

THE EUROPEAN UNION DIRECTIVE ON THE PROTECTION OF PERSONAL DATA

On the first day of the Workshop, panelists discussed the implications of the European Union Directive on the Protection of Personal Data for the online marketplace in the United States.¹ The Directive was designed to harmonize European Union member states' laws governing the treatment of personal information. It will become effective in 1998. As Workshop participants noted, the Directive is forcing scrutiny of data privacy protection policies in both the public sector and private industry in this country.²

The Directive comprises a general framework³ of individual rights and information practices respecting the "processing"⁴ of "personal data," which the Directive defines as "any information relating to an identified or identifiable natural person."⁵ The Directive establishes a floor upon which member states may build enhanced information privacy protections.⁶ It requires that member states enact national legislation implementing its provisions.⁷

The Directive includes fair information practices developed in many countries, including the

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Eur. O.J. L281/31 (Nov. 23, 1995) [hereinafter "Directive"]. A copy of the Directive is included in this Appendix.

² CDT Comment at 29 (Doc. No. 5); Reidenberg 192.

³ Reidenberg Comment at 1-2 (Doc. No. 7).

⁴ "Processing" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Directive, Art. 2(b).

⁵ Directive, Art. 2(a).

⁶ Directive, Art. 5; CDT Comment at 26 (Doc. No. 5).

⁷ Directive, Arts. 5, 32.

United States, since the 1970's.⁸ It provides that the processing of personal data be "transparent," i.e., that data subjects be given notice of the processing of their personal information and an opportunity to make decisions about how their personal information is used.⁹

The Directive requires generally that, subject to limited exceptions, personal data may be processed only "if the data subject has unambiguously given his consent."¹⁰ It requires that, when personal data is to be collected from an individual, he or she must be informed of the identity of the "controller" of the data,¹¹ the purposes for which processing of the data is intended, and any other information that guarantees "fair processing" of the data.¹² Similar

⁸ CDT Comment at 27 (Doc. No. 5); Reidenberg Comment at 1 (Doc. No. 7).

⁹ Reidenberg 183-84. The Directive requires that personal data must be: (1) processed "fairly and lawfully;" (2) "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;" (3) "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;" (4) "accurate;" and (5) "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed." Directive, Art. 6.

Workshop participants debated the question of whether the Directive was intended to apply only to large, centralized data bases using mainframe computing technology, as was typical of the 1960's and 1970's. The IIA representative asserted that this was indeed the case. Cochetti 207-08. However, several other participants disagreed. Hendricks 223; Reidenberg 211-12; Rotenberg 210. One participant argued that the language of the Directive itself demonstrates that the Directive is "neither technology dependent nor system specific." Reidenberg Comment at 1 (Doc. No. 7). The Directive states that its protections "must not in effect depend on the techniques used [to process personal data]." Id. at 2 (citing Directive Explanatory Paragraphs 26-27). According to this panelist, the Directive's focus upon rules governing the "processing" of data and the "controller" of data, neither of which is defined in terms limited to a specific technology, is further support for this proposition. Id. (citing Directive Arts. 2(b) & (d), 6, 7, 10-12, 14).

¹⁰ Directive, Art. 7. The Directive prohibits the processing of personal data revealing the data subject's race, ethnicity, political, religious or philosophic beliefs, trade-union membership, health status or sexuality, absent the data subject's "explicit" consent, again subject to certain enumerated exceptions. Id., Art. 8.

¹¹ "Controller" is defined as the "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data" Directive, Art. 2(d).

¹² Directive, Art. 10.

protections apply where personal information about a data subject is not obtained directly from him or her.¹³

The Directive gives individuals a right of access to personal data that is subject to processing by the controller of that data, as well as the ability to correct inaccuracies or to erase or block personal data that is processed in a manner inconsistent with the Directive's standards.¹⁴ Under the Directive, the data subject has the right to object to the processing of personal data about him.¹⁵ Finally, the Directive requires member states to provide individuals with judicial remedies and a right to compensation for violations of their rights under the Directive.¹⁶

For the United States and other countries doing business with European Union member states, the critical provision of the Directive is Article 25, which governs the transfer of personal data to countries outside the European Union. Article 25 requires member states to permit the "transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer . . . only if . . . the third country in question ensures an adequate level of protection."¹⁷ This prohibition is subject to exceptions enumerated in Article 26, including an exception where the controller of the data demonstrates "adequate safeguards," such as appropriate contractual provisions, for protecting the privacy and fundamental rights of individuals.¹⁸

Under Article 25, the "adequacy" of non-member states' privacy protections is to be assessed

¹³ Directive, Art. 11.

¹⁴ Directive, Art. 12.

¹⁵ Directive, Art. 14. This includes the right either to object to the processing of personal data about him for direct marketing purposes or to be informed before the disclosure of personal data to third parties and to be expressly offered the right to object to such disclosures. Id., Art. 14(b).

¹⁶ Directive, Art. 22-23.

¹⁷ Directive, Art. 25 (1).

¹⁸ Directive, Art. 26(2). Under Article 26, member states may also permit the transfer of personal data to countries whose level of data protection is not deemed "adequate" where: the data subject has "unambiguously" consented to the proposed transfer; the transfer is necessary for the performance of a contract between the controller of the data and the data subject (or of a contract between the controller and a third party that benefits the data subject) or is necessary to protect the data subject's vital interests; the transfer is required to support a legal claim; or where the transfer is of data maintained in certain public records. Directive, Art. 26(1).

in light of the particulars of a proposed transfer of data (including the nature of the data, the purpose and duration of the proposed processing of that data, the country in which the data originates and the country to which it would finally be transferred) and "the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."¹⁹ Where, with respect to a particular proposed data transfer, a country is found not to have an "adequate" level of data protection, the Directive requires member states to prevent any transfer of the same type of data to the country in question.²⁰ The Directive provides only general guidance regarding the assessment of the "adequacy" of non-member states' privacy protections.

The task of further refining the definition of "adequacy" and developing a methodology for assessing "adequacy" has fallen to the Commission's Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, created by the Directive to, among other things, render an opinion on the level of data privacy protections in non-member states.²¹ "Adequacy" standards are currently being hotly debated by the European data protection commissioners serving as members of the Working Party.²² The unsettled nature of the "adequacy" standards is reflected in the divergent views of workshop participants regarding the impact the Directive may have on online data collection in, and international transfers of personal information to, the United States.

