



Federal Trade Commission Protecting America's

Consumers

IV. CHILDREN AND PRIVACY ONLINE

[\[BACK\]](#)[\[NEXT\]](#)

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 influence the expenditure of billions more.(1) At the same time, children have generally been treated as a special, vulnerable group for purposes.

During the Workshop, industry representatives were generally optimistic about the possibilities flowing from children's interaction with the but also recognized the potential for abuse. Consumer and privacy advocates focused on the special needs and vulnerabilities of children 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 Web sites targeted to children. It describes the traditional law and policy approach to children, the current state of online information collection 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 abilities and judgment of adults.(2) It is evidenced by an array of federal and state laws, including those that ban sales of tobacco and alcohol to minors, prohibit child pornography, require parental consent for medical procedures,(3) and make contracts with children voidable.(4) In arenas of marketing and privacy rights, moreover, several federal statutes and regulations recognize the need for special protections for well as the special role that parents have in implementing these protections.(5)

Marketers have traditionally employed a variety of methods to collect information from and about children, including contests, subscription box tops, magazine surveys, and letters to publications.(6) While parents may be aware of the collection of such information, it is not clear how parents know how such information is being used and whether it is being sold to third parties when it is collected in traditional media.(7)

Industry groups have established various self-regulatory frameworks to promote responsible marketing aimed at children in traditional media. Existing guidelines for children's advertising do not generally cover collection and use of information about children,(9) however, two recent proposed industry privacy guides do specifically address information practices as they relate to children.(10)

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 much easier to collect information without any parental involvement or awareness.(11) Young children sitting at a computer terminal can easily collect 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.(12)

Several participants noted that the unique qualities of the Internet make it a particularly intrusive medium for children.(13) The medium of "one to one marketing" and permits the site to develop a personal relationship with the user.(14) 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 and urging him to purchase a specific product(15) -- 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.(16)

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 number support. It was suggested that feedback from consumers via this two-way medium allows marketers to provide more personalized services.(18) Some industry representatives highlighted the benefits of information collection in designing entertaining and educational program content for children, customizing the interaction to improve user experience, and providing useful information to help consumers find the best products or services at the best price.(19)

1. Current Practices

Staff surveyed numerous Internet sites targeted to children to determine how the industry is collecting and using online information.(20) In 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, and 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.(21) Many site operators gather information to determine aggregate demographic profile of site users and to evaluate and improve the site.(22) Operators also collect names and e-mail addresses for 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.(23) Operators collect full names and postal addresses from all contestants so they can deliver prizes to winners. Others collect e-mail addresses only to contact winners to request their full name and address.(24) Sites also gather information for market research purposes.(25) Some sites collect detailed questionnaires, soliciting information about visitors' ages, gender, geographic location, interests and preferences. Web operators 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.(26) Finally, although marketers are not currently using data collected online for micro-targeting,(27) they maintain that they should be permitted to micro-target children.

2. Concerns

The issues raised in discussing children and privacy online largely parallel those identified on the first day of the Workshop -- notice of, access to, information collection and use; access to, and correction of, information; and security of information from unauthorized 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 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 some level of control over the collection of their children's information. As one industry participant observed, virtually all Workshop participants essentially agreed that "Knowledge, Notice and No" are the paradigms to address information collection issues.(29) However, participants 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,(30) since, as one panelist observed, children possess neither the developmental capacity nor the moral judgment to determine whether it is appropriate to release personal information to a third party.(31) 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.(32) 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.(33)

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 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.(34)

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 get your parent's permission."(35) More often, however, sites collecting information contain no such instruction,(36) and staff has identified one site that ensures it has received parental consent before collecting information online.(37)

In addition to the basic question of whether parental consent ought to be obtained, panelists discussed the appropriate age for triggering 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.(38) 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.(39) 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 to do so, as those discussed in Section IV.C.1., provide a flexible and preferable alternative to age-based rules.(40)

Several participants noted that it is difficult to determine whether a site visitor is a child, let alone the child's age.(41) Child advocates contend that some sites appear, in light of their imagery and content, to be clearly targeted to children.(42) They also noted, however, and staff's research confirms, that many sites request visitors' ages.(43)

