can customize a dictionary of terms used to terminate particular applications, including terms that would prevent disclosure of confidential personal information.[228]
- *Specs for Kids* provides a database of sites rated and labeled for children. Children are blocked from accessing non-approved sites.[229] As of August 1996, Specs for Kids did not prevent a child from typing in personal information on an approved site.
- *SafeSurf* is a site rating system. Publishers voluntarily rate their own sites and ratings are verified.[230] SafeSurf has added an advertising category and has the capacity to add a privacy category in the future.

While all Workshop participants supported the continued development of technological solutions for privacy protection, there were a number of reservations about a technological fix to privacy concerns. Many of these concerns are outlined above in Part III. Some participants were skeptical of the possibility of adapting technological tools designed to protect children from objectionable content to the task of protecting children from objectional information practices.[231] Others, who generally support technological controls, believe they do not obviate the need to obtain valid parental consent before collecting information from children.[232] They noted that many technological solutions are essentially "opt-out" requirements that let marketers collect detailed personal information from children unless their parents take preventive action. They suggest instead an "opt-in" approach that would place the burden on the marketer to ensure receipt of parental approval before soliciting information from a child.[233] It was suggested that parents consent via postal mail until effective electronic "opt-in" mechanisms are developed.[234] Yet others were concerned that placing the burden on parents and technology may absolve Web

---

[228] Ross 384-89.

[229] Runge 392-95.

[230] Simpson 396-98.

[231] Montgomery 332.

[232] CME/CFA Proposal at 2 (Doc. No. 19); Blanke 417.

[233] Fise 327; Blanke 417.

[234] CME/CFA Proposal at 7 (Doc. No. 19).

sites from responsibility for their information practices.[235]

Other participants, including marketers, favored technological solutions.[236] Privacy advocates, moreover, noted that technological solutions, like a PICS privacy system and blocking technologies,[237] permit parents to control the flow of information without requiring them to divulge additional information for purposes of consent. Industry representatives, who support technological solutions,[238] indicated that laws and regulations will not reach many bad actors, let alone the international sector.[239] They asserted that technological solutions give parents control over dissemination of sensitive information in the online setting that they do not have when the child walks "out [the] front door into the real world."[240] Parents can control children's access to the Internet, track where children have traveled, and control information that comes into the home, as well as information that leaves it.[241] One participant characterized the options as "parental empowerment technologies," permitting parents to decide when their child is mature enough to exercise independent control over personal information.[242] Although participants recognized that the available technological tools are not self-executing and may not solve all of the Internet's privacy problems, they believe these tools may move this developing medium in the direction of better serving privacy goals.[243]

---

[235] Doug Blanke, of the Minnesota Attorney General's Office, praised the technological demonstrations and suggested that these technologies could be valuable tools to assist parents, but urged that the "default setting" should be to respect children's privacy from the outset, as proposed by CME/CFA. Blanke 417.

[236] Jaffe 365-68; Consumer Alert Comment at 4 (not paginated) (Doc. No. 13).

[237] Some online services, for example, have provided parents with free access to blocking software.

[238] Ek 304; Getgood 377-78; ISA Comment at 6 (Doc. No. 15).

[239] Ek 421-22.

[240] Id.

[241] Jaffe 327-30.

[242] CDT Comment at 24 (Doc. No. 5).

[243] Vezza 78; Ek 96-97, 371; Weitzner 353; Jaffe 365.

2. Self-Regulation

Industry participants voiced unanimous support for self-regulation, although their proposals are preliminary and vary substantially in the protections they would afford. Proposed guidelines or statements specifically addressing children's information practices were submitted by DMA, ISA, and the Ingenius Group.[244] CARU is also currently developing guidelines to address privacy for personal information about children.[245]

The DMA and ISA's proposed Children's Marketing Statement begins with a general request that Web marketers take into account the age, knowledge, sophistication, and maturity of children and be sensitive to parents' concerns about data collection. This broad principle is followed by a statement that marketers should support the ability of parents to limit the collection of such data for marketing purposes through notice and opt-out.[246] The Ingenius Group recommends that marketers request parental permission when seeking personal information about children, including e-mail and mailing address, but does not require that parental consent actually be obtained prior to collection.[247]

Industry statements also address notice of information practices and appropriate uses of such information. The DMA and ISA's proposed Children's Marketing Statement calls on marketers to indicate clearly that the information is being requested for marketing purposes and to implement strict security measures to ensure against unauthorized access, alteration, or dissemination of the data. It limits marketers' use of data collected from children in the course of their online activities to the "promotion, sale, and delivery of goods and services, the provision of all necessary customer services, the performance of market research and other appropriate marketing activities, in conjunction with support for the ability of parents to limit the collection

---

[244] This group comprises Ingenius, I/PRO and Yahoo. Ingenius Group Comment (Doc. No. 29).

