REGULATORY ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: **July 2001** **NO: 01-RA-07**

TO: **All Federal Credit Unions**

SUBJECT: **Children's Online Privacy Protection Act (COPPA)**

ENCL:
(1) Federal Register – 16 CFR Part 312 – Children's Online Privacy Protection Rule; Final Rule
(2) How to Comply With The Children's Online Privacy Protection Rule[1]
(3) Frequently Asked Questions about the Children's Online Privacy Protection Rule[2]
(4) How to Protect Kids' Privacy Online[3]

The Children's Online Privacy Protection Act (COPPA) was signed into law on October 21, 1998. COPPA prohibits unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from and about children on the Internet. The Federal Trade Commission (FTC) issued the enclosed final rule, 16 CFR Part 312, effective April 21, 2000.

COPPA and the FTC's implementing rule generally apply to financial institutions that operate commercial websites or provide online services (or portions thereof) directed to, or knowingly collect personal information from, children under the age of 13.

COPPA and the FTC's rule require those financial institutions to:

- Provide parents notice of their information practices;
- Obtain prior verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions for the collection of "online contact information," e.g., an e-mail address);

[1] www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm
[2] www.ftc.gov/privacy/coppafaqs.htm
[3] www.ftc.gov/bcp/conline/pubs/online/kidsprivacy.htm

- Provide a parent, upon request, with the means to review the personal information collected from his/her child;

- Provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child;

- Limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and

- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

COPPA gives the NCUA authority to enforce compliance with COPPA for Federal credit unions. The FTC has authority to enforce compliance with COPPA for all other credit unions.

In addition to the final rule (Enclosure 1), enclosed are three documents from the FTC that should assist you in complying with COPPA. Enclosure 2 provides an overview of how to comply with the rule. Enclosure 3 contains a list of the most frequently asked questions about COPPA. Enclosure 4 is a summary of what web operators must do and what parents should do to protect a child's privacy online.

We encourage credit union officials and staff to review the requirements of COPPA and to evaluate the credit union's policies and procedures to ensure compliance.

Sincerely,

/s/

Dennis Dollar
Acting Chairman

Enclosures

Federal Register

Wednesday
November 3, 1999

Part III

Federal Trade Commission

16 CFR Part 312

Children's Online Privacy Protection Rule; Final Rule

FEDERAL TRADE COMMISSION

16 CFR Part 312

RIN 3084–AA84

Children's Online Privacy Protection Rule

AGENCY: Federal Trade Commission.

ACTION: Final rule.

SUMMARY: The Federal Trade Commission issues its final Rule pursuant to the Children's Online Privacy Protection Act of 1998 (''COPPA'' or ''the Act''). Section 6502 of the Act requires the Commission to enact rules governing the online collection of personal information from children under 13 within one year of the date of the enactment of the COPPA, October 21, 1998.

DATES: The rule will become effective on April 21, 2000.

ADDRESSES: Requests for copies of the Rule and the Statement of Basis and Purpose should be sent to Public Reference Branch, Room 130, Federal Trade Commission, 6th Street and Pennsylvania Avenue, N.W., Washington, D.C. 20580. Copies of these documents are also available at the Commission's website, <*www.ftc.gov*>.

FOR FURTHER INFORMATION CONTACT: Division of Advertising Practices: Toby Milgrom Levin (202) 326–3156, Loren G. Thompson (202) 326–2049, or Abbe Goldstein (202) 326–3423, Federal Trade Commission, 6th Street and Pennsylvania Avenue, N.W., Washington, D.C. 20580.

SUPPLEMENTARY INFORMATION: The Rule implements the requirements of the COPPA by requiring operators of websites or online services directed to children and operators of websites or online services who have actual knowledge that the person from whom they seek information is a child (1) to post prominent links on their websites to a notice of how they collect, use, and/or disclose personal information from children; (2) with certain exceptions, to notify parents that they wish to collect information from their children and obtain parental consent prior to collecting, using, and/or disclosing such information; (3) not to condition a child's participation in online activities on the provision of more personal information than is reasonably necessary to participate in the activity; (4) to allow parents the opportunity to review and/or have their children's information deleted from the operator's database and to prohibit further collection from the child; and (5) to establish procedures to protect the confidentiality, security, and integrity of personal information they collect from children. As directed by the COPPA, the Rule also provides a safe harbor for operators following Commission-approved self-regulatory guidelines.

Statement of Basis and Purpose

I. Introduction

Congress enacted the COPPA to prohibit unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from and about children on the Internet.[1]

Section 6502(b)(1) of the Act sets forth a series of general privacy protections to prevent unfair or deceptive online information collection from or about children, and directs the Commission to adopt regulations to implement those protections. The Act requires operators of websites directed to children and operators who knowingly collect personal information from children to: (1) Provide parents notice of their information practices; (2) obtain prior verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions for the collection of ''online contact information,'' *e.g.*, an e-mail address); (3) provide a parent, upon request, with the means to review the personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.[2]

The COPPA authorizes the Commission to bring enforcement actions for violations of the Rule in the same manner as for other rules defining unfair or deceptive acts or practices under section 5 of the Federal Trade Commission Act.[3] In addition, section 6504 of the COPPA authorizes state attorneys general to enforce compliance with the final Rule by filing actions in federal court after serving prior written notice upon the Commission when feasible.[4]

The Commission published a Notice of Proposed Rulemaking and Request for Public Comment (''NPR'') in the **Federal Register** on April 27, 1999,[5] and the 45-day comment period closed on June 11, 1999. The Commission received 132 comments from a wide array of interested parties, all of which were extremely informative and which the Commission has considered in crafting the final Rule. The commenters included private individuals; companies operating Internet sites or businesses; public interest organizations; marketing and advertising trade groups; library, school, and other educational organizations; Federal government entities; State Attorneys General; publishers and publishing trade groups; Internet service providers; and organizations sponsoring Internet privacy seal programs.

Because of particular interest among commenters in the issue of how to obtain verifiable parental consent under the Rule, Commission staff conducted a public workshop on that issue on July 20, 1999, to obtain additional information and learn more about the views expressed.[6] The 32 panelists at the workshop included representatives from industry (including website operators and technology companies), as well as privacy advocates, consumer groups, and representatives of other government agencies. Approximately 100 other parties also attended the workshop. Panelists discussed methods of obtaining verifiable parental consent that are currently in use; whether and how e-mail could be used to obtain verifiable parental consent; and technologies or methods that are under development that could be used in the future to obtain verifiable parental consent. Workshop attendees were invited to comment during question and answer sessions. The proceeding was transcribed, and the transcript was placed on the public record.[7] In addition, the Commission accepted further public comment on issues raised at the workshop. The workshop

[1] 15 U.S.C. 6501–6505.

[2] 15 U.S.C. 6502(b)(1).

[3] Section 6502(c) of the Act provides that the Rule shall be treated as a rule issued under § 18(a)(1)(B) of the FTC Act (15 U.S.C. 57a (a)(1)(B)).

[4] 15 U.S.C. 6504.

[5] 64 FR 22750 (Apr. 27, 1999) (to be codified at 16 CFR pt. 312).

[6] 64 FR 34595 (June 28, 1999) (announcement of the public workshop).

[7] The transcript and all of the comments received in the course of this proceeding appear on the FTC's website at <*www.ftc.gov*>. References to the workshop transcript are cited as ''Speaker/affiliation (Workshop Tr. at ____)'' followed by the appropriate page designation. Initial references to the comments are cited as ''Name of commenter (Comment or Workshop comment number) at (page number).''

comment period, which ended on July 30, 1999, yielded 14 comments.[8]

In drafting this final Rule, the Commission has taken very seriously the concerns expressed about maintaining children's access to the Internet, preserving the interactivity of the medium, and minimizing the potential burdens of compliance on companies, parents, and children. The Commission believes that the final Rule strikes the appropriate balance between these concerns and the Act's goals of protecting children's information in the online environment. It looks forward to continuing to work with industry, consumer groups, and parents to ensure widespread compliance in as efficient a manner as possible, to educate the public about online privacy protections, and to assess the Rule's effectiveness on a periodic basis.[9]

II. The Rule

As noted above, the Commission published the proposed Rule and accompanying analysis in the **Federal Register** in April 1999. Unless specifically modified herein, all of the analysis accompanying the proposed Rule in the NPR is adopted and incorporated into this Statement of Basis and Purpose for the final Rule.

A. Section 312.2: Definitions

Section 312.2 of the proposed Rule included definitions of a number of key terms.[10] The Commission sought comment as to whether these definitions were clear, comprehensive, flexible, and appropriate.[11] In the Rule, the Commission has modified the definitions of four of these terms: ''collects or collection,'' ''disclosure,'' ''personal information,'' and ''third party.'' All other definitions have been adopted without change.

1. Definition of ''Child''

In the proposed Rule, the Commission adopted the statutory definition of ''child'' as ''an individual under the age of 13.''[12] The Commission received only one comment on this issue, which supported the definition.[13] Thus, the final Rule retains the statutory definition.

2. Definition of ''Collects or Collection''

The proposed Rule defined ''collects or collection'' to include ''the direct or passive gathering of any personal information from a child by any means, including but not limited to: (a) [a]ny online request for personal information by the operator regardless of how that personal information is transmitted to the operator; (b) [c]ollection using a chat room, message board, or other public posting of such information on a website or online service; or (c) [p]assive tracking or use of any identifying code linked to an individual, such as a cookie.''[14] The term was meant to encompass the many ways that website operators could gather information from children.

Responsive comments contended that subparagraph (a) swept within the proposed Rule information requested online but submitted offline that was clearly meant to be excluded under the COPPA.[15] These comments also noted that it would be burdensome to require a business that solicits the same information from children in a number of ways, including through the Internet, to determine the source of the request in order to provide the required parental notice and seek consent for information submitted online.

The Commission is persuaded that the Congress intended the COPPA to apply only to information collected online by an operator. Therefore, based on the written comments, subparagraph (a) of the definition of collects or collection has been modified to cover any request by the operator that children submit information online.[16]

Other commenters were concerned that including public postings in the definition of ''collects or collection'' would confer liability on operators of general audience (*i.e.*, non-child-directed) chat sites for unsolicited postings by children.[17] The Commission believes that these concerns are legitimate, and therefore the Rule now provides that such sites would only be liable if they (1) have actual knowledge that postings are being made by a child under 13, and (2) when they have such knowledge, fail to delete any personal information before it is made public, and also to delete it from their records.

For general audience sites, the Act explicitly covers operators who have *actual knowledge* that they are collecting personal information from children.[18] Therefore, the operator of a general audience chat site who has actual knowledge that a child is posting personal information on the site must provide notice and obtain verifiable parental consent if the child is to continue to post such information in that site's chat room.[19] In most cases, if the operator does not monitor the chat room, the operator likely will not have the requisite knowledge under the Act. However, where the operator does monitor the chat room, the Commission has amended the Rule so that, if the operator strips any posting of individually identifiable information before it is made public (and deletes it from the operator's records), that operator will not be deemed to have collected the child's personal information.[20]

One group of commenters stated that requiring operators to get parental consent in order for a child to participate in a chat room would violate the child's First Amendment right to free speech.[21] These commenters also

---

[8] On July 27, 1999, the Commission also issued an Initial Regulatory Flexibility Analysis (''IRFA'') under the Regulatory Flexibility Act, 64 FR 40525. The IRFA focused on the impact of the proposed Rule on small businesses and sought additional public comment on that issue. This final comment period closed on August 6, 1999. Five comments were received. These comments are cited as ''Name of commenter (IRFA comment number) at (page number).''

[9] Shortly after issuing this final Rule, the Commission plans to develop and distribute educational materials to assist businesses in complying with the Rule and to inform parents of the protections provided by the COPPA.

[10] 64 FR at 22751–53, 22763–64.

[11] 64 FR at 22761.

[12] COPPA, 15 U.S.C. 6501(1). *See* 64 FR at 22751, 22763.

[13] American Psychological Association (''APA'') (Comment 106) at 1.

[14] 64 FR at 22751, 22763.

[15] *See generally,* Direct Marketing Ass'n (''DMA'') (Comment 89) at 31–32; Kraft Foods, Inc. (''Kraft'') (Comment 67) at 2–3; Council of Better Business Bureaus, Inc. (''CBBB'') (Comment 91) at 4; Viacom, Inc. (''Viacom'') (Comment 79) at 4–5; Time Warner, Inc. (''Time Warner'') (Comment 78) at 6–7; Magazine Publishers of America (''MPA'') (Comment 113) at 2. These comments pointed out that the COPPA covers the collection of personal information, which is defined in the statute as ''individually identifiable information about an individual collected online. * * *'' 15 U.S.C. 6501(8). Commenters also noted that the Floor Statement accompanying the Act states ''[t]his is an online children's privacy bill, and its reach is limited to information collected online from a child.'' 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (Statement of Sen. Bryan).

[16] If, however, an operator combines in one database information collected offline with information collected online such that the operator cannot determine the source of the information, the operator will be required to disclose all of that data in response to a parent's request under section 312.6 of the Rule. *See* Section II.E, *infra.*

[17] ZapMe! Corp. (''ZapMe!'') (Comment 76) at 7; Talk City, Inc. (''Talk City'') (Comment 110) at 2. *See also* Promotion Marketing Ass'n. (''PMA'') (Comment 107) at 3.

[18] 15 U.S.C. 6502(a)(1). *See also* Rule section 312.3.

[19] Operators of sites directed to children that provide chat rooms and bulletin boards and who do not delete personally identifiable information from postings before they are made public must always provide notice and obtain parental consent as provided by the Rule.

[20] This amendment applies both to operators of websites directed to children and to websites with actual knowledge that information is being collected from a child. Because an operator who deletes such information will not be deemed to have ''collected'' it, that operator also will not have ''disclosed'' that information under the Rule.

[21] Center for Democracy and Technology, American Civil Liberties Union, American Library

Continued

asserted that the Commission's proposal went beyond what Congress intended with this legislation.[22] Congress, however, specifically included such postings in the COPPA on the grounds that children could be placed at risk in such fora, noting that one of the Act's goals was ''to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information.'' [23] As noted in the Commission's June 1998 report to Congress, children's use of chat rooms and bulletin boards that are accessible to all online users present the most serious safety risks, because it enables them to communicate freely with strangers.[24] Indeed, an investigation conducted by the FBI and the Justice Department revealed that these services are quickly becoming the most common resources used by predators for identifying and contacting children.[25] Commenters also generally acknowledged that these are among the most sensitive online activities.[26]

Several commenters expressed concerns that the proposed Rule would similarly require operators to give notice and obtain parental consent in order to give a child an e-mail account.[27] The Commission notes that, to the extent that operators who provide e-mail accounts keep records of the e-mail addresses they have assigned, along with any associated information, those operators can be considered to have ''collected'' those e-mail addresses under the Act. Operators of sites directed to children are therefore required to comply with the Act when giving children e-mail accounts. For operators of general audience sites, the Rule requires *actual knowledge* that information is being collected from a child. Such operators would only be required to provide notice and obtain parental consent if registration or other information reveals that the person seeking the e-mail account is a child.

A number of commenters noted that operators might be responsible for complying with all of the requirements of the Rule after receiving an unsolicited e-mail from a child.[28] If an operator of a site directed to children receives such an e-mail, that contact is covered under the Act's (and the Rule's) one-time e-mail exception.[29] Under that exception, an operator may collect a child's name and online contact information for the purpose of responding one time in response to a direct request from a child. This exception would allow an operator to receive an e-mail from a child and provide a response without providing parental notice and obtaining consent, as long as the name and online contact information collected from the child are deleted and not used for any other purpose.[30] And again, in the case of a general audience site, these requirements apply only if the site receiving the e-mail has actual knowledge that it was sent by a child.