Participants offered varying perspectives on the question of whether existing data privacy protections in the United States satisfy the Directive's "adequacy" standard. One participant argued that U.S. privacy law is not "adequate," within the meaning of the Directive.²³ In this

¹⁹ Directive, Art. 25(2).

²⁰ Directive, Art. 25(4). The Directive empowers the European Commission to enter into negotiations with non-member states whose privacy protections have been deemed "inadequate," in order to derive international agreements that satisfy the Directive's data protection standards. Directive, Art. 25 (5-6).

²¹ Directive, Art. 29-30; Reidenberg Comment at 3, 4 n.14 (Doc. No. 7).

²² CDT Comment at 26 n.26 (Doc. No. 5); Reidenberg Comment at 3 (Doc. No. 7). In connection with its efforts to apply the Directive's framework of rights and responsibilities to specific contexts, the European Union has begun a study of data privacy protection as it relates to online services. Blatch at 217; Reidenberg Comment at 3 and 4 n.10 (citing Notice 96/C114/11, Eur. O.J. C114/11 (April 19, 1996)).

²³ Reidenberg 193.

participant's view, the absence of an overarching federal privacy statute will cause European Union member states to examine individual companies' information practices to measure compliance with the adequacy standard;²⁴ trade association guidelines will not, in and of themselves, suffice as indicia of "adequacy."²⁵ According to this panelist, three aspects of U.S. data protection will likely be problematic from a European perspective: the lack of "transparency" of information practices, *i.e.*, the difficulty that citizens face in trying to ascertain how their personal information is being used; the degree to which secondary uses of personal information are incompatible with the purposes for which the information was initially collected; and the piecemeal nature of oversight and enforcement of information practices.²⁶

Privacy advocates agreed that current information practices on the Internet would not meet the Directive's adequacy standard, because few online entities give individuals notice of their information practices or an opportunity to consent.²⁷ Industry representatives expressed the contrary view: the current mix in the United States of sector-specific statutory privacy protections and market-driven self-regulatory approaches satisfies the Directive's adequacy standard.²⁸ According to these participants, the United States Government has the duty to convince European Union member states that this is so.²⁹ One panelist opined that, at least with respect to protecting individuals from misuse of their personal information by the government,

²⁴ Reidenberg 195.

²⁵ *Id.* Another participant argued that there is nothing inherently new about having to comply with an "adequacy" standard such as the European Union's. Friend 188. American companies doing business internationally can conform their information practices to other countries' requirements, through (for example) employee training and contractual arrangements that limit the uses of information as required by both U.S. and foreign law. This will still be necessary after the Directive is implemented, because each member state's law will govern data flows between that country and the United States. Friend 189-91.

²⁶ Reidenberg 194-95.

²⁷ CDT Comment at 30-31 (Doc. No. 5). CDT stated that the Directive's core notice and consent standards could be satisfied by implementing emerging online technologies that make it possible for individuals to express their privacy preferences and for Web sites to disclose their information practices in a uniform format. *Id.* at 29-30.

²⁸ IIA Comment at 5-6, 13 (Doc. No. 23).

²⁹ *Id.* at 13.

U.S. privacy law is more protective than the Directive.³⁰

Participants discussed the merits of adopting the Directive's requirements in toto in this country. The Directive requires that member states create national "supervisory authorities" with investigatory powers to monitor compliance with national legislation implementing the Directive.³¹ Controllers of data are required to notify the supervisory authority before any automatic processing of data.³² Several participants expressed reservations about this registration requirement, on first amendment grounds.³³

Panelists disagreed about the need for an independent data protection agency in the United States. One participant argued that a central data protection office is needed, not only to centralize data protection policy at the federal level but also to give European Union member states a single entity with which to negotiate on data protection matters.³⁴ In the absence of such an entity, the burden falls upon individual U.S. businesses to demonstrate to member states that their information practices comply with the Directive.³⁵ Other participants questioned the need for an independent regulatory agency devoted to data protection, particularly in light of the uncertainties surrounding the European Union's interpretation of the adequacy standard.³⁶

³⁰ Plesser 199-200.

³¹ Directive Art. 28.

³² Directive, Art. 18.

³³ CDT Comment at 30 (Doc. No. 5); Plesser 202.

³⁴ Reidenberg 196-98.

³⁵ Reidenberg 196.

³⁶ Plesser 201; Wellbery 205-06.

STAFF SURVEY OF CHILD-ORIENTED COMMERCIAL WEB SITES

A. Methodology

This appendix is designed to provide a snapshot of information practices that children may encounter on the World Wide Web.³⁷ In June 1996, staff identified 272 sites from several lists of children's links.³⁸ Sixty-nine sites were not operational at the time. Of the remaining 203 sites accessed by staff, 67 appeared to have some commercial content or activity on some of the site pages. Staff then conducted a closer review of 29 of these commercial sites that were collecting information about the user. Staff also reviewed 8 additional children's sites already known by staff to be collecting information.³⁹ The following is a summary of the information collection practices of those 37 sites. Sample pages, downloaded between June and September 1996, are on file at the Federal Trade Commission.

B. Summary of Findings

Staff's survey identified a number of different techniques for collecting personal information from children on the Web. Some sites request visitor's name and postal and e-mail addresses to

³⁷ Given the vast scope of the World Wide Web, it would be difficult to conduct a comprehensive review of sites and site practices, or to determine whether practices are representative of a larger sample. Staff may not have accessed all the pages of each site, and sites may have undergone revision since pages were downloaded for this survey. Further, while each of the sites below appears to have some commercial content or purpose, it is not always clear whether the information practices identified occurred in connection with a commercial activity. Staff's review included sites doing commercial marketing research.

³⁸ Staff used the following lists of children's Web sites:
"4Kids Playroom" (<http://array.4kids.com/~4kids/kidplrm.html>);
"4Kids Entertainment" (<http://array.4kids.com/~4kids/kidentrtn.html>);
"KID List" (<http://www.clark.net/pub/journalism/kid.html>);
"Yahooligans" (<http://www.yahooligans.com/docs/cool.html>);
"Kids Connection" (<http://woi.com/woi/kids.html>); and
"World Kids" (<http://www.worldaccess.com/OtherSites/KidsCorner/>).