[245] A compilation of guidelines for the Workshop record is provided in Appendix C.

[246] DMA and ISA's proposed Children's Marketing Statement (Doc. No. 2). See also Faley 401. This is consistent with CASIE's opt-out recommendation. CASIE Comment at 3 (not paginated) (Doc. No. 18).

[247] Ingenius Group Comment at 3 (1.3d)- 4 (guideline #2) (not paginated) (Doc. No. 29).

of such data."[248] The Ingenius Group argues that use of such information for purposes of micro-targeting of children is vital to the children's Internet industry.[249] It recommends that requests for children's personal information be accompanied by notice as to what information is being collected and the purposes for which it will be used.[250] Neither the DMA and ISA's proposed Children's Marketing Statement or the Ingenius Group proposal addresses consumer access to or correction of their information.

The DMA and ISA's proposed Children's Marketing Statement and the Ingenius Group proposal provide that approaches are needed that protect children without stifling the industry's opportunity to educate children and enable them to communicate with one another. The DMA and ISA's proposed Children's Marketing Statement urges parents to take advantage of available software tools to restrict their children's access to particular sites or to prevent them from disclosing personal information.[251] To assist parents in obtaining information about new technologies, the DMA Web site has created hyper-links to each of the parental control technologies' Web sites.[252]

Some Workshop participants expressed skepticism that self-regulatory guidelines would

---

[248] DMA and ISA's proposed Children's Marketing Statement at 2 (Doc. No. 2). The statement also raised other issues previously discussed in this report, such as how a marketer knows that the visitor to a site is a child without collecting information, and how the site actually obtains parental consent.

[249] Ingenius Group Comment at 6, (5.1-5.4) (not paginated) (Doc. No. 29). The Ingenius Group stated that micro-targeting is preferable to the mass marketing model and permits the industry to create the best possible user experience.

[250] In addition to the above information practices, the Ingenius Group comment recommended several other guidelines to protect children from "exploitation by online advertising and marketing": marketers should limit Internet posting to children's first name and last initial only, with age and geographic location optional (Guideline #1); advertising, marketing and promotions should be clearly indicated through text, sound, visual, or other cues (Guideline #3); links to advertisers' sites should also be clearly indicated (Guideline #4); and brand characters should not simultaneously appear as programming stars and product spokespersons (Guideline #5). Id. at 4-6.

[251] DMA and ISA's proposed Children's Marketing Statement (Doc. No. 2).

[252] Faley 401.

provide adequate protection for children's information. One participant suggested that, as Internet access becomes widespread, many children will be unsupervised; only a ban on collection of information can adequately safeguard them.[253] Another participant viewed such a ban as unwarranted, given the prevalence of offline collection. In this participant's view, a "children's fair information practices code," based on existing fair information practices, with some refinement for the online medium, would be sufficient to address online privacy.[254]

Industry proposals do not restrict anonymous or aggregate data collection. Several participants drew a distinction between clickstream data or other anonymous, aggregate data and personally identifiable information.[255] Because clickstream data collection occurs automatically at almost every Web site, is not generally identifiable, and is used typically for site development, participants argued that it need not be subject to notice or other protections warranted by the collection of personally identifiable data.[256] Several participants, however, stated that while aggregate, anonymous information may be less problematic, parents should still have a right to know what is collected and how it is used.[257]

CME and CFA argued that DMA/ISA's opt-out model does not provide a useful mechanism for preventing the unauthorized collection and tracking of information from children online.[258] CME and CFA believe that "parental consent should be obtained before the e-mail address is

---

[253] Brody 346.

[254] Westin 339-42. Professor Westin noted the existence of a very rich literature in the social sciences in psychology, sociology, psychiatry, and anthropology about children, parents, and privacy, and urged that privacy issues be considered within the existing framework of knowledge about child development and family relations. Rather than reinventing the privacy wheel, Westin spoke of adapting the children's standards that have evolved in other media as well as the fair information practices concepts used in the adult world to the children's online world.

[255] Waters 406-10; Ek 369-70; see also McGraw-Hill Home Interactive Comment at 2 (Doc. No. 28).

[256] Waters 406-10; see also CEI Comment at 1 (not paginated) (Doc. No. 31).

[257] Montgomery 416; Fise 404.