One commenter noted that a site could collect non-personally identifiable information about a child without parental notice or consent as long as that information was only tied to a screen name.[31] An operator who has solicited such information could obtain the child's name through a subsequent solicitation, and would thus have evaded the Act's requirement of prior parental consent.[32] This is a valid concern, but the Commission believes that the Rule does in fact address the issue. Indeed, under the Rule, once such information is linked to an identifier (the name), it becomes ''personal information'' and the Rule requires the operator to provide notice and obtain consent for the collection, use, and/or disclosure of all of the information.[33]

3. Definition of ''Disclosure''

The definition of ''disclosure'' in the proposed Rule covered: (1) The release of personal information collected from a child in identifiable form by an operator for any purpose, except where the operator provides the information to a person who provides support for the internal operations of the website and who does not use that information for any other purpose; [34] and (2) making personal information collected from a child publicly available in identifiable form, including through public postings, posting of personal home pages, messages boards, and chat rooms, or any other means that would enable a child to reveal personal information to others online.[35]

In the NPR, the Commission sought to clarify that entities that provide fulfillment services or technical support would be considered ''support for the internal operations of the website or online service,'' and thus disclosures to such entities need not be disclosed in the site's notices.[36] The Commission also noted that such services as merely providing the server for the website, or providing chat or e-mail service would also be considered ''support for the internal operations of the website.'' [37] The Commission cautioned, however, that because operators are also required by the Act to establish reasonable procedures to maintain the confidentiality, security, and integrity of personal information collected from children,[38] they should take appropriate measures to safeguard such information in the possession of those who provide support for the internal operations of their websites.[39]

Association (''CDT, et al.'') (Workshop comment 11) at 2–4.

[22] *Id.*

[23] 144 Cong. Rec. S11657 (Statement of Sen. Bryan).

[24] *Privacy Online: A Report to Congress* at 5 (June 1998).

[25] *Id.* The concern may be heightened where such services are directed to children because potential predators know that the majority of the participants are likely to be underage.

[26] Center for Media Education, Consumer Federation of America, Am. Academy of Child and Adolescent Psychiatry, Am. Academy of Pediatrics, Junkbusters Corp., Nat'l Alliance for Non-Violent Programming, Nat'l Ass'n of Elementary School Principals, Nat'l Consumers League, Nat'l Education Ass'n, Privacy Times and Public Advocacy for Kids (''CME/CFA et al.'') (Comment 80) at 30; Viacom (Comment 79) at 13–14; DMA (Workshop comment 02) at 1–2; Bagwell/MTV Networks Online (Workshop Tr. 32–33); Kraft (Comment 67) at 4–5; Children's Advertising Review Unit of the Council of Better Business Bureaus (''CARU'') (Workshop comment 08) at 2; Cartoon Network, et al. (Comment 77) at 18; Nikolai.com, Inc. (Comment 129) at 2; and Consumers Union (Comment 116) at 3.

[27] *See, e.g.,* Commercial Internet eXchange Ass'n and PSINet Inc. (''CIX et al.'') (Comment 83) at 8; Zeeks.com (Comment 98) at 1; CDT et al. (Workshop comment 11) at 3 (noting same First Amendment concerns as for chat rooms). Similar concerns were expressed in connection with the proposed Rule's definition of ''disclosure,'' which included ''any other means that would enable a child to reveal personal information to others online.'' *See* Section II.A.3, *infra.*

[28] *See, e.g.,* ZapMe! (Comment 76) at 7–8. *See also* Highlights for Children, Inc. (''Highlights'') (Comment 124) at 2.

[29] 15 U.S.C. 6502(b)(2)(A); section 312.5(c)(2) of the Rule. *See* Section II.D.3, *infra.*

[30] Moreover, this exception would accommodate sites that automate their responses to incoming e-mails, as long as the child's name and online contact information are deleted and not used for any other purpose. MLG Internet (Comment 119) at 2 (asking about automated e-mail responses).

[31] CDT (Comment 81) at 18.

[32] *Id.*

[33] *See* Section II.A.8, *infra.* Moreover, under section 312.6 of the Rule, the operator must disclose that information to the parent upon request and the parent may request that the operator delete that information. *See* Section II.E, *infra.*

[34] The ''release of personal information'' is defined in the Rule to mean the ''sharing, selling, renting, or any other means of providing personal information to any third party.'' *See* section 312.2 of the Rule. For additional guidance as to whether an entity is a ''third party'' under the Rule, see discussion, *infra,* regarding definitions of ''operator'' and ''third party.''

[35] 64 FR 22752, 22764.

[36] 64 FR at 22752.

[37] *Id.*

[38] 15 U.S.C. 6502(b)(1)(D).

[39] 64 FR at 22752. Some commenters objected to the notion of holding operators liable for the action of contractors because operators have no way of ensuring that contractors will follow the Rule. *See, e.g.,* DMA (Comment 89) at 35. The Act and the Rule require operators to establish and maintain reasonable procedures to protect the confidentiality,

Two commenters expressed a concern that the last clause of the proposed definition, which covered ''any other means that would enable a child to reveal personal information to others online,'' would include an Internet Service Provider (''ISP'') or cable company that simply provides Internet access without offering any content or actively collecting any information from children.[40] Although the Commission notes that this language was not meant to reach such entities,[41] it has decided to eliminate this language as confusing and unnecessary.[42]

4. Definition of ''Internet''

The proposed Rule's definition of ''Internet'' made clear that it applied to the Internet in its current form and to any conceivable successor.[43] Given that the technology used to provide access to the Internet will evolve over time, it is imperative that the Rule not limit itself to current access mechanisms. The Commission received three comments regarding this definition.[44] One commenter suggested that the Commission clarify that the definition ''clearly includes networks parallel to or supplementary to the Internet such as those maintained by the broadband providers * * * [and] intranets maintained by online services which are either accessible via the Internet or have gateways to the Internet.'' [45] The Commission believes that the proposed definition of ''Internet'' was sufficiently broad to encompass such services and adopts that definition in the final Rule.

5. Definition of ''Online Contact Information''

The Commission received several comments [46] regarding the definition of ''online contact information.'' [47] One commenter suggested that the Commission include in the definition such identifiers as instant messaging user identifiers, which are increasingly being used for communicating online.[48] The Commission believes that these identifiers already fall within the proposed definition, which includes ''any other substantially similar identifier that permits direct contact with a person online.'' [49] After reviewing the comments, the Commission has determined that no changes to this definition are necessary.

6. Definition of ''Operator''

The definition of ''operator'' is of central importance because it determines who is covered by the Act and the Rule. Consistent with the Act, the proposed Rule defined operator (with some limitations) as ''any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users or visitors * * * or on whose behalf such information is collected or maintained * * *'' [50] In the NPR, the Commission clarified the scope of the definition by listing a number of factors to consider, including who owns and/or controls the information, who pays for its collection and maintenance, the pre-existing contractual relationships regarding collection and maintenance of the information, and the role of the website or online service in collecting and/or maintaining the information (*i.e.*, whether the site participates in collection or is merely a conduit through which the information flows to another entity).[51] The Commission also clarified that entities that merely provide access to the Internet, without providing content or collecting information from children, would not be considered operators.[52] In the NPR, the Commission asked about the impact of the proposed definition, and whether it was sufficiently clear to provide notice as to who is covered by the Rule.[53] After carefully reviewing the comments received, the Commission has determined that no changes to the proposed definition are necessary.

A number of commenters proposed various tests to determine how corporate affiliates should be treated under the Rule.[54] The Commission believes that an entity's status as an operator or third party under the Rule should be determined not by its characterization as a corporate affiliate, but by its relationship to the information collected under the factors described in the NPR. Not all affiliates play a role in collecting or maintaining the information from children, and making an entity an operator subject to the Act simply because one of its affiliates collects or maintains information from children online would not serve the goals of the COPPA. If, however, the entity has an interest in the data collected under the factors listed in the NPR, then it, too, will be covered by the Rule.[55]

One commenter sought clarification of the status of network advertising companies, or companies that provide banner ads on websites or online

security, and integrity of personal information collected from children. 15 U.S.C. 6502(b)(1)(D); section 312.8 of the Rule. As long as the operator follows reasonable procedures to ensure that such contractors protect the information (for example, contractual provisions that limit the contractors' ability to use the information), operators should not be liable for the actions of contractors.

[40] *See* CIX, *et al.* (Comment 83) at 8–9; National Cable Television Association (''NCTA'') (Comment 71) at 6–8.

[41] *See* 64 FR at 22752. To the extent that ISPs do not operate websites or online services that are directed to children, or knowingly collect information from children, they are not subject to the COPPA.

[42] One commenter also asked whether the term ''disclosure'' covered the inclusion of a child's name on a list of contest winners, which is often required under state laws. *See* PMA (Comment 107) at 4. If the operator collects only name and online contact information, then the exception under section 312.5(c)(5)(iv) would apply. However, if the operator collects additional information online, then the release of that information would be considered a disclosure under the Rule.

[43] 64 FR at 22752, 22764.

[44] CME/CFA et al. (Comment 80) at 18; E.A. Bonnett (Comment 126) at 1; CDT (Comment 81) at 10–11. Two of the comments praised the proposed definition as comprehensive. E.A. Bonnett (Comment 126) at 1; CDT (Comment 81) at 10–11.

[45] CME/CFA et al. (Comment 80) at 18.

[46] CyberAngels (Comment 120) at 1; CME/CFA et al. (Comment 80) at 6–7; Aftab & Savitt (Comment 118) at 3–4; CDT (Comment 81) at 16–18.

[47] The definition in the proposed Rule was identical to the one contained in the Act. *See* 15 U.S.C. 6501(12); 64 FR at 22752, 22764.

[48] CyberAngels (Comment 120) at 1.

[49] Another example of ''online contact information'' could be a screen name that also serves as an e-mail address. *See* Section II.A.8, *infra*.

[50] 15 U.S.C. 6501(2); 64 FR at 22752, 22764.

[51] 64 FR at 22752.

[52] Thus, ISPs and cable operators that merely offer Internet access would not be considered operators under the Rule.

[53] 64 FR at 22761.

[54] *See, e.g.*, Council of Better Business Bureaus, Inc. (''CBBB'') (Comment 91) at 6–7; Attorneys General of the States of New York, Alabama, California, Florida, Georgia, Hawaii, Illinois, Indiana, Maryland, Nevada, Ohio, Oklahoma, Tennessee, Vermont, and Washington (''Attorneys General'') (Comment 114) at 6; PMA (Comment 107) at 4–5; Am. Ass'n of Advertising Agencies (''AAAA'') (Comment 134) at 3; Ass'n of Nat'l Advertisers (''ANA'') (Comment 93) at 6–7. Some commenters argued in support of automatically including all corporate affiliates as operators. Others thought that all affiliates with identical privacy policies should be considered operators, or, alternatively, that operators should be required to disclose that an affiliate has a different privacy policy and describe how it differs from the primary operator's. As noted in Section II.C.3.c, *infra*, the notice is required to describe the privacy policies of the various operators. One commenter suggested a consumer perception standard: that an affiliate would be considered an operator if a consumer would reasonably expect that the affiliated entities are part of one organization that shares information within itself. PMA (Comment 107) at 5. The Commission believes that the proposed standard, which places responsibility for compliance on the entities that control the information, is the most workable test for who is an operator.

[55] In the NPR, the Commission stated that operators are jointly responsible for implementing the requirements of the Rule. 64 FR at 22752. In an investigation into a potential Rule violation, the Commission will examine all the facts and circumstances in determining the appropriate party or parties to pursue. The Commission likely will not pursue an entity that is an ''operator,'' but has not facilitated or participated in, and has no reason to know of, any Rule violations.

services.[56] If such companies collect personal information directly from children who click on ads placed on websites or online services directed to children, then they will be considered operators who must comply with the Act, unless one of the exceptions applies.[57] Moreover, if such companies collect personal information from visitors who click on their ads at general audience sites, and that information reveals that the visitor is a child, then they will be subject to the Act. In addition, if they do not collect information from children directly, but have ownership or control over information collected at a host children's site, they will be considered operators. If, however, no personal information is collected or maintained by such companies, either directly or through the host website, then they will not be deemed to be operators.

Some commenters sought greater clarity regarding the meaning of ''actual knowledge'' that a particular visitor is a child and inquired whether an operator of a general audience site has any duty to investigate the age of its visitors.[58] Actual knowledge will be present, for example, where an operator learns of a child's age or grade from the child's registration at the site or from a concerned parent who has learned that his child is participating at the site. In addition, although the COPPA does not require operators of general audience sites to investigate the ages of their site's visitors, the Commission notes that it will examine closely sites that do not directly ask age or grade, but instead ask ''age identifying'' questions, such as ''what type of school do you go to: (a) elementary; (b) middle); (c) high school; (d) college.'' Through such questions, operators may acquire actual knowledge that they are dealing with children under 13.

Finally, one commenter sought assurance that an operator would not be liable if his site contained a link to another site that was violating the Rule.[59] If the operator of the linking site is not an operator with respect to the second site (that is, if there is no ownership or control of the information collected at the second site according to the factors laid out in the NPR), then the operator will not be liable for the violations occurring at the second site.

7. Definition of ''Parent''

The Act and the proposed Rule defined ''parent'' as ''includ[ing] a legal guardian.'' [60] The Commission received two comments regarding this definition, both of which sought additional guidance concerning the Rule's application in non-traditional family situations.[61] The Commission believes that the proposed definition is sufficiently flexible to account for a variety of family structures and situations, including situations where a child is being raised by grandparents, foster parents, or other adults who have legal custody. Therefore, the Commission retains the definition of parent contained in the proposed Rule.

8. Definition of ''Personal Information''

The definition of ''personal information'' is another critical part of the Rule because it specifies the type of information covered by the Rule. The proposed definition included a number of different types of individually identifiable information, including name, address, and phone number; e-mail address; and other types of information that could be used to locate an individual either online or offline.[62] The proposed definition also covered non-individually identifiable information (*e.g.,* information about a child's hobbies or toys) that is associated with an identifier.[63]

One commenter asked the Commission to clarify that operators are not required to provide parental notice or seek parental consent for collection of non-individually identifiable information that is not and will not be associated with an identifier.[64] The Commission believes that this is clear in both the Act and the Rule.

Several commenters sought further guidance on whether the use of screen names would trigger the Act's requirements.[65] If a screen name is not associated with any individually identifiable information, it is not considered ''personal information'' under this Rule.[66]

Another commenter criticized the proposed Rule on the grounds that it encourages operators to set up sites using screen names.[67] This commenter argued that it is important to have accountability online—*i.e.,* that it is important for operators to be able to identify and take action against visitors who post inappropriate information or harass other online visitors. The Commission agrees that these are important considerations, but notes that the Rule does not foreclose operators from taking such precautions. Operators are free to request parental consent to collect such information. Moreover, the exception to the requirement of prior parental consent under section 312.5(c)(5)(i) of the Rule allows operators to collect the child's online contact information for this very purpose.[68]

One commenter noted that there are some persistent identifiers that are automatically collected by websites and can be considered individually identifying information, such as a static IP address or processor serial number.[69] If this type of information were considered ''personal information,'' the commenter noted, then nearly every child-oriented website would automatically be required to comply with the Rule, even if no other personal information were being collected. The Commission believes that unless such identifiers are associated with other individually identifiable personal information, they would not fall within the Rule's definition of ''personal information.''