Finally, some participants contended that it may be difficult for sites to verify that they have, in fact, obtained parental consent.(44) One participant in the future, "digital signature" systems may serve as a consent mechanism,(45) while another suggested that verified certificates or enhanced identification could serve as parental consent mechanisms in the future.(46) Privacy advocates were concerned, however, that such mechanisms might require a central repository of names and ages, which would further compromise consumers' privacy.(47)

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.(48) While a few sites currently give notice, some panelists found the notice inadequate,(49) and one participant argued that notice given directly to children younger than 12, "just doesn't mean anything."(50)

Notice of the identity of the information collector is not always simple. While most sites surveyed by staff identify their sponsor, others are 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. 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 developer, is often inconspicuous. One online service provider's privacy policy warns members that some of the services they may encounter operated by independent entities that may not adhere to the provider's policies.(51)

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,(52) this disclosure may be far from the page where information is collected.(53)

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,(54) DMA stated that it did not know of any DMA members that currently provide data collected online to a third party 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 inspect, correction or deletion.(56) 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.(57) 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]."(58) 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,(59) and the need to protect data from loss or misuse, occurred in the context of general consumer privacy.(60) One participant stated that when collecting data from children, her firm secures that data from unauthorized or unintended access by other parties.(61) The DMA and ISA's proposed Children's Marketing Statement specifically included a provision that requires marketers to implement strict security measures to ensure against unauthorized access, alteration, or dissemination of children's data.(62)

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.(63) 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.(64)

- Cyber Patrol allows parents to manage access, set time limits, and block access to inappropriate sites.(65) The new 3.0 version, ChatGard, which permits parents to identify the information they do not want released, e.g., name, address, school, e-mail address, 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.(67)
- *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.(68)
- *Specs for Kids* provides a database of sites rated and labeled for children. Children are blocked from accessing non-approved sites. 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.(70) *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 concerned about the possibility of adapting technological tools designed to protect children from objectionable content to the task of protecting children from objectionable information practices.(71) Others, who generally support technological controls, believe they do not obviate the need to obtain parental consent before collecting information from children.(72) 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 suggested 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.(73) It was suggested that parents consent via postal mail until effective electronic "opt-in" mechanisms are developed.(74)

Yet others were concerned that placing the burden on parents and technology may absolve Web sites from responsibility for their information practices.(75)

Other participants, including marketers, favored technological solutions.(76) Privacy advocates, moreover, noted that technological solutions

PICS privacy system and blocking technologies,(77) permit parents to control the flow of information without requiring them to divulge information for purposes of consent. Industry representatives, who support technological solutions,(78) indicated that laws and regulation reach many bad actors, let alone the international sector.(79) They asserted that technological solutions give parents control over disseminate sensitive information in the online setting that they do not have when the child walks "out [the] front door into the real world."(80) Parents 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.(81) One participant characterized the options as "parental empowerment technologies," permitting parents to control when their child is mature enough to exercise independent control over personal information.(82) 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 be a developing medium in the direction of better serving privacy goals.(83)

2. Self-Regulation

Industry participants voiced unanimous support for self-regulation, although their proposals are preliminary and vary substantially in the protection they would afford. Proposed guidelines or statements specifically addressing children's information practices were submitted by DMA, ISG, and the Ingenius Group.(84) CARU is also currently developing guidelines to address privacy for personal information about children.(85)

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 an opt-out.(86) 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.(87)

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 information collected from children in the course of their online activities to the "promotion, sale, and delivery of goods and services, the provision of necessary customer services, the performance of market research and other appropriate marketing activities, in conjunction with support of the ability of parents to limit the collection of such data."(88) The Ingenius Group argues that use of such information for purposes of micro-targeting children is vital to the children's Internet industry.(89) It recommends that requests for children's personal information be accompanied by notice of what information is being collected and the purposes for which it will be used.(90) 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 Web sites or to prevent them from disclosing personal information.(91) To assist parents in obtaining information about new technologies, the DMA has created hyper-links to each of the parental control technologies' Web sites.(92)

Some Workshop participants expressed skepticism that self-regulatory guidelines would 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 personal information can adequately safeguard them.(93) Another participant viewed such a ban as unwarranted, given the prevalence of offline communication. 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.(94)