³⁹ In its site review, staff also accessed numerous children's sites that appear to be entirely noncommercial, but collect detailed information from children, *i.e.*, sites conducting online pen-pal programs and chat rooms for children that require registration to participate.

enable the child to correspond with fictional characters, to provide feedback regarding the site, or to receive information from the site, such as product information or notice of future site changes.⁴⁰ Some sites collect information by requesting visitors to sign a "guest book," register, or "join" a site. Such information often includes name, age, gender, e-mail and postal addresses, or phone number.⁴¹ A number of sites conducting surveys and polls collect name, e-mail and postal addresses, age, and gender.⁴² Sites conducting contests collect such information as name, birth date, e-mail and postal addresses, gender, or phone numbers.⁴³ Sites offering interactive features, such as bulletin boards and chat rooms, collect information including a participating visitor's name, e-mail address, age, or gender.⁴⁴ Online pen-pal services (keypals) collect especially detailed information regarding children's interests in addition to their names and birth dates.⁴⁵ Finally, sites that initiate or complete product sales online ask for information including e-mail and postal addresses, or phone number.⁴⁶

C. Information Practices by Site

The following is a brief description of the types of information collected at each of the 37 commercial sites included in staff's survey.

1. Aha Kids

www.aha-kids.com

- Requests name, age, e-mail address for bulletin board posting and for survey submission.
- Sells toys, games but order must be placed offline (800 number).

⁴⁰ E.g., sites 2, 3, 5, 14, 15, 21, and 30. Site 27 also asks for age or gender.

⁴¹ E.g., sites 4, 9, 12, 15, 21, 22, 31, and 36.

⁴² E.g., sites 5, 8, 11, 13, 17, 18, 19, and 20. Other information collected included age and gender of other household members, income and occupation (site 11), product preference (site 18), cereal eating preference (site 19), and interests (site 20).

⁴³ E.g., sites 6, 8, 13, 15, and 26. Site 6 also collected parent's name and e-mail address.

⁴⁴ E.g., sites 1, 6, 10, 13, 33, 34, 35, and 37. In addition, site 13 requested parent or guardian name and e-mail address, site 35 birth date, and site 37 preference information.

⁴⁵ E.g., sites 16 (nickname, birth date, current age, gender, favorite interests, hometown; and 20 (full name, birth date, gender, number in household, grade, favorite show, commercial and musical group, interests).

⁴⁶ E.g., sites 2, 7, 9, 10.

2. Atari Jag-Wire www.atari.com

- Requests postcard providing name, address, e-mail address for placement on mailing list for new product information.
- Sells products by e-mail if provide name, address, phone, e-mail address, credit card number.

3. Aunt Annie's Craft Page www.auntannie.com; www.outreach.com

- Requests name, e-mail address to be added to monthly mailing list of page updates; provides option to be removed from mailing list.
- Requests name, e-mail address, any other personal information persons wish to submit from those who submit craft ideas; provides option to indicate that name, e-mail address should not be published online.
- Provides option to order products (craft instructions) online by providing credit card information, e-mail address, or shipping address if diskette purchase is made.

4. Beakman and Jax www.nbn.com/youcan/index.html

- Visitors sign the Guest Book by providing first and last names, e-mail address, information re: favorite Web pages.

5. CBS www.cbs.com; concrete.onlinelabs.com

- Visitors wishing to vote in 1996 Family Film awards required to provide e-mail address, full name, full street address, birth date.
- Visitors wishing to send a message to CBS Kidzone requested to provide e-mail address.
- Visitors wishing to answer CBS Kidzone questionnaire re: "what's the best thing you did this summer?" requested to provide name or e-mail address and state.
- Visitors wishing to enter CBS Kidzone poll requested to provide e-mail address, gender, age, answer survey.
- Visitors wishing to be listed as a KidTriv winner requested to provide name, city/town, state and e-mail address.
- Legal disclosure link advises that any information disclosed to CBS "is ours to use without restriction."

6. CyberJacques www.cyberjaques.com

- Registration form to play game, participate in bulletin board requests full name, date of birth, gender, e-mail address, full street address, parent's full name and e-mail address.
- Site states that name and address of parent is requested "so we can let them know what you are up to," and that e-mail address of player is required so site can locate visitor, track eligibility for prizes. Another area of site states that information is requested so site can have a better idea of who visitors are, what they like, and to enable the site to reach visitors by phone or postal mail if e-mail is unavailable.

7. Discover Magazine www.eneews.com/magazines/discover/webtur.html

- Subscriptions may be purchased online if visitor provides name, e-mail address, phone number, street address, credit card number; separate page states that the Electronic Newsstand is not responsible for the confidentiality of credit card information provided over the Internet.
- Sells other merchandise offline (1-800 number).

8. Disney www.disney.com; game2.disney.com

- Site has a sign-in process for visitors wishing to participate in the numerous contests at the site. Sign-in form requests full name, e-mail address and states that visitors can get "free updates" by providing birth date, mailing address, and by indicating areas about which they would like to receive information.
- Some contests permit entry by submission on postcard of full name, mailing address, e-mail address, date of birth and daytime phone number.
- One survey permits entry by submission online of full name, mailing address, daytime phone number, age and survey responses.
- In June 1996, site advised that "information provided by our guests during the registration process is for internal Disney use only and will not be made available to third parties."
- In September 1996, site featured the following warning: "If you are under 18 years of age, Disney.com recommends that you get your parent or guardian's permission before you provide any information about yourself." In September, however, the site no longer contained a promise to limit information to internal use.
- Site also features contest rules and "Legal Restrictions" pages, but none state the use of information collected.
- Merchandise sold offline.

9. Dodoland www.swifty.com/azatlan/dojune/castle.htm

- Online request for visitors to provide e-mail and home address via postal service in order to obtain membership; need membership to access some portions of the site. As staff could not access entire site, it could not determine what additional information it collects.

10. ParentsPlace www.parentsplace.com

- Features chat rooms for adults and kids. To participate, visitors must register by providing full name, e-mail address, age, gender; also requests number and age of children. This sites states that it will not sell trade or exchange information provided and that information will be kept confidential.
- Sells magazine subscription online to those who provide name, e-mail, phone, and billing address.
- Features birthday club. To join, visitors must input name, e-mail address and birth date. Each day the site's birthday page prints out name and age of registered visitors celebrating birthdays.

11. Family Internet www.familyinternet.com

- Includes a survey that requests name, e-mail address, gender, age, age and gender of other household members, education, occupation, household income, and whether user has ever bought anything on Internet or is likely to do so.