Several commenters asked whether information stored in cookies falls within the definition of personal information.[70] If the operator either collects individually identifiable information using the cookie or collects non-individually identifiable information using the cookie that is

---

[56] Media Inc., AdForce, Inc., DoubleClick, Inc., Engage Technologies, Inc., Flycast Communications Corp., and Real Media, Inc. (Comment 92) at 4–8.

[57] It may be appropriate for such companies to provide a joint notice with the operator of the host website.

[58] *See* PMA (Comment 107) at 6; Attorneys General (Comment 114) at 7. See also MLG Internet (Comment 119) at 1–2.

[59] MaMaMedia, Inc. (''MaMaMedia'') (Comment 85) at 7.

[60] 15 U.S.C. 6501(7); 64 FR at 22752, 22764.

[61] Ass'n of Educational Publishers (''EdPress'') (Comment 130) at 2; Highlights (Comment 124) at 1.

[62] 64 FR at 22752–22753, 22764.

[63] *Id.*

[64] *See* National Retail Federation (''NRF'') (Comment 95) at 2.

[65] ZapMe! (Comment 76) at 8–9; KidsOnLine.com (Comment 108) at 1–2; TRUSTe (Comment 97) at 3.

[66] One commenter also asked whether operators would be required to ensure that a screen name chosen by a child did not contain individually identifiable information. TRUSTe (Comment 97) at 3. Operators do not have a specific duty to investigate whether a screen name contains such information. However, an operator could give children warnings about including such information in screen names, especially those that will be disclosed in a public forum such as a chat room.

[67] KidsOnLine.com (Comment 108) at 1–2.

[68] *See also* 15 U.S.C. 6502(b)(2)(E)(i). As noted above, an operator who wishes to collect name and online contact information under this exception may not use or disclose that information for any other purpose. An operator, however, who collects other personal information and links it with online contact information collected under this exception would be in violation of the Rule unless the operator provided parental notice and obtained verifiable parental consent for the collection of all of that information.

[69] CDT (Comment 81) at 16. *See also* E.A. Bonnett (Comment 126) at 2–3.

[70] *See, e.g.,* Consumers Union (Comment 116) at 4.

combined with an identifier, then the information constitutes ''personal information'' under the Rule, regardless of where it is stored.

After reviewing the comments, the Commission has decided to retain the definition of ''personal information'' with slight modifications. In response to the suggestion of one commenter, one item was added to subparagraph (f) of the definition: a photograph of the individual, when associated with other information collected online that would enable the physical or online contacting of the individual.[71] The Commission is also making slight modifications to ensure consistency within the definition.

9. Definition of ''Third Party''

The proposed Rule defined the term ''third party'' as ''any person who is neither an operator with respect to the collection of personal information * * * nor a person who provides support for the internal operations of the website or online service.'' [72] Under the Rule, an operator is required to provide notice of its practices with respect to the disclosure of information to third parties and to allow parents to choose whether the operator may disclose their children's information to third parties.[73] Because third parties are not operators, they are not responsible for carrying out the provisions of the Rule.

Comments regarding this definition raised issues similar to those raised in response to the proposed definition of ''operator''—specifically, when and whether corporate affiliates would be considered ''operators'' or ''third parties.'' As noted above, the Commission believes that the most appropriate test for determining an entity's status as an operator or third party is to look at the entity's relationship to the data collected, using the factors listed in the NPR.[74] If an entity does not meet the test for operator, that entity will be considered a third party.

One commenter asked that the Commission require third parties to comply with the Rule.[75] However, the statute applies only to the practices of the operator, and the Commission does not have the authority to extend liability to third parties.

After reviewing the comments, the Commission has made minor revisions to the definition of ''third party'' to maintain consistency across the Rule. These revisions consist of adding the words ''and maintenance'' following ''collection,'' and clarifying that, in order to be excluded from the definition, a person who provides internal support for the website may not disclose or use information protected under this Rule for any other purpose.

10. The Definition of ''Obtaining Verifiable Parental Consent''

The proposed Rule included a definition of ''obtaining verifiable parental consent'' that was substantially similar to the definition contained in the COPPA.[76] The term was defined to mean ''making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child'' receives notice of the operator's information practices and consents to those practices. The Commission received no comments suggesting modification to this definition, and therefore retains the proposed definition.

11. Definition of ''Website or Online Service Directed to Children''

In the proposed Rule, the Commission listed a number of factors that the Commission would consider in determining whether a site would be ''directed to children,'' including, among other things, the site's ''subject matter, visual or audio content, age of models, language or other characteristics of the website or online service. * * *''[77] The Commission also stated in the proposed Rule that it would consider competent and reliable empirical evidence regarding audience composition as well as evidence regarding the intended audience of the site.[78] In addition, under the proposed Rule, a general audience website would not be deemed to be directed to children simply because it referred or linked to another website or online service that is directed to children.[79] Finally, if a general audience site has a distinct children's ''portion'' or ''area,'' then the operator would be required to provide the protections of the Rule for visitors to that portion of the site.[80]

Several commenters asked for more guidance about the factor analysis laid out in this definition.[81] One commenter asked that the Commission clarify that the presence of only one of the listed factors would not cause a site to be classified as ''directed to children''; rather that *all* of the factors would be taken into account.[82] In response, the Commission notes that the proposed definition makes it clear that the Commission will look at the overall character of the site—and not just the presence or absence of one or more factors—in determining whether a website is directed to children.

Another commenter noted that operators should not be able to construct a ''veil of ignorance'' where the operator can determine through questions whether a visitor is a child without specifically asking for the visitor's age.[83] As discussed above in Section II.A.6 concerning the definition of ''operator,'' the Commission will closely examine such sites to determine whether they have actual knowledge that they are collecting information from children. A similar concern was raised with respect to sites that ask for age ranges that include both children and teens (*e.g.*, a ''15 and under'' category).[84] Because it is simple for operators to craft a ''12 and under'' age range, the Commission will look closely at sites that do not offer such a range if it appears that their operators are trying to avoid compliance with the Rule.

B. Section 312.3: Regulation of Unfair or Deceptive Acts or Practices in Connection With the Collection, Use, and/or Disclosure of Personal Information From and About Children on the Internet

Section 312.3 of the proposed Rule set out the Rule's general requirements, which were detailed in the later provisions.[85] The Commission received no comments that directly pertained to section 312.3 of the proposed Rule, which was a restatement of the requirements laid out in the Act,[86] and therefore retains it without change. Comments regarding the sections

[71] Aftab & Savitt (Comment 118) at 4. This commenter also asked the Commission to remove the phrase ''collected online'' from this definition in order to cover information that is submitted to an operator offline, then posted online by the operator. While we are cognizant of the risks posed by such practices, the Commission believes that the COPPA does not apply to information submitted to an operator offline. *See* Section II.A.2, *supra*, concerning the definition of ''collection.''

[72] 64 FR at 22753, 22764.

[73] *See* Sections II.C.3.d, and II.D.1, *infra*.

[74] *See* Section II.A.6, *supra;* 64 FR at 22752.

[75] CME/CFA et al. (Comment 80) at 6, 11.

[76] *See* 64 FR 22753, 22764; 15 U.S.C. 6501(9).

[77] 64 FR 22753, 22764.

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] JuniorNet Corp. (''JuniorNet'') (Comment 100) at 2; Int'l Digital Software Ass'n (''IDSA'') (Comment 103) at 2; CDT (Comment 81) at 20–21; MLG Internet (Comment 119) at 2; Time Warner (Comment 78) at 4, 5.

[82] JuniorNet (Comment 100) at 2.

[83] Consumers Union (Comment 116) at 4–5.

[84] CME/CFA et al. (Comment 80) at 7; Attorneys General (Comment 114) at 7. *See also* TRUSTe (Comment 97) at 2.

[85] 64 FR at 22753, 22764.

[86] 15 U.S.C. 6502(b)(1).

implementing its requirements are discussed in the relevant sections below.

C. Section 312.4: Notice

1. Section 312.4(a): General Principles of Notice

The COPPA mandates that an operator provide notice on its website and to parents of ''what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices regarding such information.'' [87] The proposed Rule set out general principles of notice, followed by a specific set of guidelines for the online placement and content of those notices, to ensure that parents receive all the information that they would find material when reviewing a site.[88] As noted in the NPR, the operator's notice will form the basis for a parent's decision whether to give the operator consent to collect, use, and/or disclose personal information from his or her child.[89] In order to provide informed consent, a parent must have a clear idea of what the operator intends to do.[90] Therefore, the proposed Rule required an operator's notice to ''be clearly and understandably written,'' [91] be complete, and * * * contain no unrelated, confusing, or contradictory materials.'' [92] The Commission believes that these are the core principles underlying a consent-based system and, therefore, retains this section in the final Rule.[93]

2. Section 312.4(b)(1): Notice on the Website or Online Service—Placement of the Notice

Section 312.4(b)(1) of the proposed Rule set forth the requirements for online placement of the notice of the operator's information practices. It required operators to place a link to the notice on the home page of the website or online service such that a typical visitor would see the link without having to scroll down from the initial viewing screen.[94] In addition, the proposed Rule required operators to post a link to that notice in a similar manner at each place on the website or online service where information is collected from children.[95]

A large number of commenters noted that with the multitude of Web browsers available and the advent of ever-smaller machines that can access the Internet, it may not be technically feasible to ensure that the link to the notice can be seen without scrolling down from the initial viewing screen.[96] The Commission acknowledges that the proposed Rule's requirement regarding the placement of the online notices may not be a workable standard. Therefore, the Commission has modified section 312.4(b)(1)(ii) to require that a link to the notice be placed ''in a clear and prominent place and manner on the home page of the website or online service.'' ''Clear and prominent'' means that the link must stand out and be noticeable to the site's visitors through use, for example, of a larger font size in a different color on a contrasting background. The Commission does not consider ''clear and prominent'' a link that is in small print at the bottom of the home page, or a link that is indistinguishable from a number of other, adjacent links.

Some commenters noted that general audience sites with distinct children's areas should be allowed to post the link to the children's privacy policy at the home page of the children's area, rather than the home page of the overall site.[97] The Commission believes that this is a sensible approach to providing notice. Parents who are reviewing the operator's practices with respect to children would likely go directly to the children's area; therefore, operators of sites with distinct children's areas must post a prominent link at the home page of that area.[98]

Further, in response to comment, section 312.4(b)(1)(iii) has been modified to require that a link to the notice be placed ''at each area on the website or online service where children directly provide, or are asked to provide, personal information and in close proximity to the requests for information in each such area.'' The comment noted—and the Commission agrees—that it makes sense to require that the link be in close proximity to the initial request for information in an area so that visitors do not have to scroll up or down the page to find the link.[99] In response to comments, the Commission also changed the requirement of notice at each ''place'' where children provide information to notice at each such ''area'' in order to make clear that there does not need to be a link accompanying each question, but simply at each separate area where such information is collected.[100]

3. Section 312.4 (b)(2) and (c)(1)(i)(B): Content of the Notice

Section 312.4(b)(2) of the proposed Rule details the information that operators must include in their notice on the site. That information was also required to be included in the notice to the parent under Section 312.4(c)(1)(i)(B).[101] Under the proposed Rule, operators were required to include in their notices, among other things: (1) names and contact information for all operators; (2) the types of personal information collected through the site and how such information is collected; (3) how the personal information would be used; (4) whether the personal

---

[87] 15 U.S.C. 6502(b)(1)(A)(i). One commenter stated that Congress included these general guidelines in the Act as a performance standard, rather than intending them to be a source of detailed regulations. Yahoo! Inc, theglobe.com, inc., DoubleClick, Inc. (''Yahoo et al.'') (Comment 73) at 2. Congress, however, specifically delegated to the Commission the authority to issue regulations to implement the Act.

[88] Sections 312.4(a), (b); 64 FR at 22753–56, 22764–65.

[89] 64 FR at 22754–55.

[90] The Commission notes that it has authority under this section, as well as under Section 5 of the Federal Trade Commission Act, to take action against operators whose notices are deceptive or misleading.

[91] CME/CFA et al. (Comment 80) at 9; The McGraw-Hill Companies (''McGraw-Hill'') (Comment 104) at 6. One commenter asked whether the Commission would apply a particular standard in evaluating how a notice is written. Jeff Sovern, St. John's University School of Law (''Sovern'') (Comment 33) at 3–4. Traditionally, the Commission has applied a ''reasonable consumer'' standard in evaluating whether a notice is clearly and understandably written. Because the notices required by the Act are intended for parents, the Commission will look at whether they are written such that a reasonable parent can read and comprehend them.

[92] 64 FR at 22754.

[93] Two commenters voiced support for these general principles. *See* Attorneys General (Comment 114) at 7; Kraft (Comment 67) at 1.

[94] 64 FR at 22754.

[95] *Id.* Several commenters supported the use of other mechanisms for providing notice, such as pop-up or interstitial pages, which typically appear temporarily when visitors move from one part of the site to another. America Online, Inc. (''AOL'') (Comment 72) at 11; NRF (Comment 95) at 3; iCanBuy.com (Comment 101) at 2. The Commission notes that pop-up or interstitial pages will only satisfy the notice requirements of the Rule if they are clear, prominent, and easily accessible to users, *i.e.*, they do not disappear after the initial viewing or users can re-access them through a clear and prominent link on the home page.

[96] *See, e.g.*, Am. Advertising Fed. (''AAF'') (Comment 87) at 2; ANA (Comment 93) at 5; Dell Computer Corp. (''Dell'') (Comment 102) at 3–4; McGraw-Hill (Comment 104) at 7; Time Warner (Comment 78) at 9; Viacom (Comment 79) at 6–7.

[97] ANA (Comment 93) at 5; MPA (Comment 113) at 3–4; DMA (Comment 89) at 22–23; McGraw-Hill (Comment 104) at 7.

[98] One comment argued that the notice requirements would require operators of general audience sites to have two physically separate privacy policies—one for adults and one for children. Kraft (Comment 67) at 4. Operators are free to combine the privacy policies into one document, as long as the link for the children's policy takes visitors directly to the point in the document where the operator's policies with respect to children are discussed, or it is clearly disclosed at the top of the notice that there is a specific section discussing the operator's information practices with regard to children.

[99] Mars, Inc. (''Mars'') (Comment 86) at 10.

[100] *See, e.g.*, AOL (Comment 72) at 8–11.