Industry proposals do not restrict anonymous or aggregate data collection. Several participants drew a distinction between clickstream data and other anonymous, aggregate data and personally identifiable information.(95) Because clickstream data collection occurs automatically at every Web site, is not generally identifiable, and is used typically for site development, participants argued that it need not be subject to the same other protections warranted by the collection of personally identifiable data.(96) 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.(97)

CME and CFA argued that DMA/ISA's opt-out model does not provide a useful mechanism for preventing the unauthorized collection of personal information from children online.(98) CME and CFA believe that "parental consent should be obtained before the e-mail address is captured the first instance, regardless of whether or not that address will be rented, sold, or exchanged with a third party."(99)

CME and CFA also argued that industry's notice provisions are vague and fail to require adequate disclosure of information practices,(100) and that industry's definition of permissible uses of children's information is overbroad.(101) CME and CFA would limit marketers to the uses 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.(102) 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."(103) Several other participants shared CME and CFA's perspective.

It is important to note that various industry groups, particularly CARU, are still developing their proposals for children's guidelines, and it is uncertain how these developing 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.(105)

3. Consumer and Business Education

The business and consumer representatives at the Workshop agreed that everyone should be actively engaged in consumer education : privacy rights and practices involving children. It was suggested that government work with industry to inform consumers about the avail technology.(106) Project OPEN, the educational program of the ISA and the National Consumers League, was cited as an example of a consumer education effort regarding children online.(107) One participant suggested that the Commission develop Web sites for childre educate them about pitfalls of marketing and how to deal with information collection.(108) Another participant recommended that the Coi include Web site developers in any education efforts, since many of them are new to this medium and may be engaged in problematic p simply because they are unaware of the privacy and security issues.(109)

4. Government's Role

While the interactive and advertising industries represented at the Workshop favored a self-regulatory approach to privacy issues, a coal children's advocacy organizations urged the Commission to adopt guidelines prohibiting deceptive and unfair data collection practices in children.(110) CME and CFA jointly proposed government support for guidelines that would require full and effective disclosure to the pa concerning the nature and use of all information collected from children.(111) One participant opposed governmental regulation because medium is so new, and children already have a very sophisticated view of advertising, its purposes and techniques.(112) Other participa reiterated that existing law enforcement agencies, federal and state, can already act in appropriate cases.(113)

5. Proposed Legislation

Congressman Edward J. Markey (D-MA) and Congressman Bob Franks (R-NJ) addressed the Workshop about information privacy legis introduced in the 104th Congress. (Copies of the bills are attached as Appendix D.) The Communications Privacy and Consumer Empov Act (H.R. 3685), sponsored by Rep. Markey, would have required the Commission and the Federal Communications Commission to exa impact of new technologies on privacy rights and to engage in rulemaking as necessary to correct defects in consumers' privacy rights. 7 included a specific provision directing the Commission to determine whether parents do or can exercise privacy rights on behalf of their (The Children's Privacy Protection and Parental Empowerment Act of 1996 (H.R. 3508), sponsored by Rep. Franks, would have address children's privacy in all media. In pertinent part, it prohibited the sale or purchase of personal information about children without parental required list brokers and solicitors to disclose to parents, upon request, the source and content of personal information on file about their and the names of persons or entities to whom they have distributed personal information; prohibited prisoners and convicted sex crimina processing the personal information of children; prohibited any exchange of children's personal information that one has a reason to beli used to harm or abuse a child; preserved all common law privileges, and statutory and constitutional privacy rights; and provided for civil criminal penalties, as well as a private cause of action.(114)

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

2. The Commission Deception Policy Statement recognizes that children can be unfairly exploited due to their age and lack of experienc (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 The Commission's actions regarding the marketing of pay-per-call 900 services to children also recognizes children as a vulnerable gro marketplace. See Audio Communications, Inc., 114 F.T.C. 414 (1991) (consent order); Teletelne, Inc., 114 F.T.C. 399 (1991) (consent orde Programs, Inc., 115 F.T.C. 977 (1992) (consent order); Fone Telecommunications, Inc., Docket No. C-3432, (June 14, 1993) (consent or

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

4. 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 / Infants §§ 58-68 (1987).