12. 4Kids Treehouse array.4kids.com

- Provides option to sign the Guest Book by providing e-mail address, name, and "where [visitor is] calling from."
- Page states that "Guest book entries may be used for advertising purposes."

13. Freezone freezone.com

- Registration required for entry to interactive areas (chat rooms, bulletin boards, e-pals); registration requires first and last name;
- Additional information is optional: e-mail address, mailing address, phone, parent or guardian's name and e-mail address.
- Form states that the first and last name is used for internal use only and that registration is used to help monitor live activities.
- Site contains survey requesting predictions about future; entrants are requested to provide name, age, grade, and hometown.
Site also contains short story contest. Entrants must provide name, age, address and phone number on each page of the story.
Games, clothes, etc. sold offline.

14. FritoLay DreamSite www.dreamsite.fritolay.com

Collects name, e-mail address from correspondents via e-mail.

15. Hasbro (Actionman, GI Joe, etc.) www.actionman.com

- Collects name, comments, country for voluntary registration; discloses that "all agent dossiers [visitor files] are treated as high level security. No information submitted will be passed on."
- Collects first and last name and e-mail address of those wanting notice of when Hasbro Interactive Site is operational.
- To enter competition, visitor must provide name, e-mail address, postal address, gender, and answers to questions re: number of Actionman characters owned, and how many hours per week are spent online.

16. Internet for Kids www.internet-for-kids.com

- Collects nickname, birth date, age, gender, three greatest interests, hometown for online penpal service. This information is listed on the service for anyone who wants to correspond with persons listed.
- System's business statement makes reference to conduct of market research and states that its web site is designed to "facilitate our information-gathering with children in this age group."

17. Internet Movie Database us.imdb.com

- Contains Internet movie database survey, a lengthy survey of movie viewing habits and database use, and also seeking age, gender, country, zip code, name, e-mail address, industry of employment, job title.
- States that all personal data will be treated in confidence and used only for statistical purposes.
- States that there will be a prize awarded to survey entrants who provide e-mail address.

18. Jelly Belly

www.jellybelly.com

- Awards sample of jelly beans to survey entrants who provide full name, postal address, e-mail address, age range (including “11 and under”), gender, and information regarding jelly bean preferences. States that any information provided becomes property of product vendor.

19. Kellogg

www.kelloggs.com

- Visitors to various pages of Clubhouse and Store sections of site are asked a series of questions requesting the following information: full name, e-mail address, city and state, zip code, country, age, gender, cereal eating habits, and whether the child’s parents let them pick their own cereal.
- Students wanting information for a “school report” are requested to provide e-mail, name, postal address, and educational level.
- Those wishing to place orders for products (such as t-shirts) must provide full name and address, but orders are placed offline.
- Warns that those under 18 need parent permission to order.
- Those wishing to provide feedback are requested to provide full name, e-mail and postal address.
- Site includes opportunity to ask Kellogg’s to delete visitor’s e-mail address from the database.

20. Kidscom

www.kidscom.com

- Children wishing to use site must register by providing full name, birth date, gender, number in household, grade, favorite show, commercial and musical group, interests. Page states that registration gives access to the site, registers child for pen-pal list, and lets child talk to “the Internet Guru.” Children who have registered may then use entire site (including bulletin boards, games) and seek a penpal of a specified gender, age, country and having specified interests.
- One area of the site is a survey that requests full name, e-mail address, age, gender, country, and interests. Survey changes from time to time.
- Another area of the site advises parents that information collected from the surveys has on occasion been released on an aggregate, anonymous basis to third parties for market research purposes, but that personal identities are never released.
- Registration forms and survey forms advise children to get parental consent. Children are

awarded premiums for getting parents to fax a consent form to the site.

21. Lego www.lego.com

- Requests name, age, gender, computer type, e-mail address, and information regarding number of currently owned Lego products to get membership certificate, personalized homepage.
- States that if e-mail address is provided, Lego will provide “extra information” on Lego products. Immediately upon inputting e-mail address, the site sends back a membership number.

22. Magical Secrets www.magical.com/secrets/

- Collects name, e-mail address, postal address, phone numbers, stage name if applicable, and background in magic.
- Also sells magic products, publications online if visitor provides credit card number and expiration date.

23. Nabisco www.nabisco.com

- Collects e-mail address from those who wish updates or news on coupons.
- Can enter contest to win prizes by providing first and last names, postal address, age, type of computer system.

24. NBC www.nbc.com

- E-mail address required to play games and win prizes.
- States that site will use address only for a game and will not sell or rent the e-mail address to any third party.
- Sells merchandise offline.

25. Nintendo www.nintendo.com

- Contains questionnaire requesting name, postal address, e-mail address (“so we can send you information when something really cool comes out”), age, gender, location from which Web site is accessed (home, work, school), platform, views on additions to site. States that information is requested “so we can make our site better for you” and adds, “We even promise not to sell the information.”

26. Real Kids, Real Adventures www.realkids.com/adventur.htm

- Site promotes children's book series.
- Visitors wishing to enter drawing for t-shirt must send name, postal address, phone number. States that "Monthly entries are not saved once that month's winner is drawn, or used for mailing lists."
- Also requires visitors who wish to enter Young Writer's club to provide name, e-mail address.
- E-mail address is collected automatically when a button on the site is clicked. Visitor receives an automatic e-mail message ("Gotcha!") with the introduction, "You touched the button!"
- Provides information re: products, requires purchases be made offline.

27. The Scoop www.friend.ly.net/scoop/

- Site promotes children's books.
- Feedback form requests name, e-mail address, gender, type of books preferred, favorite children's book and author, views on how to improve site. States that information is collected to build better site and to give visitors an opportunity to win new books.
- Sells children's books offline.
- Includes a chat room.

28. Silly Billy's World www.sillybilly.com/

- Author's site.
- Requests visitors to provide name, postal address, e-mail, school system, city and state, and whether visitor is student, parent, teacher, administrator, or other.
- States that in future it will sell books, software, etc, online.

29. Splash Kids www.splash.com/

- Requests name, age, birthday, postal address and e-mail address.
- Request for address is accompanied by the following language: "optional--check with your parents first.") Also asks how visitor became aware of site, and their opinions about it.
- States that entrants will have a chance to win a monthly prize and receive newsletters.
- Site includes chat area.