[101] 64 FR at 22754–56, 22765.

information would be disclosed to third parties, the types of businesses in which those third parties are engaged, whether the third parties have agreed to take steps to protect the information, and a statement that parents have the right to refuse to consent to the disclosure of their child's personal information to third parties; (5) that the operator may not condition a child's participation in an activity on the provision of more personal information than is necessary to participate in the activity; and (6) that the parent may review, make changes to, or have deleted the child's personal information.[102] Many of the comments addressing these sections expressed concern that they required the inclusion of too much information in the notices. As discussed below, the Commission believes that most of the information required in the proposed Rule would be material to parents in deciding whether to consent to their child's participation in a site. However, in order to reduce the length of the notice, the Commission has eliminated certain information that it has determined would be of limited benefit to parents.

a. Section 312.4(b)(2)(i). This section of the proposed Rule required operators to include in the notice the name, address, phone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service.[103] Some commenters objected to including this information in the notice because it would make the notice unwieldy. Operators can minimize the length of the notice by designating a single entity as a central contact point for any inquiries regarding the information practices of the site's operators. The Commission, however, believes that it is essential that all operators be identified in the notice, even if full contact information is not provided, so that parents know who will see and use their children's personal information. Therefore, the Commission has modified this provision accordingly. Operators who do not wish to designate a single contact may still minimize the length of the notice by including in the notice on the site a hyperlink to a separate page listing the information.[104]

Several comments also noted that data-sharing relationships in the online world change quickly, sometimes on a weekly basis,[105] and that it would be burdensome for operators to revise their notices with each change, as the proposed Rule required, particularly in the case of the notice to the parent.[106] While the Commission believes that it is reasonable to expect operators to keep the notice on the site current, it agrees that it would be burdensome for operators to send numerous updated notices to parents. Therefore, as discussed in Section II.C.4, below, it has modified the Rule to require a new notice to the parent only where there will be a *material change* in the collection, use, and/or disclosure of personal information from the child. Thus, for example, if the operator plans to disclose the child's personal information to a new operator with different information practices than those disclosed in the original notice, then a new consent would be required.[107]

b. Section 312.4(b)(2)(ii). Under this section of the proposed Rule, operators were required to disclose the types of personal information collected from children and whether that information is collected directly or passively.[108] In the NPR, the Commission clarified that this section did not require operators to disclose to parents every specific piece of information collected from children, but rather the *types* or *categories* of personal information collected, like name, address, telephone number, social security number, hobbies, and investment information.[109] The Commission cautioned operators to use categories that were descriptive enough that parents could make an informed decision about whether to consent to the operator's collection and use of the information.[110]

Some commenters noted that the proposed Rule required operators to provide too much detail in the notice concerning the types of information collected from children.[111] These commenters felt that a more general notice would give the operator more flexibility to change its activities without having to return to the parent for additional consent.[112] The Commission believes that a more general notice may not reveal to parents that the operator collects information that the parent does not want discussed or divulged, like personal financial information. Therefore, the Commission is retaining this portion of the Rule. However, as noted above, these concerns should be alleviated by the Commission's amendment to the Rule regarding ''material changes.'' [113]

c. Section 312.4(b)(2)(iii). Section 312.4(b)(2)(iii) of the proposed Rule required operators to notify parents about how their child's personal information ''is or may be used by the operator, including but not limited to fulfillment of a requested transaction, recordkeeping, marketing back to the child, or making it publicly available through a chat room or by other means.'' [114] In the NPR, the Commission noted that operators must provide enough information for parents to make informed decisions, without listing every specific or possible use of the information.[115] Many commenters expressed the view that the proposed Rule would require an operator to provide such detail that they would inevitably have to send new notices and obtain new consents for every minor change in the operator's practices.[116] Again, these concerns should be alleviated by the Rule amendment regarding ''material changes.'' *See* Section II.C.4, *infra.*

Because this section of the proposed Rule referred only to ''the operator,'' one commenter asked how websites should address situations in which there are multiple operators collecting information through the site but who use children's personal information in different ways.[117] Specifically, the commenter asked whether each operator was required to post a separate notice, or whether a single notice could be used. Where there are multiple operators with different information

[102] *Id.*

[103] 64 FR at 22754, 22765.

[104] In response to two comments, the Commission notes that simply providing a hyperlink to the home pages of the other operators, however, would not provide adequate notice for parents. DMA (Comment 89) at 23–24; AOL (Comment 72) at 12. It would not only be burdensome for parents, but some entities that would be categorized as ''operators'' (*i.e.*, those ''on whose behalf'' personal information was collected) may not even have websites.

[105] PMA (Comment 107) at 7–8; DMA (Comment 89) at 23–24. *See also* McGraw-Hill (Comment 104) at 7.

[106] 64 FR at 22755. In the NPR, the Commission stated that additional notices to the parent would be required if the operator wished to disclose the child's personal information to parties not covered by the original consent, including parties created by a merger or other change in corporate structure.

[107] Marketing diet pills, for example, would be a materially different line of business than marketing stuffed animals.

[108] 64 FR at 22754, 22765.

[109] 64 FR at 22754.

[110] *Id.* For example, stating ''We collect your child's name, e-mail address, information concerning his favorite sports, hobbies, and books'' would be sufficient under the Rule. It would not be necessary for the operator to state ''We ask for your child's name and e-mail address, and whether he likes to play baseball, soccer, football, or badminton. * * *''

[111] McGraw-Hill (Comment 104) at 6–7; AAF (Comment 87) at 2.

[112] *Id.*

[113] *See* Section II.C.4, *infra.* In addition, as noted in note 9, *supra*, the Commission plans to develop educational materials to assist operators in complying with the Rule.

[114] 64 FR at 22754–55, 22765.

[115] 64 FR at 22754.

[116] *See supra* note 106 and accompanying text.

[117] Attorneys General (Comment 114) at 8.

practices, there should be one notice summarizing all of the information practices that will govern the collection, use, and/or disclosure of children's personal information through the site. Thus, the Commission has modified the Rule to clarify that a discussion of all policies governing the use of children's information collected through the site should be included in the notice.

d. Section 312.4(b)(2)(iv). Under this provision of the proposed Rule, an operator was required to disclose whether children's personal information was disclosed to third parties, and if so, the types of business in which those third parties were engaged, as well as whether those third parties had agreed to maintain the confidentiality, security, and integrity of the personal information obtained from the operator.[118] In addition, the operator was required to notify the parent that he or she had the option of consenting to the operator's collection and use of the child's information without consenting to the disclosure of that information to third parties.[119] After reviewing all the relevant comments, the Commission has determined that no changes to this section are necessary.

One commenter noted that the COPPA ''requires only that an operator describe its own practices. * * *'' [120] The Commission believes that the information required in this section of the proposed Rule falls within the rubric of ''the operator's disclosure practices for such information.'' [121] Parents need to know the steps an operator has taken to ensure that third parties will protect their children's data in order to provide meaningful consent.

Some commenters felt that providing information concerning the businesses engaged in by third parties would be overly burdensome.[122] Under this section, however, operators are not required to provide detailed information concerning third party businesses, but only to describe the ''*types* of business'' in which third parties who will receive children's information are engaged—for example, list brokering, advertising, magazine publishing, or retailing.[123] The Commission believes that it is not unduly burdensome to determine the general line of business of the companies with whom one does business. Moreover, this information will enable parents to provide meaningful consent to third party disclosures.

Commenters again pointed out that relationships between companies in the online environment change rapidly, which would make notices difficult to compose and keep current.[124] Changes in the identities of third parties would necessitate repeated notices to parents, burdening both the operator and the parent.[125] Another commenter suggested that rather than give notice of third parties' information practices, operators should be allowed simply to provide a warning to parents to review those practices.[126] Once again, these concerns should be alleviated by the fact that the disclosure is only of the *types* of businesses engaged in by third parties, and new notice and consent are required only if there has been a material change in the way that the operator collects, uses, and/or discloses personal information. *See* Section II.C.4, below.

Still other commenters stated that the Commission should require operators to disclose more detailed information regarding third parties' information practices than the proposed Rule required, including whether a third party has weaker standards than the operator.[127] The Commission believes that the proposed requirement—that operators state whether or not the third parties have agreed to maintain the confidentiality,[128] security, and integrity of children's data B strikes the appropriate balance between a parent's need for information and an operator's need for an efficient means of complying with the Rule.

Alternatively, one of these commenters requested that operators be prohibited from disclosing children's personal information to any third party unless that party not only complies with the Act, but also has the same privacy policy as the operator.[129] The Act explicitly applies to ''any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child.'' [130] Therefore, the Commission cannot extend liability to third parties.

e. Section 312.4(b)(2)(v). Under Section 312.4(b)(2)(v) of the proposed Rule, operators were required to state in their notices that the Act prohibits them from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in that activity.[131] One commenter objected to including such a statement in the notice, on the grounds that it does not provide parents with helpful information.[132] The Commission believes that this information is material to parents and will assist them in evaluating the reasonableness of an operator's requests for information. Therefore, the Commission has decided to retain this provision.

f. Section 312.4(b)(2)(vi). This section of the proposed Rule required operators to describe in the notice on the site parents' right to review personal information provided by their children.[133] It generally tracked the requirements in section 312.6 of the proposed Rule [134] by requiring notice of a parent's ability to review, make changes to, or have deleted the child's personal information. In the NPR, the Commission sought public comment on whether this information was needed in the notice on the site, or only in the notice to the parent.[135]

Some commenters believed that it was only necessary to include this information in the notice to the parent, because it is only relevant once parents have consented to the collection of their children's information.[136] Other commenters, however, felt notice of parents' right to review children's information should be included in the notice on the site so that parents can evaluate a site while surfing with their children.[137] The Commission also notes

---

[118] 64 FR at 22755.

[119] *Id.* For a more detailed discussion of withholding consent to the disclosure of personal information to third parties, *see* Section II.D.1, *infra.*

[120] DMA (Comment 89) at 24, citing 15 U.S.C. 6502(b)(1)(A)(i).

[121] 15 U.S.C. 6502(b)(1)(A)(i).

[122] *See e.g.,* AAF (Comment 87) at 3; CBBB (Comment 91) at 11; PMA (Comment 107) at 8; TRUSTe (Comment 97) at 1.

[123] 64 FR at 22755.

[124] TRUSTe (Comment 97) at 1–2; McGraw-Hill (Comment 104) at 7; AAF (Comment 87) at 3; PMA (Comment 107) at 8.

[125] *Id.*

[126] CBBB (Comment 91) at 11. The Commission believes that requiring parents to search out this information, which may not even be available or accessible, would be unduly burdensome.

[127] CME/CFA et al. (Comment 80) at 23–24; Electronic Privacy Information Center (''EPIC'') (Comment 115) at 8–9; Attorneys General (Comment 114) at 8.

[128] The Commission expects that third parties who have agreed to maintain the confidentiality of information received from operators will not disclose that information further.

[129] CME/CFA et al. (Comment 80) at 23. *See also* CDT (Comment 81) at 23.

[130] 15 U.S.C. 6502(b)(1)(A).

[131] 15 U.S.C. 6502(b)(1)(C); 64 FR at 22755, 22765, citing 15 U.S.C. 6502(b)(1)(C). *See also* 64 FR at 22758, 22766.

[132] Mars (Comment 86) at 4.

[133] 64 FR at 22755, 22765.

[134] 64 FR at 22757–58, 22766. For a detailed discussion of section 312.6, *see* Section II.E, *infra.*

[135] *See* 64 FR at 22762.

[136] DMA (Comment 89) at 19–20; PMA (Comment 107) at 8–9 (operator should be able to choose whether to include this information in the notice).

[137] Attorneys General (Comment 114) at 8–9; E.A. Bonnett (Comment 126) at 4; CBBB (Comment 91)

that if the parent accidentally deletes or misplaces the notice received from the operator, he or she would likely turn to the notice on the site for information on reviewing the child's information. If that information were not in the notice on the site, the parent may be foreclosed from exercising the right to review the child's information. Therefore, the Commission has retained this provision.

4. Section 312.4(c): Notice to a Parent

This provision of the proposed Rule required operators to ''make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives notice of an operator's practices with regard to the collection, use, and/or disclosure of the child's personal information, including any collection, use, and/or disclosure to which the parent has not previously consented.'' [138] After reviewing the relevant comments, the Commission has amended this provision to require new notice to the parent only when there is a material change in the way the operator collects, uses, and/or discloses personal information from the child.

In the NPR, the Commission noted that ''reasonable efforts'' to provide a parent with notice under this section could include sending the notice to the parent by postal mail or e-mail, or having the child print out a form to give to the parent. These methods were intended to be non-exclusive examples.[139] The Commission also noted that operators must send the parent an updated notice and request for consent ''for any collection, use, or disclosure of his or her child's personal information not covered by a previous consent.'' [140] Examples of situations where new notice and request for consent would be needed included if the operator wished to use the information in a manner that was not included in the original notice, such as disclosing it to parties not covered by the original consent, including parties created by a merger or other corporate combination.[141]

Many commenters argued that the Commission's interpretation concerning when a new notice and request for consent would be required was burdensome and unnecessary.[142] Given the high rate of merger activity in this industry, the commenters asserted, operators would be required to send many additional notices to parents.[143] Moreover, commenters noted that many mergers do not change the nature of the business the operator engages in or how the operator uses personal information collected from children. Therefore, many additional notices to parents under the proposed interpretation of this provision would not provide parents with meaningful information.

The Commission agrees with these comments. In order to balance an operator's need for efficiency and parents' need for relevant information, the Commission has amended the Rule to require new notice and consent only when there is a *material change* in how the operator collects, uses, or discloses personal information from children. For example, if the operator obtained consent from the parent for the child to participate in games which required the submission of limited personal information but now wishes to offer chat rooms to the child, new notice and consent will be required. In addition, if an operator (*e.g.*, a toy company) merged with another entity (*e.g.*, a pharmaceutical company) and wished to use a child's personal information to market materially different products or services than those described in the original notice (*e.g.*, diet pills rather than stuffed animals), new notice and consent would be required. Likewise, new notice and consent would be required to disclose the information to third parties engaged in materially different lines of business than those disclosed in the original notice (*e.g.*, marketers of diet pills rather than marketers of stuffed animals). On the other hand, if the operator had parental consent to disclose the child's personal information to marketers of stuffed animals, it does not need to obtain a new consent to disclose that information to other marketers of stuffed animals.

One commenter suggested that the Rule also requires the operator to obtain parental confirmation that the notice was received, either through a return e-mail or a business reply postcard.[144] The Commission believes that this proposal would burden parents and operators without adding significantly to the protection of children online. In most cases, the operator's receipt of parental consent will serve as confirmation that the parent received the notice.[145] Likewise, in most instances, if the parent does not receive the notice, then the operator simply will not receive consent.

One commenter suggested that the Commission permit the notice to the parent to take the form of an e-mail with an embedded hyperlink to the notice on the site.[146] In response, the Commission notes that the notice to the parent must contain additional information that is not required in the notice on the site.[147] However, as long as the additional, required information is clearly communicated to parents in the e-mail, and the hyperlink to the notice on the site is clear and prominent, operators may include the hyperlink to the notice on the site in an e-mail to parents.

a. Section 312.4(c)(1) (i) and (ii): information in the notice to a parent. The proposed Rule required an operator's notice to a parent to include all the information included in the notice on the site (section 312.4(c)(1)(i)(B)), as well as additional information. In cases that do not implicate one of the exceptions to prior parental consent under section 312.5(c), an operator must tell the parent that he or she wishes to collect personal information from the child (section 312.4(c)(1)(i)(A)) and may not do so unless and until the parent consents, and the operator must describe the means by which the parent can provide that consent (section 312.4(c)(1)(ii)).[148]

In the NPR, the Commission requested public comment on whether there was additional information that

at 12; CME/CFA et al. (Comment 80) at 24; TRUSTe (Comment 97) at 1–2.

[138] 64 FR at 22755, 22765.

[139] *Id.* One commenter requested that we include this information in the text of the Rule. DMA (Comment 89) at 27. The Commission believes that the performance standard enunciated in this provision is appropriate in light of the operator's need for flexibility and the additional protections that are provided by the parental consent requirement. As discussed below, the Rule provides more specific guidance as to the appropriate mechanisms for obtaining parental consent *See* Section II.D.2, *infra.*

[140] 64 FR at 22755, 22765

[141] *Id.*

[142] *See, e.g.*, AOL (Comment 72) at 14–15; DMA (Comment 89) at 26; Kraft (Comment 67) at 2, 5–6. *See also* CBBB (Comment 91) at 13–14.