[258] They stated that the opt-out tradition, currently applied to stop mail and telephone solicitations, is ineffective for children, who do not have the cognitive skills to weigh the benefits and drawbacks of releasing personal information. CME/CFA Comment at 6-7 (Doc. No. 20).

captured in the first instance, regardless of whether or not that address will be rented, sold, or exchanged with a third party."[259]

CME and CFA also argued that industry's notice provisions are vague and fail to require adequate disclosure of information practices,[260] and that industry's definition of permissible uses of children's information is overbroad.[261] CME and CFA would limit marketers to the use(s) specifically disclosed in their disclosure notices and would require notice and parental consent for any additional uses.

CME and CFA oppose any communication from a marketer to a child by e-mail without parental consent, regardless of how the e-mail address is obtained.[262] Arguing that parental control is the norm in all other media, they posit that "no one would question the unethical nature of . . . marketers . . . going door-to-door to solicit information from children."[263] Several other participants shared CME and CFA's perspective.[264]

It is important to note that various industry groups, particularly CARU, are still developing their proposals for children's guidelines, and it is as yet uncertain how these developing

---

[259] Id. at n.16.

[260] CME/CFA Comment at 8-9 (Doc. No. 20). CME/CFA stated that both the DMA/ISA and CASIE notice provisions are inadequate, as they do not require full disclosure of all future information practices at the time of the initial collection. Id. and at 12-13.

[261] Id. at 9-10. See DMA/ISA provision regarding permissible uses quoted above. DMA and ISA's proposed Children's Marketing Statement at 2 (Doc. No.2).

[262] They contend that unsolicited e-mails unfairly take advantage of children's inability to comprehend the source and purpose of the communication. The child does not understand that the e-mail letter addressed to them from a spokescharacter is a targeted marketing solicitation and not simply a friendly letter. CME/CFA Comment at 10-11 (Doc. No. 20).

[263] Id. at 11, quoting Robert Ellis Smith, publisher of Privacy Journal.

[264] One Workshop participant stated that protecting children would require a "mix" of parental participation, consent, and control, as well as some government support and industry self-regulation. She rejected the notion that the burden rests solely with parents and the technology. Rafel 423. Another participant suggested the establishment of a "federal ombudsman" to protect children's privacy. In this participant's view, neither a self-regulatory approach or the technology will provide adequate protection. Sylvia Goodman Comment (Doc. No. 26).

guidelines will be implemented. In addition, further experience with online technologies may be needed to determine how they are being utilized and the level of privacy protection they provide for children's information. One participant urged that advertisers be given more time to work with CARU and with the developing technology toward a system of parental control of personally identifiable information.[265]

3. Consumer and Business Education

The business and consumer representatives at the Workshop agreed that everyone should be actively engaged in consumer education about privacy rights and practices involving children. It was suggested that government work with industry to inform consumers about the available technology.[266] Project OPEN, the educational program of the ISA and the National Consumers League, was cited as an example of a valuable consumer education effort regarding children online.[267] One participant suggested that the Commission develop Web sites for children to educate them about pitfalls of marketing and how to deal with information collection.[268] Another participant recommended that the Commission include Web site developers in any education efforts, since many of them are new to this medium and may be engaged in problematic practices simply because they are unaware of the privacy and security issues.[269]

---

[265] Petruccelli 418.

[266] IIA Comment at 13-14 (Doc. No. 23).

[267] ISA Comment attachments (Doc. No. 15). Currently, the Project OPEN Web site provides information on parental controls, tools for schools online, PICS, and its brochure "Child Safety on the Information Highway." (http://www.isa.net/project-open)

[268] Smith 349.

[269] Clarke 425-26.

4. Government's Role

While the interactive and advertising industries represented at the Workshop favored a self-regulatory approach to privacy issues, a coalition of children's advocacy organizations urged the Commission to adopt guidelines prohibiting deceptive and unfair data collection practices involving children.[270] CME and CFA jointly proposed government support for guidelines that would require full and effective disclosure to the parent concerning the nature and use of all information collected from children.[271] One participant opposed governmental regulation because the medium is so new, and children already have a very sophisticated view of advertising, its purposes and techniques.[272] Other participants reiterated that existing law enforcement agencies, federal and state, can already act in appropriate cases.[273]

5. Proposed Legislation

Congressman Edward J. Markey (D-MA) and Congressman Bob Franks (R-NJ) addressed the Workshop about information privacy legislation they introduced in the 104th Congress. (Copies of the bills are attached as Appendix D.) The Communications Privacy and Consumer Empowerment Act (H.R. 3685), sponsored by Rep. Markey, would have required the Commission and the Federal Communications Commission to examine the impact of new technologies on privacy rights and to engage in rulemaking as necessary to correct defects in consumers' privacy rights. The bill included a specific provision directing the Commission to determine whether parents do or can exercise privacy rights on behalf of their children. The Children's Privacy Protection and Parental Empowerment Act of 1996 (H.R. 3508), sponsored

---

[270] CME/CFA Comment cover letter at 1 (Doc. No. 19).