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

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

6. A Consumers Union's 1990 study, "Selling America's Kids: Commercial Pressures on Kids of the 90's," describes a number of exampl offline marketing to children, including kids' clubs. The study indicates that such clubs sell membership lists to direct mail advertisers, an

ad messages may come disguised as club benefits. Consumers Union Comment, Attachment (Doc. No. 30).

7. CME/Consumer Federation of America (CFA) Comment Appendix A-58 is a listing of 15 offline solicitations, all of which required a mail envelope (envelope and stamp), implying parental involvement and consent. Eleven of them also required a check or money order, a clear sign of agreement. CME/CFA cited these examples as demonstrating the norm in traditional media. CME/CFA Comment at 21-22 (Doc. No. 20) 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 Culnan Comment at 2 (Doc. No. 1).) She explained that responsible list brokers require sample mail pieces before selling or renting 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 to personal safety. Professor Culnan observed, however, that based on her research, it is unlikely that most parents were informed that their children were to be disclosed or given an opportunity to object.

8. 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, 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 pressure sales techniques, such as telling children to ask a parent to buy a product, and, like CARU guides, they also prohibit "host sell" personalities or characters both as program hosts and in ads placed within or immediately adjacent to the program.

9. 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.

10. 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 the Children's Internet Industry. Ingenius Group Comment (Doc. No. 29). See Appendix C for copies of both proposals.

11. Montgomery 307-8, 416.

12. Lascoux 342; See Appendix E, which describes a sampling of children's Web sites and the types of information collected online. In one instance, one participant recited an incident where an adult had harvested his daughter's name from a chat room and sent her e-mail. Awerdick 42

13. Dr. Michael Brody of the American Academy of Child and Adolescent Psychiatry referred to the Batman Forever Web site in which a character asks kids to enter information about their family. Brody 345. See also Baecher 362; Blanke 357-58; Fise 326; Hendricks 411-12; Montgomery 416; Smith 348-49.

14. Montgomery 334; O'Connell 319-21.

15. Montgomery 336.

16. Montgomery 306-7.

17. Clark 294.

18. O'Connell 319.

19. 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 (Doc. No. 31.).

20. 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 universe of Web sites.

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

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

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

24. Appendix E n.7.

25. Ek 304; Waters 406-7.

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

27. O'Connell 321-22.

28. See Ingenius Group Comment at 6 (stating that " 'microtargeting' is preferable to the 'mass marketing' model that tosses every child big lump.") (not paginated) (Doc. No. 29). See also CEI Comment at 1-4 (not paginated) (Doc. No. 31).
29. Kamp 325.
30. Weitzner 353, 361; Hendricks 355; Brody 344; Fise 327
31. Brody 344-45; see also Brody Comment at 1, 2 (Doc. No. 27).
32. Id.; Montgomery 333. Appendix E supports the observation that children often are provided with incentives for revealing personal info whether it be entry into a contest, or the ability to engage in site activities.
33. Fise 327; Montgomery 416; Rafel 422-23.
34. Rafel 373; see also Culnan Comment at 1 (Doc. No. 1).
35. Appendix E, Site 20.
36. Appendix E, Site 13; Site 18.
37. Stevens 313. This marketing research site recruits parents first, in order to obtain permission to interview their children. Id.
38. CME/CFA Proposal at 1 (Doc. No.19).
39. Westin 337-38.
40. CDT Response to CME/CFA Proposal at 3 (Doc. No. 21).
41. Westin 339; Weitzner 350; Jaffe 363.
42. Montgomery 335. Some children's Web sites, however, may also attract a number of adult visitors.
43. 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.
44. Jaffe 363-64; CDT Response to CME/CFA Proposal at 4 (Doc. No. 21).
45. CME/CFA Proposal at 7 n.11 (Doc. No. 19).
46. Harter 310.
47. Weitzner 350; Hendricks 356; CDT Comment at 25 (Doc. No. 5).
48. 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) Additional Comments at 1-3 (not paginated) (Doc. No. 22); Ingenius Group Comment at 4 (not paginated) (Doc. No. 29).
49. Montgomery 336; CME/CFA Comment at 8-10 (Doc. No. 20); CDT Additional Comments at 1-2 (not paginated) (Doc. No. 22).
50. Weitzner 361.
51. AOL Comment, Attachment A at 10 (Doc. No. 17).
52. See generally, the sites described in Appendix E. Site 12, for example, contains a statement, immediately below the collection vehicle "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.
53. One site, for example, states that information disclosed to the marketer "is ours to use without restriction" but the disclosure appears on a page unrelated to the collection page. Appendix E, Site 5. Another site that collects substantial children's information in connection with a marketing program states in a Business Statement located far from the collection page that it engages in market research, and that its Web site is created to "facilitate our information-gathering with children in this age group." Appendix E, Site 16.
54. Blanke 417; Fise 405; Montgomery 416.
55. DMA Comment at 7 (Doc. No. 24).
56. Fise 405.
57. Appendix E, Site 3.
58. E.g., Appendix E, Site 18.
59. CME/CFA Comment at 16 (Doc. No. 20).