[143] *Id.*

[144] CME/CFA et al. (Comment 80) at 24–25. Similarly, one commenter noted that many parents share an e-mail account with their children. A & E Television Networks (''AETN'') (Comment 90) at 17–18. In these situations, the commenter argued, it would be impossible for the operator to determine whether the notice has been received by the parent. *Id.* In many cases, however, the children will have the incentive to give the notice to the parent in order to obtain parental consent. Further, as noted above, in most cases, the operator's receipt of parental consent will confirm that the parent has received the notice.

[145] *See* Section II.D.2 *infra*, for a detailed discussion of the requirements for obtaining verifiable parental consent under Section 312.5 of the Rule.

[146] Mars (Comment 86) at 12.

[147] For example, the notice to the parent must contain information concerning how to provide parental consent (section 312.4(c)(1)(ii)).

[148] 64 FR at 22755, 22765. One commenter thought that the notice should also inform parents that they have the option of denying consent. CME/CFA et al. (Comment 80) at 12. The Commission believes that a right of refusal is implied in a request for consent, and therefore is not modifying this provision.

should be included in the notice.[149] One commenter suggested that the notice include a statement recommending that parents warn their children not to post personal information in chat rooms or other public venues.[150] While the Commission does not believe this information should be required in the notice under the COPPA, it strongly encourages parents, operators, and educators to teach children about the dangers of posting personal information in public fora. After reviewing the comments concerning these provisions, the Commission believes that no changes are necessary.

b. Section 312.4(c)(1)(iii) and (iv): Notices under the multiple-contact exception, section 312.5(c)(3), and the child safety exception, section 312.5(c)(4). In cases where an operator wishes to collect a child's name and online contact information for purposes of responding more than once to a specific request of the child under Section 312.5(c)(3), or for the purpose of protecting the safety of a child participating on the website or online service under Section 312.5(c)(4), the operator was required to provide notice to the parent, with an opportunity to opt out of future use or maintenance of the child's personal information. Section 312.4(c)(1) (iii) and (iv) required the operator to notify the parent of the operator's intended use of the information, the parent's right to refuse to permit further contact with the child, or further use or maintenance of the information, and that ''if the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice.'' [151] The Commission received only one comment regarding this provision [152] and has determined that no changes are necessary.

Because the types of contact with children covered under section 312.5(c)(3) and (4) do not require a parent's affirmative consent, the operator must clearly notify the parent that, in these instances, if the parent fails to respond to the notice, the operator may use the information for the purpose stated in the notice.[153] The Commission expects operators to process in a timely manner responses from parents prohibiting the use of their children's information.

D. Section 312.5: Verifiable Parental Consent

1. Section 312.5(a): General Requirements

Section 312.5(a) of the proposed Rule set forth two requirements: (1) That operators obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including any collection, use and/or disclosure to which the parent had not previously consented; and (2) that the operator give the parent the option to consent to collection and use of the child's personal information without consenting to its disclosure to third parties.[154] In the NPR, the Commission also stated that, because the Act required parental consent *prior to any* collection, use, *and/or* disclosure, the parental consent requirement applied to the subsequent use or disclosure of information already in possession of an operator as of the effective date of the proposed Rule.[155]

Commenters generally supported the principle of prior parental consent.[156] However, several argued that, by requiring parental consent for future use of information collected before the effective date of the Rule, the Commission was attempting to apply the Act retroactively.[157] They also stated that it would be extremely costly and burdensome to obtain consent for information collected years ago, especially in instances where they were unaware of a child's past or current age or had no information on how to contact the parents.[158] The Commission is persuaded that the Act should not be interpreted to cover information collected prior to its effective date. While the Act clearly gives parents control over the use and disclosure of information, and not just its collection,[159] it also appears to contemplate that such control be exercised only with regard to information ''collected'' under the Act—*i.e.*, collected after the Act's effective date.[160] Further, the Commission believes that it could be difficult and expensive for operators to provide notice and consent for information collected prior to the Rule's effective date. Therefore, the Commission has eliminated this requirement from the Rule.

The Commission notes, however, that notwithstanding any prior relationship that an operator has with the child, any collection of ''personal information'' by the operator after the effective date is covered by the Rule. Thus, for example, if an operator collected a child's name and e-mail address before the effective date, but sought information regarding the child's street address after the effective date, the later collection would trigger the Rule's requirements. Similarly, if after the effective date, an operator continued to offer activities involving the ongoing collection and disclosure of personal information from children (*e.g.*, a chatroom or message board), or began offering such activities for the first time, notice and consent would be required for all participating children regardless of whether they had previously registered or participated at the site.

The Commission also notes that, for information collected prior to the effective date of the Rule, it retains the authority to pursue unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act. Thus, the Commission will continue to examine information practices in use before the effective date of the COPPA for deception and unfairness, and will

---

[149] 64 FR at 22762.

[150] CBBB (Comment 91) at 13.

[151] 64 FR at 22756, 22765.

[152] CME/CFA et al. (Comment 80) at 12 (generally requesting more information in the notices).

[153] 64 FR at 22757, 22765–66.

[154] 64 FR at 22756, 22765.

[155] *Id.* at 22751.

[156] *See, e.g.*, Gail Robinson (Comment 132); Tessin J. Ray (Comment 131); BAWSELADI (Comment 133); Deb Drellack (Comment 20); Valorie Wood (Comment 36); Deanie Billings (Comment 37); Nancy C. Zink (Comment 38); Susan R. Robinson (Comment 42); Joyce Patterson (Comment 43); Elaine Bumpus (Comment 44); Greg Anderson (Comment 46); Deanna (Comment 47); Mark E. Clark (Comment 48); Sue Bray (Comment 50); Cindy L. Hitchcock (Comment 55); Stephanie Brown (Comment 50); Samantha Hart (Comment 59); Tammy Howell (Comment 59); Jean Hughes (Comment 60); dinky (Comment 61); PrivaSeek (Comment 112) at 2; CDT (Comment 81) at 25; Consumers Union (Comment 116) at 1; EPIC (Comment 115) at 5, 9; FreeZone (IRFA comment 01) at 2; Kidsonline.com (IRFA comment 02) at 1; AAF (Comment 87) at 2; CBBB (Comment 91) at 1–2; CARU (Workshop comment 08) at 3; AAAA (Comment 134) at 2, 5; Mars (Comment 86) at 1; Time Warner (Comment 78) at 10; Viacom (Comment 79) at 9–10; Children's Television Workshop (''CTW'') (Comment 84) at 2, 6. *See also* 144 Cong. Rec. at S11659 (List of Supporters of Children's Internet Privacy Language).

[157] DMA (*citing Landgraf* v. *U.S. Film Products*, 511 U.S. 244 (1994)). *See also* EdPress (Comment 130) at 2; AAF (Comment 87) at 3–4; ANA (Comment 93) at 3–4; Grolier Enterprises (Comment 111) at 4; IDSA (Comment 103) at 7–8; McGraw-Hill (Comment 104) at 5; MPA (Comment 113) at 4; NRF (Comment 95) at 1–2; Time Warner Inc. (Comment 78) at 3–4; Walt Disney Company and Infoseek Corp. (''Disney, et al.'') (Comment 82) at 12–13.

[158] IDSA (Comment 103) at 7; TRUSTe (Comment 97) at 2–3.

[159] *See, e.g.*, 15 U.S.C. 6502(b)(1)(B)(ii) (giving parents the opportunity at any time to refuse to permit further use, disclosure, or maintenance of information collected from their children); 15 U.S.C. 6502(b)(1)(A)(ii) (requiring operators to obtain verifiable parental consent for the collection, use, and/or disclosure of personal information from children).

[160] *See* 144 Cong. Rec. at S11658 (Statement of Sen. Bryan) (stating that parents can opt out of further collection, use, or maintenance of their child's information and that ''[t]he opt out * * * operates as a revocation of consent that the parent has previously given'').

pursue enforcement in appropriate circumstances.[161]

Many commenters also objected to the requirement that operators obtain a new parental consent for any changes to the collection, use, and/or disclosure practices which were the subject of a previous consent.[162] As in the notice section of the Rule,[163] they argued that notification of minor changes would be extremely burdensome, especially in light of constant changes taking place in the online world, and unnecessary to achieve the purposes of the COPPA.[164] As noted above, the Commission agrees that the proposed requirement is unduly broad and would be overly burdensome, and is therefore amending the Rule to make clear that a new parental consent is required only if there is a material change in the operator's collection, use, and/or disclosure practices.

Finally, some commenters objected to the proposed Rule's requirement that parents be given an opportunity to provide consent for the collection and use of information without consenting to its disclosure to third parties.[165] Commenters argued that this requirement is not included in the COPPA and that it interferes with an operator's right under the COPPA to terminate service to a child whose parent refuses to permit further use, maintenance, or collection of the data.[166] Other commenters supported this requirement as important to the protection of children's privacy.[167]

The Commission believes that giving parents a choice about whether information can be disclosed to third parties implements the clear goals of the COPPA to give parents more control over their children's personal information, limit the unnecessary collection and dissemination of that information, and preserve children's access to the online medium.[168] The Act requires consent for the collection, use, or disclosure of information,[169] thus expressing the intent that parents be able to control all of these practices. Although the Act does not explicitly grant parents a separate right to control disclosures to third parties, the Commission believes that this is a reasonable and appropriate construction of the Act, particularly in light of the rulemaking record and other considerations.

Indeed, the record shows that disclosures to third parties are among the most sensitive and potentially risky uses of children's personal information.[170] This is especially true in light of the fact that children lose even the protections of the Act once their information is disclosed to third parties.[171] The Commission believes that these risks warrant providing parents with the ability to prevent disclosures to third parties without foreclosing their children from participating in online activities. In addition, the Act prohibits collecting more information than is reasonably necessary to participate in an activity,[172] showing Congressional intent to limit information practices (such as disclosures to third parties) that do not facilitate a child's experience at the site. Finally, the Commission believes that allowing parents to limit disclosures to third parties will increase the likelihood that they will grant consent for other activities and therefore preserve children's access to the medium.[173]

Thus, the Commission believes that providing parents with a choice about whether their children's information can be disclosed to third parties is within the authority granted by the COPPA, consistent with the rulemaking record, and important to the protection of children's privacy. The Commission is therefore retaining this provision.

2. Section 312.5(b): Mechanisms

Section 312.5(b) of the proposed Rule required that operators make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology.[174] Consistent with the language of the COPPA, the proposed Rule further clarified that the methods used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.[175] In the NPR, the Commission provided examples of methods that might satisfy these standards, and sought comment on the feasibility, costs, and benefits of those methods, as well as any others that the Commission should consider.[176] To gather additional relevant information, the Commission held a workshop devoted solely to this issue.[177]

While commenters and participants at the workshop generally supported the concept of prior parental consent, they differed on what would constitute a verifiable mechanism under this provision. In particular, there was considerable debate over whether e-mail based mechanisms could provide adequate assurance that the person providing consent was the child's parent.

---

[161] *See GeoCities,* Docket No. C–3849 (Final Order Feb. 12, 1999); *Liberty Financial Cos., Inc.,* Docket No. C–3891 (Final Order Aug. 12, 1999). *See also* Staff Opinion Letter, July 17, 1997, issued in response to a petition filed by the Center for Media Education, at <*www.ftc.gov/os/1997/9707/cenmed.htm*>.

[162] IDSA (Comment 103) at 5–6; CBBB (Comment 91) at 13–14; DMA (Comment 89) at 26; Aftab & Savitt (Comment 118) at 5; ANA (Comment 93) at 6–7.

[163] *See* Section II.C.4, *supra.*

[164] One commenter supported this provision on the basis that not requiring it would render parental consent meaningless. Attorneys General (Comment 114) at 10. However, even one commenter who supported the requirement still expressed concern that parents might be ''badgered'' by too many of these requests. CME/CFA et al. (Comment 80) at 13.

[165] Section 312.5(a)(2). *See, e.g.,* DMA (Comment 89) at 25; NRF (Comment 95) at 4; McGraw-Hill (Comment 104) at 7; PMA (Comment 107) at 11.

[166] ANA (Comment 93) at 6; IDSA (Comment 103) at 4–5; DMA (Comment 89) at 25; PMA (Comment 107) at 11 (all referring to section 312.6(c) of the proposed Rule and 15 U.S.C. 6502(b)(3)). The purpose of that provision was to enable operators to offer some online activities that require children to provide personal information, *e.g.,* chat rooms, which may require the operator to collect an e-mail address for security purposes. Under that provision, operators may bar children whose parents have revoked consent for the operator's use of the necessary information from participating in those activities. The Commission does not believe that disclosure to outside parties—other than those, such as fulfillment services, that provide support for the internal operations of the website—is reasonably necessary for an operator to provide online activities.

[167] EPIC (Comment 115) at 9–10; Junkbusters (Comment 66) at 1. *See also* CDT (Comment 81) at 25; CME/CFA et al. (Comment 80) at 13; Sovern (Comment 33) at 4; Mars (Comment 86) at 12–13; TRUSTe (Comment 97) at 2.

[168] *See, e.g.,* 144 Cong. Rec. at S11657, S11658 (Statement of Sen. Bryan).

[169] 15 U.S.C. 6502(b)(1)(A)(ii).

[170] *See* CME/CFA et al. (Comment 80) at 26–27; Mars (Comment 86) at 13; Kraft (Comment 67) at 4–5; Viacom (Comment 79) at 13–14. *See also* Attorneys General (Comment 114) at 4 (*citing* 1997 survey showing that 97% of parents whose children use the Internet believe that website operators should not sell or rent children's personal information).

[171] Thus, for example, parents cannot access information in the possession of third parties, or require that it be deleted, as they can for operators subject to the Rule. *See* 15 U.S.C. 6502(b)(1)(B)(ii),(iii). Nor can they prohibit future use of information in the possession of third parties. *Compare* 15 U.S.C. 6502(b)(1)(B)(ii). In fact, parents are likely to be unaware of the identities and specific information practices of many of the third parties that obtain their children's information. *See* Section II.C.3.d, *supra* (operators need only disclose types of business engaged in by third parties and whether those third parties have agreed to maintain the confidentiality, security, and integrity of personal information received from operator).

[172] 15 U.S.C. 6502(b)(1)(C) (prohibiting an operator from conditioning participation on the disclosure of more information than necessary to participate in an activity).

[173] One study found that 97% of parents online did not want their children's information disclosed to third parties, suggesting that those parents would be more likely to grant consent if they could limit such disclosures. Louis Harris & Associates and Dr. Alan F. Westin, ''Commerce, Communication, and Privacy Online: A National Survey of Computer Users,'' 1997, at 75.

[174] 64 FR at 22756, 22765.

[175] *Id.*; 15 U.S.C. 6501(9).

[176] 64 FR at 22756.

[177] 64 FR at 34595.

Because of concerns that a child using e-mail could pretend to be a parent and thereby effectively bypass the consent process,[178] some commenters favored methods that would provide additional confirmation of the parent's identity.[179] These include use of a form to be signed by the parent and returned to the operator by postal mail or fax (''print-and-send''); (2) use of a credit card in connection with a transaction; (3) having the parent call a toll-free number staffed with trained personnel; (4) use of e-mail accompanied by a valid digital signature; and 5) other electronic methods that are currently available or under development.