30. Street Sharks wid.com/sharks/

- Visitors must provide name, e-mail address, city, and state to enter contest.
- Offers visitors opportunity to write to favorite Street Sharks character by providing name, e-mail address, city and state.

31. Syndicate.com syndicate.com/index.html

- Operates word puzzle contests and states that it will offer educational products.
- Requests that participants register by providing full name, e-mail address, postal address, phone number.
- Registrants are eligible for monthly drawings and can participate in all contests. To enter specific contests for monthly prizes, visitors must again enter e-mail address and real name.

32. Tap Online www.taponline.com/

- Registration required to use message boards, enter chat areas, enter contests for prizes. Visitors register by providing full name and e-mail address. Very fine print disclosure following contest entry form states that contestants must be 18 or older.

33. Teen Court TV www.courttv.com/teens

- Visitors wanting to provide feedback or suggestions for content of the site are requested to provide name, e-mail and postal addresses, and phone number.
- Visitors wishing to participate in teen chat area must register by providing full name and e-mail address.
- Sells licensed clothing offline.

34. The Kids.com

www.thekids.com/

- Full name and e-mail address required to participate in forum (discussion) rooms. Page requesting this information states that “this is solely for our internal use. Your personal data will under no circumstances be made available to any other company. . . .Your first and last name will show up in the forum message that you will post to identify those message [sic] as yours. . . Your e-mail address will not be made available to other forum members. It is for internal forum management only.”

35. TVNet

tvnet.com/TVnet.html

- Requires full name and e-mail address to register for chat areas; also requests locale and age group. States that the e-mail address will not be shown with name in chat areas but that if visitor acts inappropriately site will send an e-mail.

36. Yahoooligans Club

www.yahoooligans.com

- To join club visitors are requested to provide name, e-mail address, city, state, age, and gender. Registrants are also asked whether they share computer and with whom, whether Yahoooligans can send e-mail to address given, and what registrant does and does not like about site.
- States that those who join club will get advance update of new sites, notice of contests and special offers.
- Promises "we won't bury you in e-mail messages."
- (Note: pages downloaded in April, 1996.)

37. Youth Central

youthcentral.apple.com

- Site requires users wishing to access message boards to provide full name and e-mail address. States that it will terminate or suspend a participant's access if site rules are violated.
- Site also features opinion polls. One poll asks opinion of site, gender, year of birth, country of residence.
- Site features contests. Contest targets 10-19 year olds, states that by entering contest visitor acknowledges that he has his parent's or guardian's approval. To enter contest visitor must provide full name, parent's or guardian's name, postal address, e-mail address, and phone number.
- Site also features keypal service.

INTERNET FILTERING SOFTWARE

Overview

Software developers have responded to concerns about protecting children from objectionable content on the Internet by developing “filtering software” to enable parents and other supervising adults to set content and access preferences for children. Most filters currently act simply as content filters. Software companies are now working to add privacy preferences to their content filters. In the future, label-reading software could enable consumers to set their computers to access only those Internet sites whose privacy policies match their privacy preferences.

Content screening software uses either a filtering or rating method. The **filtering** method allows access to the Internet, but blocks the sites (or materials) that the software publisher defines as objectionable. Typically, the software recognizes a database of banned sites and search words. The database, however, requires regular updating, which may be at a cost to users through subscriptions. This design is not foolproof. It does not prevent a user from clicking on a link to a site that is not in the database, and it cannot stop a clever search that avoids the search words listed in the database.

The **rating** method blocks access to sites that do not bear a particular rating. The two currently operational rating systems are Recreational Software Advisory Council on the Internet (RSACi)⁴⁷ and SafeSurf⁴⁸. Rating programs identify a site’s HTML code and only those that

⁴⁷ The Recreational Software Advisory Council (RSAC), an organization initially formed by software publishing companies in 1994 to rate video game software for violence, adapted its rating system to the Web and expanded the categories to include ratings for the level of violence, sex, nudity, and offensive language. The RSAC asks Web sites to create ratings for their own pages by answering a questionnaire at the RSAC’s home page. After completing the questionnaire a PICS-compatible HTML tag is designated and the site can insert it into its pages. The tag is then added to the RSACi ratings system. The RSAC reserves the right to verify the accuracy of each rating. A number of the filters described in this Appendix support the RSACi ratings system, including Cyber Patrol, Microsoft Internet Explorer 3.0, Net Shepherd, and SurfWatch.

⁴⁸ SafeSurf was begun by a group of parents in 1995 to create a “child safe” environment on the Internet. Its Web site provides HTML tags that Web sites can use to rate their sites according to SafeSurf’s criteria.

contain the code with the rating are allowed through. Parents can, for example, restrict their children's access to sites that are rated as having no sexual material, foul language, or violence. This rating method uses the Platform for Internet Content Selection (PICS) specifications described in Section II of this Workshop report. SafeSurf and RSACi use the PICS format, but rely on Web sites to rate their own pages, while they reserve the right to verify each site's rating. Only a minority of existing Web sites is currently rated by these systems. Filtering software companies can add additional blocked sites to their databases on an ongoing basis. Rating systems, however, are largely relying on Web sites to insert rating labels on their sites, and sites have been slow to do so.

The explosive growth of the Internet makes it very difficult for software programs to completely monitor and control access to Internet sites. By the time a list of blocked sites is installed, thousands of new sites may have appeared. Moreover, since only a small percentage of existing sites has been reviewed, unreviewed Web sites are screened using search or trigger words or phrases. Objectionable sites, however, can still slip through the filters. For example, a new site may have a Web address that appears to be innocuous, but may in fact contain objectionable content. Until it is manually screened, it may not be filtered out. In addition, a site may contain explicit graphics alongside unrelated text, which cannot be detected even by software that filters full text as it appears on the screen. Foreign languages and unusual spellings may also bypass filter software. Conversely, unintentional blocking may occur, preventing access to harmless medical and historical data. Phrases with dual meanings or contexts can also cause unintentional blocking. For example, a site containing Hitler's name or the word "fascism" may be blocked because the filter screens for hate content. To some extent, if the software can be customized, some of these problems can be alleviated by allowing the supervising adult to adjust the software's lists.