60. See Section II.C.3.
61. Clark 296.
62. DMA/ISA Comment at 2 (Doc. No. 2).
63. Demonstrators included Microsystems Software Inc. (Cyber Patrol) at 375-76; PrivNet at 381; TROVE Investment Corporation (Net 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.
64. A description of the filtering software is found in Appendix F.
65. Getgood 376; Microsystems Software Inc. Comment (Doc. No. 16).
66. Parents enter words or character strings onto a ChatGard list. Then, when the child types these words or characters, they are replaced with XXXX. All settings are password controlled so only the parent can make modifications. Microsystems Software Inc. Comment at 4. (Doc. No. 16).
67. Howard 381-82.
68. Ross 384-89.
69. Runge 392-95.
70. Simpson 396-98.
71. Montgomery 332.
72. CME/CFA Proposal at 2 (Doc. No. 19); Blanke 417.
73. Fise 327; Blanke 417.
74. CME/CFA Proposal at 7 (Doc. No. 19).
75. 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 in the CME/CFA. Blanke 417.
76. Jaffe 365-68; Consumer Alert Comment at 4 (not paginated) (Doc. No. 13).
77. Some online services, for example, have provided parents with free access to blocking software.
78. Ek 304; Getgood 377-78; ISA Comment at 6 (Doc. No. 15).
79. Ek 421-22.
80. Id.
81. Jaffe 327-30.
82. CDT Comment at 24 (Doc. No. 5).
83. Vezza 78; Ek 96-97, 371; Weitzner 353; Jaffe 365.
84. This group comprises Ingenius, I/PRO and Yahoo. Ingenius Group Comment (Doc. No. 29).
85. A compilation of guidelines for the Workshop record is provided in Appendix C.
86. 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).
87. Ingenius Group Comment at 3 (1.3d)- 4 (guideline #2) (not paginated) (Doc. No. 29).
88. DMA and ISA's proposed Children's Marketing Statement at 2 (Doc. No. 2). The statement also raised other issues previously discussed in the 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.
89. 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.
90. 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

geographic location optional (Guideline #1); advertising, marketing and promotions should be clearly indicated through text, sound, visual 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.

91. DMA and ISA's proposed Children's Marketing Statement (Doc. No. 2).

92. Faley 401.

93. Brody 346.

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

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

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

97. Montgomery 416; Fise 404.

98. 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).

99. Id. at n.16.

100. 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.

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

102. 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 spokesperson is a targeted marketing letter and not simply a friendly letter. CME/CFA Comment at 10-11 (Doc. No. 20).

103. Id. at 11, quoting Robert Ellis Smith, publisher of Privacy Journal.

104. One Workshop participant stated that protecting children would require a "mix" of parental participation, consent, and control, as well as government support and industry self-regulation. She rejected the notion that the burden rests solely with parents and the technology. R: 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).

105. Petruccelli 418.

106. IIA Comment at 13-14 (Doc. No. 23).

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

108. Smith 349.

109. Clarke 425-26.

110. CME/CFA Comment cover letter at 1 (Doc. No. 19).

111. 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 consent when personally identifiable information is collected; correction procedures for previously collected information; prevention of further uses of the information; a disclosure notice that is easy to understand, compelling, and prominently displayed, in language appropriate to the child, and placed on the same page where collection or tracking of information occurs.

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

113. Kamp 324-25; Smith 347-48.

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

[[BACK](#)][[NEXT](#)]

Last Modified: Monday, June 25, 2007