Some commenters took the position that print-and-send was the method least subject to falsification;[180] they also noted that, because it is used by schools, most parents are familiar with it.[181] In addition, participants at the workshop noted that industry members currently use print-and-send to ensure that they are obtaining parental permission in certain circumstances—for example, when obtaining consent to publish a child's art work or letter, or to send a contest winner a prize.[182] Commenters also supported the use of credit cards in obtaining parental consent on the grounds that few, if any, children under the age of 13 have access to credit cards.[183] With regard to the use of a toll-free number, commenters and workshop participants noted that, with proper training, employees can easily learn to differentiate between children and adult callers, and that parents prefer this method.[184] Commenters also supported use of digital signatures to obtain consent, stating that they would effectively verify identity and are currently available.[185] Finally, testimony at the workshop showed that there are a number of other electronic products and services that are available now, or under development, that could be used to confirm a parent's identity and obtain consent. These included services that would provide a parent with a digital signature, password, PIN number, or other unique identifier after determining that the person seeking the identifier is an adult.[186]

Many commenters, however, criticized some of these methods for the costs and burdens they are likely to impose on operators. Regarding print-and-send, one commenter cited a figure of $2.81 per child to process mailed or faxed parental consent forms.[187] Another noted an 80% decline in online subscriptions to its magazine when it switched from an online subscription model to a form that had to be downloaded and mailed.[188] Still others pointed out that there is no way to authenticate a signature to be sure that it is actually the parent who has signed the form.[189]

Regarding the use of credit cards, commenters noted that operators would be charged a fee for each transaction,[190] that not every parent has a credit card,[191] and that some parents do not

[178] This is of particular concern where a child shares an e-mail account with a parent, which is a common practice. *See* CME/CFA et al. (Comment 80) at 28; APA (Comment 106) at 2; Attorneys General (Comment 114) at 11; AETN (Comment 90) at 17–18. In fact, one workshop participant reported that 40% of its registered parents shared an e-mail address with their children. Aledort/Disney (Workshop Tr.153). Another participant reported that 10–20% of its registered parents shared the same e-mail address as their children. Herman/iCanBuy.com (Workshop Tr 153–54).

[179] CME/CFA et al. (Comment 80) at 28; APA (Comment 106) at 1–2; Nat'l Ass'n of Elementary School Principals (''NAESP'') (Comment 96) at 1; CARU (Workshop comment 08) at 1–2; Consumers Union (Comment 116) at 5–6. *See also* Attorneys General (Comment 114) at 11 (supporting the traditional offline consent methods). One commenter stressed the need for a high standard for parental consent because children under the age of 13 do not have the developmental capacity to understand the nature of a website's request for information and its implications for privacy. APA (Comment 106) at 1–2.

[180] CBBB (Comment 91) at 18; CARU (Workshop comment 08) at 2; NAESP (Comment 96) at 1.

[181] NAESP (Comment 96) at 1. This commenter noted that young children rarely falsify their parents' signatures. *Id. See also* Douglas L. Brown (Comment 21); Don and Annette Huston (Comment 22).

[182] Bagwell/MTV Networks Online (Workshop Tr. 30, 35); Randall/MaMaMedia (Workshop Tr. 28); Aledort/Disney (Workshop Tr. 151); FreeZone Network (IRFA comment 01) at 2; Aftab & Savitt (Comment 118) at 6. One comment identified four children's websites that have implemented offline consent mechanisms pursuant to the CARU guidelines. CARU (Workshop comment 08) at 2; *see also* CBBB (Comment 91) at 23.

[183] AOL (Comment 72) at 18–19; iCanBuy.com (Comment 101) at 1; Mars (Comment 86) at 13. Among other things, credit cards can be used to set up a ''master account'' for the parent with an e-mail address to be used exclusively by the parent. Curtin/AOL (Workshop Tr. 36–7); Aftab (Comment 117) at 3. *See also* KidsOnLine.com (Comment 108) at 3; Talk City (Comment 110) at 3 (supporting the use of a credit card as a method of consent).

[184] CARU (Workshop comment 08) at 2; CME/CFA et al. (Comment 80) at 14; Aftab (Workshop Tr. at 52).

[185] *See* Brandt/VeriSign (Workshop Tr. 199–202) and (Comment 99) at 1–4 (stating that one year to 18 months would be sufficient time for testing and adoption of digital technology applications); Teicher/CyberSmart! (Workshop Tr. 191–92, 199); Lucas/PrivaSeek (Workshop Tr. 244–45, 299–300) and (Comment 112) at 4 (noting that the next step is the adoption of digital signatures by online businesses so that they can be made widely available to consumers); Hill/ZeroKnowledge (Workshop Tr. 269–73); Johnson/Equifax Secure, Inc. (Workshop Tr. 250–59).

[186] For example, one workshop participant described a service now under development which would use schools to assist in issuing a digital certificate to a child after obtaining parental consent. Teicher/CyberSmart! (Workshop Tr. 190–94; 196–97; 199). Another announced that his portal site would soon launch an e-mail authentication system that could verify the age or profession of a person, and then assign that person an e-mail address associated with his age or status, *e.g., John.doe@validadult.com; Mary.teacher@validteacher.com*. Ismach/BizRocket.com (Workshop comment 12) at 1–3; (Workshop Tr. 231–232). Still another has developed a permission-based infomediary service that will enable consumers to set their preferences as to how their information may be disclosed online. PrivaSeek (Comment 112) at 1. Under this service, which is expected to be launched by the end of the year, a parent could be assigned a password or digital signature following initial verification. The charge to participating websites is anticipated to be $0.10-$0.20 per name. Lucas/PrivaSeek (Workshop Tr. 242–49); PrivaSeek (Comment 112) at 1.

In addition, another company is currently providing digital credentials (a certificate, PIN or password) to consumers after authenticating their identity. The company estimates that the cost for sites to use this service is $3 to $4 per customer. Johnson/Equifax Secure (Workshop Tr. 249–59). Another company offers a service that enables a child to make purchases, with a parent's permission, at participating websites. Parents use a credit or debit card to establish an account and then authorize the sites to be accessed and the amounts to spend. Herman/iCanBuy.com (Workshop Tr. 185–190). Yet another company is also planning to launch (by spring 2000) a free verification service that uses both credit and bank cards in conjunction with algorithms to verify the validity of the card numbers. The card number would be checked at the consumer's browser and would not be collected or transferred over the Internet, addressing some consumers' concerns about using credit cards online. Oscar Batyrbaev (Comment 125) at 1; Batyrbaev/eOneID.com (Workshop Tr. 235–39). Parents without online access will be able to obtain verification by telephone. *Id.*

Finally, another online company will provide parents and children with digital pseudonyms that, following initial verification using a digital signature, can be used to verify identity. Hill/ZeroKnowledge (Workshop Tr. 268–73). *See also* Brandt/VeriSign (Workshop Tr. 195–96, 199–202).

[187] Clarke/KidsCom.com (Workshop Tr. 22). *See also* Cartoon Network et al. (Comment 77) at 8 (estimating that cost to open and sort written consent forms is about $0.08 to $0.31 per child). Another comment estimated that the cost per consent by fax and mail, including overhead, were $0.94 and $0.89, respectively. Zeeks.com (IRFA comment 05) at Attachment (''Compliance Cost Estimate'').

[188] Time Warner (Comment 78) at 11. Other commenters stated that offline methods might be inconvenient or labor-intensive for parents. Dell (Comment 102) at 2; Cartoon Network et al. (Comment 77) at 6; DMA (Comment 89) at 6–8; Grolier (Comment 111) at 1–2.

[189] Richard Storey (Comment 02) at 1; PMA (Comment 107) at 3–4, 10; PrivaSeek Inc. (Comment 112) at 3.

[190] Disney et al. (Comment 82) at 8; MPA (Comment 113) at 5; DMA (Comment 89) at 7. Two comments stated that credit cards cost up to $3 per verification to process. Cartoon Network et al. (Comment 77) at 10–11; DMA (Comment 89) at 7. One company experienced costs ranging from $2 to $3 per verification. Aftab (Workshop Tr. 17).

[191] McGraw-Hill (Comment 104) at 3; Cartoon Network et al. (Comment 77) at 9; KidsOnLine.com (Comment 108) at 3; DMA (Comment 89) at 7. Some commenters also thought consumers might be troubled by the privacy implications of divulging personal information for the purpose of granting consent. Brian Burke (Comment 05); Disney et al. (Comment 82) at 9; PrivaSeek (Comment 112) at 3; Cartoon Network et al. (Comment 77) at 9–10; PMA

like to use credit cards online.[192] One credit card company opposed the use of credit cards in this manner because it could foster unauthorized use and undermine systems used to detect fraud.[193] Commenters also noted that the use of a toll-free number would require operators to hire personnel just to answer phones, and would therefore be costly.[194] Finally, a number of commenters contended that while digital signatures and other electronic methods may be promising alternatives, they are not yet widely available, and therefore are impracticable as current methods of compliance.[195]

In response to a request for comment on whether e-mail alone would satisfy the Act's requirements, commenters presented a variety of views. A number of commenters opposed use of e-mail on the grounds that it is easily subject to circumvention by children.[196] While a significant number of commenters advocated the use of e-mail,[197] most of them acknowledged that taking additional steps in conjunction with e-mail would increase the likelihood that the consent was submitted by the parent and not the child.[198] Such steps would include: the use of PIN numbers or passwords; [199] sending follow-up e-mails to the parent to increase the likelihood that the parent will see the request for consent; [200] or allowing e-mail consent only if the parent and child have different e-mail addresses.[201] Still others recommended including in the e-mail questions to which the child would be unlikely to know the answer.[202]

Finally, many commenters urged the Commission to temporarily adopt a standard under which the consent mechanism required would depend upon how the operator intended to use the information (*i.e.*, a ''sliding scale'').[203] Such an approach would permit operators to obtain consent at a reasonable cost until secure electronic mechanisms become more widely available and affordable. Generally, these commenters advocated use of an e-mail based mechanism for purposes of consenting to an operator's *internal* use of information, such as an operator's marketing to a child based on the child's preferences, but a ''higher'' method of consent, such as use of a credit card or print-and-send form, for purposes of consenting to activities that present greater risks to children.[204] In comments and at the workshop, commenters cited public postings by children (*e.g.*, in chat rooms and on bulletin boards), as well as disclosures of information to third parties, as activities that pose such risks.[205] Other commenters opposed the ''sliding scale'' on the ground that it could permit the use of consent mechanisms that fall short of the COPPA's requirements.[206]

In determining whether a particular method of obtaining consent is ''verifiable'' under the COPPA, the Commission must consider: (1) whether the method ensures that it is the parent providing the consent; and (2) whether the method is a ''reasonable effort,'' taking into consideration available technology. In determining what is a ''reasonable effort'' under the COPPA, the Commission believes it is also appropriate to balance the costs imposed by a method against the risks associated with the intended uses of the information collected. Weighing all of these factors in light of the record, the Commission is persuaded that temporary use of a ''sliding scale'' is an appropriate way to implement the requirements of the COPPA until secure electronic methods become more available and affordable.

The record shows that certain methods of consent—print-and-send, credit card, toll-free number with trained personnel, and digital signature—provide appropriate assurances that the person providing consent is the child's parent, and thus satisfy the first part of the inquiry.[207] In addition, testimony at the Commission's workshop shows that a number of electronic products and services, which could also be used to verify a parent's identity and obtain consent, are currently available or under development.[208] The record also shows, however, that some of these methods may be costly and others may not be widely available at the present time.

(Comment 107) at 110; EPIC (Comment 115) at 10; DMA (Comment 89) at 7; Viacom (Comment 79) at 11.

[192] Cartoon Network et al. (Comment 77) at 9–11; DMA (Comment 89) at 7; PMA (Comment 107) at 10; Viacom (Comment 79) at 11.

[193] Visa USA, Inc. (Comment 75) at 2. The Commission recognizes that there may be risks in using credit cards for this purpose, but notes that this method is already being used for similar purposes—for example, to verify that a person is over 18 for purposes of obtaining access to adult materials online. *See* amicus of Senators Oxley and Coates; eOneID.com (Workshop comment 09) at Appendix A.

[194] Alison J. Richards (Comment 105) at 1; MPA (Comment 113) at 5; Cartoon Network et al. (Comment 77) at 11–2. One commenter estimated that the cost for telephone consents would be $0.97 for an automated answering system, the tapes of which would then need to be manually swept to weed out children and enter data into the system. Zeeks.com (IRFA Comment 05) at Attachment (''Compliance Cost Estimate''). Another commenter estimated the cost of a live operator to be $55 per hour plus training costs. Cartoon Network et al. (Comment 77) at 12.

[195] Richard Storey (Comment 02) at 1; Viacom (Comment 79) at 12; Disney et al. (Comment 82) at 8–9; DMA (Comment 89) at 5; Alison J. Richards (Comment 105) at 1; Amazon.com (Comment 109) at 3; Cartoon Network et al. (Comment 77) at 13–15; Grolier (Comment 111) at 1; CBBB (Comment 91) at 16–17.

[196] Attorneys General (Comment 114) at 11; Robert F. Reid (Comment 06); Joseph C. DeMeo (Comment 08); Patrick O'Heffernan (Comment 17); NAESP (Comment 96) at 1; APA (Comment 106) at 2; Consumers Union (Comment 116) at 5; CME/CFA et al. (Comment 80) at 15.

[197] Cartoon Network et al. (Comment 77) at 15–18; Disney et al. (Comment 82) at 7–9; Time Warner (Comment 78) at 10–11; DMA (Comment 89) at 5–6. Several commenters stated that Congress must have intended e-mail to be used for consent purposes because the Act allows online contact information to be collected for the purpose of seeking parental consent. *Id.* (*citing* 15 U.S.C. 6502(b)(2)(B)). Some commenters stated that, in their experience, parents preferred to use e-mail to grant consent. Bagwell/MTV Networks Online (Workshop Tr. 33–34); Aftab (Workshop Tr. 31).

[198] *See* Aledort/Disney (Workshop Tr. 149–51); Bruening/TRUSTe (Workshop Tr. 39); CARU (Workshop comment 08) at 2; Viacom (Comment 79) at 13; Cartoon Network et al. (Comment 77) at 17; NRF (Comment 95) at 4.

[199] AAAA (Comment 134) at 2; ANA (Comment 93) at 2; Talk City (Comment 110) at 3.

[200] Disney et al. (Comment 82) at 9; DMA (Comment 89) at 6.

[201] AAAA (Comment 134) at 2; ANA (Comment 93) at 2; NRF (Comment 95) at 4; MPA (Comment 113) at 5; DMA (Comment 89) at 6. The Commission notes that, because children can easily obtain multiple e-mail addresses from free e-mail services, this method may not ensure verifiability.

[202] NRF (Comment 95) at 4; Cartoon Network et al. (Comment 77) at 17; Time Warner (Comment 78) at 11; DMA (Comment 89) at 6. The Commission notes that this method could pose problems if it requires operators to verify the ''answer'' to the questions, or if the child is reasonably sophisticated.