The various filtering software products offer a wide range of features. The least complicated software simply maintains a list of Web site addresses and blocks user access to the sites on the list. Some products offer the option of using lists and employing PICS compliant rating systems as a backup filter. Many programs offer a monitoring option, which creates a record of where the user attempted to go and when. This can be either in addition to or as an alternative to blocking access. Programs may also shut down an application entirely or e-mail the "Administrator"⁴⁹ of

⁴⁹ This appendix uses the term "Administrator" to refer to the person who controls the implementation of the filtering software, *i.e.*, the parent, teacher or employer who installs and configures the software program.

an attempt to access a blocked site. Filtering can vary as well, from one-way, where only the incoming text is screened, or two-way, where what the user types in (ie., a computerized order form or e-mail) is also monitored. Two-way screening is useful to prevent the flow of personally identifiable information. Two-way screening occurs in conjunction with custom lists of blocked terms, including names, addresses, birth dates, and credit card numbers. Currently only four products, Cyber Patrol, Cybersitter, Net Nanny, and Specs for Kids, are able to prevent a child from sending out the blocked information. While some products are limited to interactions on the Internet, many give users the option to continue screening offline, in word processors, games, financial managers, and any other software on the computer.

Server-based filtering options, available more commonly for business use, install filters directly on the server of a system of computers (usually a Local Access Network). This option serves all computers directly attached to the network, as well as those connecting through a dial-up service by modem. Most filtering packages created for home use, however, are client-based, meaning software is installed directly by the user and is limited to their system, regardless of their mode of online connection (modem, LAN, etc.). While the difficulty of setup varies, all software packages are fairly simple. The actual installation, whether the software is downloaded from the Internet to the hard drive or by floppy disk, occurs in a matter of minutes. Configuration is more complicated, and the time needed is directly related to the complexity of the software. Those which offer customizable lists, multi-user options, PICS compliant lists, and other choices take longer to set up and master. Most instructions are clear, and technical support is readily available with each package, making it possible to get any software package up and running in a short period of time. Though prices vary, many home and school editions are available for free or at a low cost. Many server-based online services provide filtering software at no additional cost to their members.

Major Online Services

Each of the major online providers is increasing its efforts to create a safer environment for children using the Internet. America Online (AOL) offers parents a number of blocking options. Parents may limit their children's access to the "Kids Only" or the "Teens Only" areas, which consist of preselected entertainment and educational sites, as well as adult monitored chat and message areas. Users are kicked out of a chat room if the supervisor deems their language to be inappropriate. AOL's Member Profile, e-mail, and chat areas permit extensive collection of personal information. A parent may block a child from all chat rooms and Internet newsgroups on AOL. The option of presetting billing limits is also provided. AOL offers its members Cyber

Patrol, which is described below.

Prodigy provides parents with the option to control access to its individual bulletin boards, chat areas, or newsgroups. Parents can also block complete access to the Web for certain users. Prodigy offers kids and teen chat rooms, as well as special Web areas exclusively for children and teens. Prodigy also makes Cyber Patrol available to its members. Within Prodigy's chat rooms and public forums, users are prevented from posting items deemed unacceptable for children.

CompuServe offers parents the option of controlling which areas members of the family can enter by using passwords. No chat areas are available for children. Parents have the option of having e-mail sent to them first for screening before a child receives it. CompuServe also makes Cyber Patrol available to its members.

Microsoft's new browser, Internet Explorer 3.0, offers a built-in parental control feature. Through the "Ratings" options menu, the Administrator can select to block access to a site or single page based on a number of content categories, e.g. violence, nudity, and adult language. The default parental controls are based on the RSACi standards, but the Explorer will also support ratings from any organization that follows the PICS standard.

SUMMARY OF FILTERING SOFTWARE

SurfWatch

SurfWatch, by Spyglass Inc., screens for objectionable content (violence, hate crimes, drugs/alcohol and sex) on the Web and in chat rooms. SurfWatch screens using a list of objectionable Web addresses (updated monthly) and specific trigger words within an address. Unreviewed sites and those that do not contain the identified trigger words within their Web addresses may not be blocked. SurfWatch claims to block over 10,000 sites. SurfWatch does not work with the online services. The Administrator can independently update the SurfWatch lists or create his or her own inclusive or exclusive lists.

Cybersitter

Developed by Solid Oak Software, Cybersitter filters the Web, newsgroups, chat rooms, and e-mail and also offers the option of blocking offline applications, including games. It blocks sites related to adult themes such as sex, hate, violence, and drugs. Most importantly, Cybersitter addresses privacy issues by offering a custom blocking service, allowing a user to create a list of words and phrases that screen both incoming and outgoing information, in addition to the default restrictions. This can prevent the transfer of information such as credit card numbers and other personally identifiable information. Its "Advanced Phrase Definitions Capabilities" allows a user to offer sentence combination possibilities -- [I, we] live [at, on] [1234] [Main Street] to maximize the prevention of the transfer of such information. For additional blocking, a user can

choose to add the PICS standard rating systems, which are included in the package. The program does not block sites that have not been rated by one of the lists. A unique feature of Cybersitter is its "Intelligent Phrase Filtering" system, which looks at words in context to prevent accidental access or unnecessary blocking of phrases with multiple meanings. It also offers the option of logging the sites visited without actually blocking them.

Net Nanny

Trove Investment Corporation's Net Nanny emphasizes the parents' role in determining what is appropriate for their children, rather than the software company's determination. It offers a custom dictionary that is entirely defined by the Administrator. The Administrator can control transfer of personal information and credit card numbers. The Administrator can also control access to chat areas and Web sites, as well as to any program executable on both Windows and DOS, including all online services. To provide assistance, Net Nanny has created a sample dictionary list as a start-up point. Once the list is completed, the package screens both incoming and outgoing information. It also maintains a log of blocked sites and can display the frequency of each type of violation. On request, the Administrator can choose to have the system shut down after a pre-selected number of violations has occurred.

Cyber Patrol

Cyber Patrol, a Microsystems Software Inc. product, filters objectionable material on online services, the Web, and chat rooms and continues filtering offline software programs as long as the Internet connection is maintained. It works with either an exclusive "CyberNot" list or an inclusive, but more restrictive, "CyberYes" list. The Administrator can customize either list to include or exclude particular sites. The Administrator may also review a series of content categories and choose those that are appropriate for each user. Cyber Patrol is not able to filter new sites with unidentifiable addresses. It can filter by time of day or by total hours allowed. Upon request, the package can generate reports and charts of time usage. Cyber Patrol also addresses privacy concerns with its newly added "ChatGard." This feature enables the Administrator to block transfer of personally identifiable information using a custom list of words and phrases. When information from this list is typed in, "x" marks appear on screen instead. Cyber Patrol is now offered by AOL, CompuServe, and Microsoft's Internet Explorer. It is also PICS compatible and can read SafeSurf and RSACi ratings.