[271] Id. at 4 (Doc. No. 19); Fise 404-5. The recommendation defines a child as under age 16 and calls for the following protections: valid parental consent when personally identifiable information is collected; correction procedures for previously collected information; prevention of unauthorized further uses of the information; a disclosure notice that is easy to understand, compelling, and prominently displayed, in language appropriate for a child, and placed on the same page where collection or tracking of information occurs.

[272] CEI Comment at 2 (not paginated) (Doc. No. 31). CEI believes that while some consumers might find collection and sale of personal data to be disturbing, other consumers value the information they receive from "microtargeting" and so-called "junk mail" about products and potential savings opportunities.

[273] Kamp 324-25; Smith 347-48.

by Rep. Franks, would have addressed children's privacy in all media. In pertinent part, it prohibited the sale or purchase of personal information about children without parental consent; required list brokers and solicitors to disclose to parents, upon request, the source and content of personal information on file about their children and the names of persons or entities to whom they have distributed personal information; prohibited prisoners and convicted sex criminals from processing the personal information of children; prohibited any exchange of children's personal information that one has a reason to believe will be used to harm or abuse a child; preserved all common law privileges, and statutory and constitutional privacy rights; and provided for civil and criminal penalties, as well as a private cause of action.[274]

[274] The Subcommittee on Crime of the House Judiciary Committee held hearings on H.R. 3508 on September 12, 1996.

V. CONCLUSION

The Commission staff used this Workshop to explore the full range of views about privacy in the online marketplace. The informal format worked especially well to continue a dialogue that was both educational and helpful to all participants and the Commission staff.

The Workshop produced a rich factual record about the current collection and use of personal information online, the technology that exists to collect such information, and the still developing technological and self-regulatory initiatives to address online privacy concerns. It also prompted an extremely thoughtful discussion about self-regulation and the role of government in this new and rapidly evolving marketplace.

Workshop participants agreed that privacy is a significant concern in the new online environment. Consumers have concerns about the online collection of personal data generally, and those concerns are heightened when the collection and use of data is from and about children. Participants acknowledged that privacy concerns must be addressed if consumers are to have confidence in the online marketplace, and if it is to thrive.

The Workshop testimony also reflected broad areas of agreement on the necessary elements of effective consumer privacy protection online, namely, notice, choice, security and access. Workshop participants agreed that notice to consumers about information practices is essential, and that consumers should be able to exercise choice about whether and how their personal information is used. Further, participants agreed that security of personal information is crucial, and many agreed that consumers should have access to their information. Viewpoints varied considerably, however, on more specific issues of implementation, such as the form notice to consumers should take, how consumer choice is to be exercised, and when and how to obtain parental consent when information is collected from children.

Panelists disagreed about whether government regulation is needed, or whether the issues addressed at the Workshop, at least initially, should be addressed by self-regulatory efforts and emerging technologies. Industry participants presented a variety of self-regulatory proposals, some in the very early stages of development. Technology experts demonstrated a wide array of technology-based protections, a number of which already have entered the marketplace. Some participants asserted that self regulation and technological tools are sufficient to implement privacy protections. Others argued that although self-regulation and technology are useful tools, they have been and will remain inadequate in the absence of government regulation.

Events continue to unfold with respect to both emerging technologies and self-regulatory

initiatives. Staff therefore recommends that the Commission keep abreast of these developments by convening a follow-up workshop. The purpose of the workshop would be to educate the Commission about changes in the collection and use of personal information online since the last workshop, including technological advances and self-regulatory efforts. This updated information should assist the Commission in considering the implications of online privacy issues for its consumer protection mission.

VI. APPENDICES

APPENDIX A

WORKSHOP AGENDA

APPENDIX B

THE EUROPEAN UNION DIRECTIVE ON THE PROTECTION OF PERSONAL DATA

APPENDIX C

PRIVACY GUIDELINES AND PROPOSALS SUBMITTED FOR THE RECORD

APPENDIX D

LEGISLATION PROPOSED BY

CONGRESSMEN EDWARD MARKEY AND BOB FRANKS

APPENDIX E

STAFF SURVEY OF CHILD-ORIENTED COMMERCIAL WEB SITES

APPENDIX F

INTERNET FILTERING SOFTWARE

APPENDIX G

WORKSHOP PARTICIPANTS

APPENDIX H

INDEX OF COMMENTS FILED