[203] *See, e.g.*, Cartoon Network et al. (Comment 77) at 18 (suggesting that sliding scale sunset in five years); DMA (Workshop comment 02) at 1–3 (suggesting that the Commission reexamine the scale after a specific period of time or at a point when technology has changed); Viacom (Comment 79) at 9–10, 12–14 (five year sunset date); Kraft (Comment 67) at 5; Bagwell/MTV Networks Online (Workshop Tr. 32–33); CBBB (Comment 91) at 15–18; CTW (Comment 84) at 6–7; CARU (Workshop Comment 08) at 1–2; Mars (Comment 86) at 13–14; PMA (Comment 107) at 4, 11. *See also* Herman/iCanBuy.com (Workshop Tr. 209) (if adopted, should sunset within 12–18 months); Teicher/CyberSmart! (Workshop Tr. 199) (predicting significant changes in technology that would permit sunset within 18 months).

[204] Bagwell/MTV Networks Online (Workshop Tr. 32–33); Kraft (Comment 67) at 5.

[205] Kraft (Comment 67) at 4–5; Cartoon Network et al. (Comment 77) at 18; ANA (Comment 93) at 2; CBBB (Comment 91) at 15–18; PMA (Comment 107) at 11; CARU (Workshop Comment 08) at 1; Viacom (Comment 79) at 13; and Bagwell/MTV Networks Online (Workshop Tr. 33). The legislative history also reflects special concern for children's safety in such online fora as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information. *See* 144 Cong. Rec. S11657 (Statement of Sen. Bryan).

[206] *See, e.g.*, CME/CFA et al. (Comment 80) at 7.

[207] Print-and-send and digital signatures were listed as acceptable consent mechanisms in Senator Bryan's Floor Statement. *See* 144 Cong. Rec. S11657.

[208] *See* note 186, *supra*, describing such services.

Therefore, under the second prong of the inquiry, the Commission believes that, until reliable electronic methods of verification become more available and affordable, these methods should be required only when obtaining consent for uses of information that pose the greatest risks to children.

Thus, under the ''sliding scale,'' the more reliable methods of consent will be required for activities involving chat rooms, message boards, disclosures to third parties, and other ''disclosures'' as defined in Section 312.2 of the Rule.[209] As noted above, these methods include the methods identified in the NPR (print-and-send, credit card, toll-free number, and digital signatures),[210] as well as other reliable verification products and services to the extent that they are currently available. To minimize costs, the Rule makes clear that such methods also include the use of e-mail, as long as it is accompanied by a PIN or password obtained through one of the above procedures.[211]

For internal uses of information, operators will be permitted to use e-mail to obtain consent, as long as some additional steps are taken to provide assurances that the parent is providing the consent. Based on the comments, the Commission is persuaded that e-mail alone does not satisfy the COPPA because it is easily subject to circumvention by children.[212] The additional steps include sending a delayed confirmatory e-mail to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent[213] and confirming the parent's consent by letter or telephone call.[214] If such consent mechanisms are used, the operator must notify parents that they can revoke any consent given in response to the earlier e-mail.

Based on evidence in the record, the Commission believes that use of a ''sliding scale'' is necessary only in the short term, and that, with advances in technology, companies will soon be able to use more reliable verifiable electronic methods in all of their transactions.[215] Indeed, as noted above, the record shows that a number of products and services, including digital signatures, will soon be more widely available to facilitate verifiable parental consent at reasonable cost. The Commission therefore plans to phase out the ''sliding scale'' two years from the effective date of the Rule (*i.e.*, April 2002), unless presented with evidence showing that the expected progress in available technology has not occurred.[216] The Commission will conduct a review of this issue, using notice and comment, approximately eighteen months from the effective date of the Rule (*i.e.*, in October 2001).

The Commission believes that temporary adoption of this ''sliding scale'' fulfills the statutory requirement that efforts to provide ''verifiable parental consent'' be ''reasonable.'' It provides operators with cost-effective options until more reliable electronic methods become available and affordable, while providing parents with the means to protect their children.

3. Section 312.5(c): Exceptions to Prior Parental Consent

The COPPA sets forth five exceptions to the general requirement that operators obtain verifiable parental consent before collecting personal information from children.[217] These limited exceptions were intended to facilitate compliance with the Rule, allow for seamless interactivity in a wide variety of circumstances, and enable operators to respond to safety concerns.[218] Indeed, many of the concerns raised by the commenters, are, in fact, addressed in these exceptions.[219]

This subsection of the proposed Rule permitted an operator, without prior parental consent, to collect: (1) a parent's or child's name and online contact information to seek parental consent or to provide parental notice;[220] (2) a child's online contact information in order to respond on a one-time basis to a specific request of the child (e.g., to provide one-time homework help or to send a document);[221] (3) a child's online contact information in order to respond directly more than once to a specific request of the child (e.g., to provide an online magazine subscription, or a contest entry and subsequent award)[222] when such information is not used to contact the child beyond the scope of that request, and the operator provides the parent with notice and an opportunity to opt-out;[223] and (4) the name and online contact information of the child to the extent reasonably necessary to protect the safety of a child participating on the website.[224] Furthermore, under the proposed Rule, the operator may collect, use, or disseminate such information as necessary to protect the security or the integrity of the site or service, to take precautions against liability, to respond to judicial process, or, to the extent permitted under other provisions of law,

---

[209] *See also* 15 U.S.C. 6501(4).

[210] 64 FR at 22756.

[211] For example, there may be verifying services available to operators that would verify a parent's identity and then provide the parent with a PIN or password for use with e-mail. Upon receipt of the parent's consent via e-mail, an operator could confirm the parent's identity with the verifying service. Similarly, as noted above, an operator could use e-mail, as long as it were sent through an account set up by an adult using a credit card (a ''master account''), and reserved for the adult's use. *See* note 184, *supra*.

[212] Attorneys General (Comment 114) at 11; Robert F. Reid (Comment 06); Joseph C. DeMeo (Comment 08); Patrick O'Hefferman (Comment 17); NAESP (Comment 96) at 1; APA (Comment 106) at 2; Consumers Union (Comment 116) at 5; CME/CFA et al. (Comment 80) at 28. In particular, where a parent and child share the same e-mail account, as is often the case, a child may easily pretend to be the parent and provide consent for himself. *See* note 179, *supra*.

[213] The Commission expects that operators will keep confidential any information obtained from parents in the course of obtaining parental consent or providing for parental review of information collected from a child.

[214] One variation on this approach would require not only a confirmatory e-mail to the parent, but also a response from the parent confirming the consent. Aledort/Disney (Workshop Tr. 149–150). *See also* Disney (Workshop comment 06) at 12. Using this method, one workshop participant reported that 33% of parents granted consent; 30% declined consent; and 37% never responded. Aledort/Disney (Workshop Tr. 152).

[215] Likewise, with advances in technology, the use of e-mail (without the more reliable methods of verification) may no longer be regarded as a ''reasonable effort'' under the Rule.

[216] Comments and testimony at the workshop showed that digital signatures and other reliable electronic methods are likely to be widely available and affordable within approximately a year to eighteen months from the July 1999 the workshop. *See* Brandt/VeriSign (Workshop Tr. 199–202). *See also* note 188, *supra* (other secure electronic methods are available now or will be available within a year from the date of the workshop). Thus, the proposed Rule's longer timetable for implementing the ''sliding scale''—two years from the Rule's effective date or almost *three* years from the date of the workshop—should provide ample time for these mechanisms to develop and become widely available.

[217] 15 U.S.C. 6502(b)(2).

[218] *See* 144 Cong. Rec. S11658 (Statement of Sen. Bryan).

[219] *See, e.g.*, Section II.A.8, *supra*, regarding the use of the exception to maintain website security.

[220] Section 312.5(c)(1).

[221] Section 312.5(c)(2). This exception also requires that the operator not use the information to recontact the child and that the operator delete the information from its records. If the website wishes to retain the child's e-mail address for future homework assistance, then it would fall into the scope of the exception in section 312.5(c)(3) and require parental notice and opt-out. Moreover, if the operator wishes to use the information collected under this—or any other—exception for other purposes, then the operator must follow the notice and consent requirements of the Rule.

[222] Section 312.5(c)(3). Sending an electronic postcard where the website retains the online contact information until the postcard is opened would fall under this exception. However, where the operator's postcard system sends the requested postcard without maintaining the online contact information, this collection would fall under section 312.5(c)(2).

[223] Section 312.5(c)(3).

[224] Section 312.5(c)(4). For example, operators may collect online contact information from children participating in their chat rooms in order to report to authorities a child's claim that he is being abused.

to provide information to law enforcement agencies or for an investigation related to public safety.[225] A workshop participant noted that these exceptions include some of the most popular and common online activities.[226]

A number of commenters had specific suggestions with regard to modifying the exceptions.[227] However, the Commission believes that the exceptions, which closely track the statutory language, strike the appropriate balance between an operator's legitimate need to collect information without prior parental consent and the safety needs of children. It is therefore retaining the language of the exceptions as proposed.

4. Response to Comments Requesting an Exception for Information Collection in the Educational Setting

Numerous commenters raised concerns about how the Rule would apply to the use of the Internet in schools.[228] Some commenters expressed concern that requiring parental consent for online information collection would interfere with classroom activities, especially if parental consent were not received for only one or two children.[229] In response, the Commission notes that the Rule does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parents' agent in the process. For example, many schools already seek parental consent for in-school Internet access at the beginning of the school year. Thus, where an operator is authorized by a school to collect personal information from children, after providing notice to the school of the operator's collection, use, and disclosure practices, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent.

Operators may wish to work with schools to educate parents about online educational activities that require websites to collect personal information in the school setting. To ensure effective implementation of the Rule, the Commission also intends to provide guidance to the educational community regarding the Rule's privacy protections.

E. Section 312.6: Right of Parent To Review Personal Information Provided by Child

Section 312.6 of the proposed Rule set forth the requirements for providing parental access to personal information collected from the child, including what information must be disclosed and how the parent could be properly identified.[230] In the NPR, the Commission sought comment regarding methods of identification, particularly in non-traditional family situations, and technological advances under development that might ease the process.[231]

1. Access to Information

The proposed Rule contemplated a two-step approach to parental review under §§ 312.6(a) (1) and (3). First, upon request of a properly identified parent, the operator was required to tell the parent what types of personal information have been collected from the child (*e.g.*, ''Your child has given us his name, address, e-mail address, and a list of his favorite computer games''). Second, if requested, the operator was required to provide the specific personal information collected from the child.[232]

One commenter suggested that operators be required to provide parents with the option of directly requesting the specific information collected.[233] As was explained in the NPR, operators, after obtaining proper identification, can in fact skip the first step relating to disclosure of the types of information collected, and simply allow parents to review the specific information.[234] Section 312.6(a) was not intended to mandate unnecessary steps, but rather to allow for flexibility for all parties. In some instances, parents may be satisfied with learning the types of information collected and may not need to see the specific personal information provided by the child. Similarly, if a parent asks only for the specific information collected from the child, the operator need not first provide a general list of the categories of information collected.[235]

Another commenter called for operators to provide information within a reasonable time or within a specified number of days, and suggested that information should be provided to parents on an ongoing basis.[236] The Commission declines to prescribe a specific time period applicable to all parental requests for information, but expects that operators will respond to such requests promptly and without imposing undue burdens on parents. In addition, the Commission believes that requiring operators to provide information to the parent on an ongoing basis would be unduly burdensome for both operators and parents, who may not need or want this information from the operator.

2. Parent's Right To Review Information Provided by the Child

Sections 312.6(a)(2) and (3) of the proposed Rule allowed parents to review, change, and delete personal information collected from their children.[237] Many commenters objected to granting parents the right to change information,[238] asserting that it was unduly burdensome and went beyond the language of the Act.[239] Other commenters noted that a right to alter data is much broader than the right to correct data,[240] and expressed concern that parents might use this right to

[225] Section 312.5(c)(5). Thus, an operator may collect limited information in order to protect the security of its site, for example, from hackers.

[226] Sehgal-Kolbet/CARU (Workshop Tr. 40–41). *See also* CARU (Workshop comment 08) at 2–3.

[227] For example, some commenters suggested that the Rule define ''a reasonable time'' for obtaining consent and deleting information under section 312.5(c)(1). PMA (Comment 107) at 12; Mars (Comment 86) at 14; CBBB (Comment 91) at 19; CME/CFA et al. (Comment 80) at 14. *See also* CDT (Comment 81) at 27. The Commission believes that the time period for obtaining consent may vary depending on the mechanism used; however, it expects operators to delete information obtained under this exception in a timely manner.

[228] Association of American Publishers (''AAP'') (Comment 70) at 4–5; EdPress (Comment 130) at 1–2; MaMaMedia (Comment 85) at 3–4; ZapMe! (Comment 76) at 4–5; ALA (Comment 68) at 2–3.

[229] *Id.*

[230] 64 FR at 22757–58, 22766.

[231] 64 FR at 22762–63.

[232] 64 FR at 22757–22758.

[233] CME/CFA et al. (Comment 80) at 16.

[234] 64 FR at 22758 n.11. However, as noted in the discussion of parental verification below, the Commission has modified the Rule to require proper identification only for access to the child's specific personal information, not for the types of information collected, as originally proposed.

[235] One commenter suggested that parental access be limited in cases where the operator has collected minimal personal information, such as an e-mail address for the sole purpose of sending a periodic newsletter or similar mailing, to a simple confirmation that the child is on the mailing list. AOL (Comment 72) at 19. In response, the Commission notes that the COPPA requires access to all information collected from children, regardless of the circumstances. *See* 15 U.S.C. 6502(b)(1)(B).

[236] Sovern (Comment 33) at 5.

[237] 64 FR at 22757–58, 22766.

[238] *See* NRF (Comment 95) at 4; DMA (Comment 89) at 17–19; ANA (Comment 93) at 6; MPA (Comment 113) at 5–6. *See also* McGraw-Hill (Comment 104) at 8.

[239] Commenters also asserted that allowing parents to change the information provided by their children threatens the confidentiality, security, and integrity of information in the operator's possession, putting the operator in jeopardy of violating section 312.8 of the Rule. *See* NRF (Comment 95) at 4; DMA (Comment 89) at 17–19; MPA (Comment 113) at 5–6. *See* also McGraw-Hill (Comment 104) at 8; Section II.G, *infra*. Two commenters also stated that this provision was unnecessary in light of the parent's right under section 312.6(a)(2) to prohibit further collection, use, and maintenance of information and to have information deleted. NRF (Comment 95) at 4; MPA (Comment 113) at 5–6.

[240] DMA (Comment 89) at 17–18; MPA (Comment 113) at 5–6.

change or delete grades or test scores at educational sites in conflict with federal education statutes and state policies.[241]

Based on the comments, the Commission is revising the Rule to eliminate the proposed Rule's requirement that parents be allowed to change information provided by their children. Even in the absence of a regulatory requirement, however, the Commission believes that operators may choose to permit parents to correct data given operators' strong incentives to maintain accurate information.[242] The Commission also agrees that the opportunity to refuse to permit further use or to delete information under section 312.6(a)(2) adequately protects the interests of the child and parent in this context.

One commenter noted that a child may not want a parent to know about certain information—for example where the child is seeking guidance regarding problems with the parent.[243] The Act does not give the Commission the authority, however, to exempt certain kinds of information from the right of parental review.

Another commenter asked the Commission to consider whether a parent's request to delete data should also extend to third parties who have received that information from the operator.[244] As noted above, the Act covers the actions of ''operators,'' not third parties. However, the Commission encourages operators to structure their contractual arrangements with third parties to require compliance with requests for deletion where practicable.