Net Shepherd

Net Shepherd, marketed by Net Shepherd Inc., enables the Administrator either to independently rate Web pages using an onscreen, point-and-click ratings bar or to screen sites using any of the PICS compliant rating systems, such as SafeSurf or RSACi. The Administrator can rate sites as "general," "child," "pre-teen," "teen," "adult" or prohibited. Net Shepherd can be configured to block unrated material or to create a list of selected sites. It is not designed to screen sites that do not bear ratings, and it only block sites on the Web and not newsgroups or chat rooms. Net Shepherd Inc. plans to extend the same rating and filtering capabilities to newsgroups.

Parental Guidance

Providence Systems markets Parental Guidance, which categorizes sites as “child,” “adolescent,” or “parent.” Parental Guidance has approved over 100,000 sites and offers the option of downloading approximately 20,000 new sites each month. The list of approved Web sites is provided by the McKinley Group, which publishes the McKinley Internet Directory. The program also enables the Administrator to restrict access to specific newsgroups and chat areas. While Parental Guidance does not directly target the collection of personal information, the Administrator may add sites to the McKinley list that he or she feels are inappropriate. Another product, Parental Guidance Plus, permits the Administrator to block a user’s access to offline programs, control the amount of time spent on the computer, and monitor its usage.

Specs for Kids

Newview, Inc.’s Specs for Kids creates an inclusive environment in which children can explore the Internet. The Specs for Kids home page includes a search tool and links to reference tools, news sources, entertainment, and other pages approved for children’s access. In addition, the Administrator can customize the software to create a dictionary of restricted words and phrases to override the default inclusive list. Administrators may choose between five different levels of restriction within 15 rating categories, including a whole range of adult topics. Specs for Kids is PICS compliant and has added such screening categories as credit cards and advertising, preventing the transfer of some personally identifiable information. One limitation of the program is that it does not prevent a child from transferring information on a site approved by Specs for Kids’ reviewers. Upcoming editions plan to support blocking of individual newsgroups and chat rooms and to include an encryption capability for all messages. Specs for Kids is not compatible with the online services.

InterGo Communications

TeacherSoft’s InterGo Communications is a filter and an Internet access package designed to appeal to adults and children. After installation, users view a “desktop” home page: a literal image of a desk from which point and click functions lead the user to various online functions. Included are e-mail, educational resources, and Internet search functions. Administrators can set up multiple users with individual settings, depending on age and preferences. InterGo’s “KinderGuard” system filters sites based on five levels ranging from EC (early childhood) to AO (adults only). In addition, SafeSurf ratings can be selected. InterGo screens out objectionable material from the Web, chat rooms, newsgroups, and mailing lists. The Administrator can customize the KinderGuard list by adding specific Web addresses to block; however, it cannot screen for words or phrases, thus limiting its ability to block the transfer of personal information. It also supports SafeSurf. Its “Cybrarian Search” feature is an Internet search tool that checks sites (including Web documents, reference materials, news and discussion groups) for offensive words and assigns a rating.

Bess

Bess is a server-based filter, which is available for online subscription. Subscribers dial into Bess and use the Bess browser. Bess offers links to preselected sites and blocks entire Web sites or individual pages, depending on the amount of inappropriate material. Access to selected newsgroups is an option, but chat areas are not accessible. Both incoming and outgoing e-mail are screened for inappropriate language. Bess offers the benefits of a continually updated service provided through the server and is resistant to tampering, since the controls are located at the server.

WORKSHOP PARTICIPANTS

Charlotte Baecher

Director of Education Services, Consumers Union

Jerry Berman

Executive Director, Center for Democracy and Technology

Doug Blanke

Minnesota Attorney General's Office
National Association of Attorneys General

Mari Ann Blatch

Consumer & Government Affairs Consultant, Reader's Digest

Dr. Michael Brody

American Academy of Child and Adolescent Psychiatry

William Burrington

Assistant General Counsel & Director of Public Policy
America Online, Inc.
Interactive Services Association
Chairman, Project OPEN (Online Public Education Network)

Trudie Bushey

Director, Legislative Affairs
TRW Information Systems & Services

Celeste A. Clark

Vice President, Kellogg Company

Roger Cochetti

Program Director, Policy & Business Planning, Internet Division
International Business Machines Corporation
Interactive Services Association

Steven J. Cole

Senior Vice President and General Counsel
Council of Better Business Bureaus, Inc.

Kawika Daguio

Federal Representative, Operations and Retail Banking
American Bankers Association

Mallory Duncan

Vice-President, General Counsel, National Retail Federation

Brian R. Ek

Vice President, Government Affairs, Prodigy Services Company
Interactive Services Association

Particia Faley

Vice President Consumer Affairs
Direct Marketing Association

Mary Ellen R. Fise

General Counsel, Consumer Federation of America

Kathleen Frawley

Director, Washington D.C. Office

American Health Information Management Association

Gary I. Friend

Vice President, Government Relations and Marketing

The Dun & Bradstreet Corporation

Susan J. Getgood

Director of Marketing, Microsystems Software, Inc. (Cyber Patrol)

Beth Givens

Project Director, Privacy Rights Clearinghouse

Center for Public Interest Law, University of San Diego

Janlori Goldman

Deputy Director, Center for Democracy and Technology

Linda Golodner

President, National Consumers League

Michael Hammer

American Marketing Association

Peter Harter

Public Policy Counsel, Netscape Communications Corporation

Connie Heatley

Senior Vice President, Public Relations / Communications

Direct Marketing Association

Evan Hendricks

Editor/Publisher, Privacy Times

James Howard

President, PrivNet, Inc.

Daniel L. Jaffe

Executive Vice President, Government Relations

Association of National Advertisers, Inc.

John Kamp

Senior Vice President, Washington Office

American Association of Advertising Agencies

Steven Knight

Tennessee Attorney General's Office

National Association of Attorneys General

Janet Koehler

Senior Manager, Electronic Commerce, AT&T Universal Card Services

Smart Card Forum

Marsha Kramarck

Delaware Attorney General's Office

National Association of Attorneys General

Katherine Krause

Senior Attorney, U S WEST, Inc.,
Chair, Privacy Committee, Information Industry Association

Jack Krumholtz

Interactive Services Association

Elizabeth Lascoux

Director, Children's Advertising Review Unit (CARU)

Lucy Lieberman

Magnet Studios

Scott McClellan

Director of Communications, Canadian Direct Marketing Association

Robert Merold

Vice President, IMS America, Ltd.

Kathryn Montgomery

President and Co-founder, Center for Media Education,

Bill Nielsen

Associate General Counsel, Kellogg Company

Gerald O'Connell

Managing Partner, Modem Media

Paul Petrucci

Senior Food and Drug Counsel, Kraft Foods
American Advertising Federation

Ronald Plessner

Piper & Marbury

Ariel Poler

Chairman and Founder, I/PRO (Internet Profiles Corporation)

Vicki Rafel

Member of the Board of Directors and Media Liaison
The National PTA

Pierce Reid

Product Manager 1, CompuServe
Direct Marketing Association

Joel Reidenberg

Associate Professor, Fordham University School of Law

Paul Resnick

Technical Staff, AT&T Research
Platform for Internet Content Selection

Gordon A. Ross

CEO & President, TROVE Investment Corporation & Net Nanny Ltd.

Marc Rotenberg

Director, Electronic Privacy Information Center

Chuck Runge

Vice President Business Development, New View Communications (Specs for Kids)

Shirley Sarna

New York Attorney General's Office

National Association of Attorneys General

Robert Sherman

Paul, Hastings, Janofsky & Walker,
General Counsel, Direct Marketing Association

Wendy Simpson

Co-founder and President, SafeSurf

Robert Ellis Smith

Editor, Privacy Journal

Craig Stevens

Director of Research, Digital Marketing Services, Inc

Andrew J. Strenio, Jr.

Hunton & Williams

Albert Veza

Associate Director, Laboratory for Computer Science, MIT
Chairman, World Wide Web Consortium

Jackie Ward

Maryland Attorney General's Office
National Association of Attorneys General

Bryan Waters

Vice President Technology and Production
McGraw-Hill Home Interactive

Daniel Weitzner

Deputy Director, Center for Democracy and Technology

Barbara Wellbery

Chief Counsel, National Telecommunications and Information Administration
U.S. Department of Commerce

Alan Westin

Professor of Law and Government, Columbia University
Publisher, Privacy & American Business

Victor Zimmermann

Ingenius

INDEX OF COMMENTS FILED

- 001 Professor Mary J. Culnan, Georgetown University, School of Business, "Consumer Privacy -- Comment: The Collection and Use of Information about Children"
- 002 Direct Marketing Association and Interactive Services Association, "Joint Statement on Children's Marketing Issues"
- 003 Direct Marketing Association and Interactive Services Association, "Principles for Unsolicited Marketing E-Mail"
- 004 Direct Marketing Association and Interactive Services Association, "Joint Statement on Online Notice and Opt-Out"
- 005 Center for Democracy and Technology, Jerry Berman, Janlori Goldman, Daniel J. Weitzner and Deirdre K. Mulligan, "Statement of the Center for Democracy and Technology"
- 006 Direct Marketing Association, "DMA Commentary -- FTC Workshop on Privacy and Cyberspace"
- 007 Professor Joel R. Reidenberg, Fordham University, "Consumer Privacy Comments"
- 008 Nynex, Bryan McGannon, "The Nynex Privacy Principles"
- 009 Privacy Rights Clearinghouse, Beth Givens, "Consumer Privacy on the Global Information Infrastructure"
- 010 Ram Avrahami, "My Life is not for Sale"
- 011 Privacy & American Business, "Interactive Services, Consumers, and Privacy: A National Survey"
- 012 Internet (I/PRO), Ariel Poler, "Consumer Privacy Comment"

- 013 Consumer Alert, "Comments to the Federal Trade Commission Re: Issues Discussed at the Public Workshop on Consumer Privacy on the Global Information Infrastructure"
- 014 PICS Technical Committee, Paul Resnick, "Privacy Applications of PICS: the Platform for Internet Content Selection"
- 015 Interactive Services Association, "Interactive Services Association Formal Comments in Connection with the FTC Workshop on Privacy and Cyberspace"
- 016 Microsystems Software, Susan J. Getgood, "Consumer Privacy -- Comments"
- 017 America Online, Inc., David W. Phillips, Comment Letter
- 018 Coalition for Advertising Supported Information & Entertainment (CASIE), Harold A. Shoup and Daniel L. Jaffe, "Goals for Privacy in Marketing on Interactive Media"
- 019 Center for Media Education/Consumer Federation of America, Kathryn Montgomery and Mary Ellen Fise, "Guidelines for the Collection and Tracking of Information from Children on the Global Information Infrastructure and in Interactive Media"
- 020 Center for Media Education/Consumer Federation of America, "Comments of Center for Media Education and Consumer Federation of America"
- 021 Center for Democracy and Technology, Janlori Goldman and Daniel J. Weitzner, "Comment on Joint Proposal of Center for Media Education and the Consumer Federation of America, 'Guideline for the Collection and Tracking of Information from Children on the Global Information Infrastructure and in Interactive Media'"
- 022 Center for Democracy and Technology, Janlori Goldman and Daniel J. Weitzner, "Additional

Comments on Notice and Individual Control in
Interactive Communications Media”

- 023 Information Industry Association (IIA), Alden Schacher, “Comments of the Information Industry Association”
- 024 Direct Marketing Association, Patricia Faley, “Additional Comments to the FTC -- Consumer Privacy in Cyberspace”
- 025 CompuServe, Russ Kennedy, “Summary of CompuServe’s Existing Written Privacy Policies”
- 026 Sally Goodman, Illinois Privacy Council, John Marshall Law School Center for Information and Privacy Law, Comment Letter
- 028 McGraw-Hill Home Interactive, Bryan Waters, Comment Letter
- 029 Ingenius, Internet Profiles Corporation, and Yahoo, “Self-Regulation Proposal for Children’s Internet Industry”
- 030 Consumers Union, Charlotte M. Baecher, “Selling America’s Kids -- Commercial Pressures on Kids of the 90's”
- 031 Competitive Enterprise Institute (CEI), Julie C. DeFalco, Comment Letter
- 032 Michael Brody, “Children in Cyberspace: Webs of Non-Consent”