One commenter asked whether and how long an operator would be required to maintain personal information for review.[245] More specifically, the commenter requested that the Commission revise the Rule to include a statement that an operator is not required to maintain all personal information collected from the child indefinitely in anticipation of a subsequent request for review by a parent.[246] This is particularly important, noted the commenter, where an operator wishes to delete personal information quickly—for example when monitoring a chat room or message board.[247] The Commission does not believe it is necessary to so modify the Rule, but reiterates that if a parent seeks to review his child's personal information after the operator has deleted it, the operator may simply reply that it no longer has any information concerning that child.

Another commenter asserted that Congress did not intend that an operator be required to scour all of its databases for all personal information about a child, whether collected online or offline, in response to a request from the parent.[248] As currently amended, the Rule applies only to personal information submitted online,[249] and, therefore, a parent's access rights under the Act do not generally extend to data collected offline.[250] Nevertheless, if an operator maintains the information such that its source (online or offline) cannot be determined, the Commission would expect the operator to allow the parent to review all of the information. Similarly, if the operator has collected information prior to the effective date of the Rule, but maintains it in a database with information collected online after the effective date in such a way that its source cannot be determined, then the operator should allow the parent access to all of the information.

3. Right To Prohibit Further Use and Collection of the Child's Information

Section 312.6(a)(2) of the proposed Rule allowed parents to refuse to permit the operator's further use or collection of the child's personal information and to direct the operator to delete the information.[251] One commenter asserted that, according to the legislative history, the parental opt-out serves as a revocation of previous consent but does not preclude the operator from seeking consent from the parent for the same or different activities in the future.[252] Therefore, this commenter suggested revising the provision to specify that the refusal was limited to activities covered ''under the consent previously given.'' [253] The Commission agrees with the commenter's interpretation of this provision, but believes that such a modification is not necessary. The Act requires operators to allow parents to refuse to permit further use or future collection of personal information from their children.[254] Operators, however, are free to request a new consent from a parent if the child seeks to participate at the site in the future.[255]

4. Parental Verification

The COPPA requires operators to provide parents with ''a means that is reasonable under the circumstances for the parent to obtain any personal information collected from [the] child.'' [256] In recognition of the danger inherent in requiring an operator to release a child's personal information, the Commission, in section 312.6(a) of the proposed Rule, required operators to ensure that the person seeking to review such information was the child's parent, taking into account available technology, without unduly burdening the parent.[257] In the NPR, the Commission suggested appropriate means of complying with this provision, including using a password in conjunction with the parental consent process.[258]

Some commenters contended that parental verification was not necessary for access to the types or categories of personal information collected from the child under § 312.6(a)(1).[259] The Commission agrees, particularly since the same types or categories of information must already be disclosed

---

[241] AAP (Comment 70) at 4; McGraw-Hill (Comment 104) at 4, 8.

[242] One commenter observed that sites should be willing to permit changes as a matter of good customer service if any information is inaccurate. NRF (Comment 95) at 4. Similarly, another commenter noted that it, and many other organizations, already permit customers to correct data in some way. McGraw-Hill (Comment 104) at 8.

[243] MPA (Comment 113) at 5.

[244] Attorneys General (Comment 114) at 9.

[245] AOL (Comment 72) at 19.

[246] Such a statement was included in the NPR. 64 FR at 22758 n.12.

[247] AOL (Comment 72) at 19–20.

[248] IDSA (Comment 103) at 6–7.

[249] *See* Section II.A.2, *supra*.

[250] Operators must, however, allow parents to review information that was collected online but maintained offline.

[251] 64 FR at 22757–58, 22766. The Commission expects that operators will act upon requests under section 312.6(a)(2) in a timely fashion, especially with regard to chat and third party disclosures, where safety concerns are often heightened.

[252] DMA (Comment 89) at 19–20.

[253] Id.

[254] 15 U.S.C. 6502(b)(1)(B)(ii).

[255] Section 312.6(c) of the Rule retains the Act's proviso that an operator may terminate service to a child whose parent has refused to permit the operator's further use or collection of information from the child, or has directed the operator to delete the child's information. 15 U.S.C. 6502(b)(3). As noted in the NPR, the operator's right to terminate service to a child is limited by section 312.7 of the Rule, which prohibits operators from conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in the activity. 64 FR at 22758, 22766. Section 312.7 tracks the language of the statute. *See* 15 U.S.C. 6502(b)(1)(C). *See also* CME/CFA et al. (Comment 80) at 35–36 (supporting this reading of the Act).

[256] 15 U.S.C. 6502(b)(1)(B)(iii).

[257] 64 FR at 22757, 22766. *See also* 15 U.S.C. 6502(b)(1)(B) (requiring ''proper identification'' of parents).

[258] 64 FR at 22758. The other method suggested was using a photocopy of the parent's driver's license.

[259] CDT (Comment 81) at 29–30. *See also* Time Warner (Comment 78) at 13–14; DMA (Comment 89) at 17 (stringent identification requirements not necessary). One commenter stated that assuming an operator collects the same categories of information from visitors, access requirements could be met with a website form that tells parents the data categories maintained. CDT (Comment 81) at 29–30. The Commission believes that this method would be appropriate in cases where the request for information takes place online.

in the operator's notice.[260] Accordingly, the Rule has been modified to eliminate the requirement of parental identification for review of the types of information collected from children.[261] However, under § 312.6(a)(3), proper parental identification will be required for access to the specific information collected from a child.

Another commenter suggested that parents seeking review under this section should be required to provide operators with their children's identifying information (in the categories that the operator collects) in order to prove identity.[262] The operator would then disclose only the non-individually identifiable information (*e.g.,* hobbies) that the operator had collected from the child.[263] The commenter believed that this would prevent a non-parent from obtaining information from the operator that would enable him to contact the child offline.[264] However, this procedure would not, in fact, prevent access to a child's information by someone other than the parent, because many of the child's relatives and friends would be able to provide individually identifying information such as a telephone number or address. Moreover, the Act requires parental access to ''any'' personal information collected from the child.[265] The Commission therefore cannot limit the disclosures as suggested.

A number of commenters addressed the methods of verification that could be used to identify parents who seek access to their children's specific personal information. Several supported the option of using a password-protected e-mail or other secure method, which was specifically suggested in the NPR.[266] Another commenter noted that, in order to discourage requests from non-parents, requests for information could be made in writing, with confirmation sent to the home address.[267] The Commission recognizes that a number of methods might be appropriate for parental verification under this section, and allows the operator the flexibility to choose among them. Consistent with the verifiable parental consent requirements for ''disclosures'' under the Rule, acceptable methods would include print-and-send, use of a credit card in connection with a transaction, use of a toll-free number staffed by trained personnel, digital signatures, and use of an e-mail accompanied by a PIN number or a password obtained through one of the verification methods listed above.[268]

One commenter considered photocopies of a driver's license to be unnecessarily invasive, viewing a password system as preferable.[269] While the Commission agrees that submission of a driver's license may not be preferable to some parents, it should be retained as an option.

The Commission did not receive much feedback on technological advances under development that might ease the process of parental identification. Two commenters referred to digital signatures but noted they are not yet generally available.[270] The World Wide Web Consortium's Platform for Privacy Preferences Project (P3P) was also cited as a technology under development that might be used by operators and parents in the future.[271] As noted above, the Commission will continue to monitor technological advances that might play a useful role in identifying parents.[272]

5. Good Faith and Reasonable Procedures Under Section 312.6(b)

Section 312.6(b) of the proposed Rule, which tracked the language of the Act, stated that disclosures under section 312.6(a)(3) that were made in good faith and by following reasonable procedures would not give rise to liability under any Federal or State law.[273] Nonetheless, several commenters raised concerns about liability.[274] Two commenters called for specific examples of precautions that industry could take to protect itself against liability under other laws.[275] Comments also indicated that verification methods that would satisfy section 312.6(a)(3) should be listed in the Rule itself in order to provide certainty regarding the reasonableness of an operator's action under that provision.[276] One commenter asserted that parental requests for information should be in writing so the operator has a record to show good faith compliance with the Rule.[277]

The Commission recognizes the potential risks associated with the access provision and the related concerns about liability. The Commission believes, however, that the language of the Rule, which is identical to the language set forth in the Act,[278] strikes the proper balance in protecting the interests of the child, operator, and parent. An operator can assume that if it employs reasonable procedures to implement section 312.6(a)(3), including those listed above and in the NPR,[279] an inadvertent, good faith disclosure of a child's information to someone who purports to be a parent will not give rise to liability under any Federal or State laws.

Finally, one commenter stated that reasonable procedures for disclosure should account for situations where the consenting parent is unavailable as a result of death, divorce, or desertion.[280] The Commission understands that family situations can change and that circumstances may arise where it will be necessary to provide access to a party other than the consenting parent.[281] The Rule is not intended to preclude disclosures in such circumstances as long as they satisfy the ''good faith'' and ''reasonable procedures'' standards.

---

[260] *See also* 64 FR at 22758 n.13 (stating that it may be acceptable for an operator to use a less stringent method of parental identification when giving out the types of information collected from children).

[261] However, operators responding to requests under § 312.6(a)(1) may not reveal the names of any children from whom they have collected personal information. This change should also address the concerns of other commenters who felt the Commission's proposed approach to parental review was cumbersome and confusing. EPIC (Comment 115) at 5; Highlights (Comment 124) at 2–3.

[262] CDT (Comment 81) at 29–30.

[263] *Id.*

[264] *Id.*

[265] *See* 15 U.S.C. 6503(b)(1)(B).

[266] CDT (Comment 81) at 29; CME/CFA et al. (Comment 80) at 34 (supporting such a system until digital signatures become widely available); CBBB (Comment 91) at 22–24. *See* 64 FR at 22758 and n.14.

[267] MPA (Comment 113) at 4–5.

[268] As noted in note 213, *supra,* the Commission expects that operators will keep confidential any information obtained from parents in the process of obtaining consent or providing for parental review of information collected from a child.

[269] EPIC (Comment 115) at 5–6. Another commenter found requiring photocopies of drivers' licenses to be problematic since they may reveal additional personal information to the operator (such as parents' social security numbers) which parents should not be required to disclose. CME/CFA et al. (Comment 80) at 35. One commenter identified practicality and feasibility problems in connection with requiring a driver's license. CBBB (Comment 91) at 22.

[270] CME/CFA et al. (Comment 80) at 35; CBBB (Comment 91) at 16, 23–24.

[271] CBBB (Comment 91) at 23–24.

[272] *See* note 186, *supra* (discussing products and services that are available or under development).

[273] 64 FR at 22757–58, 22766. *See also* 15 U.S.C. 6502(a)(2).

[274] *See generally* DMA (Comment 89) at 15–16; Time Warner (Comment 78) at 12–13; EdPress (Comment 130) at 2.

[275] DMA (Comment 89) at 16; Time Warner (Comment 78) at 13.

[276] DMA (Comment 89) at 17; Time Warner (Comment 78) at 13.

[277] DMA (Comment 89) at 17.

[278] *See* 15 U.S.C. 6502(a)(2).

[279] 64 FR at 22757–58.

[280] CME/CFA et al. (Comment 80) at 16.

[281] It should be noted that the Rule's definition of ''parent'' in section 312.2 provides some flexibility in addressing changing family situations. *See* Section II.A.7, *supra.*

F. Section 312.7: Prohibition Against Conditioning a Child's Participation on Collection of Personal Information

Section 312.7 of the proposed Rule, which tracks the language of the Act and is retained in the final Rule, prohibited operators from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.[282] This section prohibits operators from tying the provision of personal information to such popular and persuasive incentives as prizes or games, while preserving children's access to such activities.

G. Section 312.8: Confidentiality, Security, and Integrity of Personal Information Collected From Children

Under section 312.8 of the proposed Rule, operators were required to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[283] More specifically, operators must have adequate policies and procedures for protecting children's personal information from loss, misuse, unauthorized access, or disclosure. In the NPR, the Commission offered a number of options that operators could use to implement this provision,[284] and sought comment regarding practices that are commonly used, practices that provide the strongest protection, and the costs of implementation.[285] After reviewing the comments, the Commission has decided to retain this provision, which tracks the requirements of the Act.[286]

Commenters suggested procedures for complying with this provision, including: using secure web servers and firewalls; [287] deleting personal information once it is no longer being used; [288] limiting employee access to data [289] and providing those employees with data-handling training; [290] and carefully screening the third parties to whom such information is disclosed.[291] The Commission agrees that these are appropriate measures to take under this provision.

One commenter noted that security procedures requiring special hardware, software, and/or encryption are costly.[292] The Commission is mindful of the potential costs of complying with the Rule, and thus, allows operators to choose from a number of appropriate methods of implementing this provision.

H. Section 312.9: Enforcement

This section of the proposed Rule stated that a violation of the Commission's rules implementing the COPPA would be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act, 15 U.S.C. 57a(a)(1)(B). The Commission has modified this provision to incorporate the final citation form for relevant provisions of the Act.[293]

I. Section 312.10: Safe Harbors

1. In General

This section of the Rule provides that an operator's compliance with Commission-approved self-regulatory guidelines serves as a safe harbor in any enforcement action for violations of this Rule.[294] As the Commission noted in the NPR, this section serves as an incentive for industry self-regulation; by allowing flexibility in the development of self-regulatory guidelines, it ensures that the protections afforded children under this Rule are implemented in a manner that takes into account industry-specific concerns and technological developments.[295] To receive safe harbor treatment, an operator can comply with any Commission-approved guidelines. The operator need not independently apply for approval if in fact the operator is fully complying with guidelines already approved by the Commission that are applicable to the operator's business.[296]

In an enforcement action, the Commission has the burden of proving non-compliance with the Rule's requirements. The standards enunciated in the Rule thus remain the benchmark against which industry's conduct will ultimately be judged. Compliance with approved guidelines, however, will serve as a safe harbor in any enforcement action under the Rule. That is, if an operator can show full compliance with approved guidelines, the operator will be deemed in compliance with the Rule. The Commission retains discretion to pursue enforcement under the Rule if approval of the guidelines was obtained based upon incomplete or inaccurate factual representations, or if there has been a substantial change in circumstances, such as the failure of an industry group to obtain approval for a material modification to its guidelines.[297]

2. Criteria for Approval of Self-Regulatory Guidelines

Section 312.10(b)(1) of the proposed Rule stated that, in order to be approved by the Commission, self-regulatory guidelines must require subject operators to implement the protections afforded children under the proposed Rule.[298] Two commenters were concerned that this provision was not sufficiently flexible to serve as an incentive for self-regulation. They expressed the view that the Rule should not dictate the content of self-regulatory guidelines.[299] Another commenter stated that the Commission should allow a wide range of self-regulation.[300] The Commission believes that the language of the proposed Rule conveyed less flexibility in this regard than was originally intended. The Rule therefore clarifies that promulgators of self-

---

[282] 64 FR at 22758, 22766; 15 U.S.C. 6502(b)(1)(C). One commenter supporting this provision stated that children should not be enticed to turn over personal information. CDT (Comment 81) at 30.

[283] 64 FR at 22758–59, 22766.

[284] Protections identified in the NPR included: designating an individual in the organization to be responsible for maintaining and monitoring the security of the information; requiring passwords for access to the personal information; creating firewalls; utilizing encryption; implementing access control procedures in addition to passwords; implementing devices and procedures to protect the physical security of the data processing equipment; storing the personal information collected online on a secure server that is not accessible from the Internet; installing security cameras and intrusion-detection software to monitor who is accessing the personal information; or installing authentication software to determine whether a user is authorized to enter through a firewall. 64 FR at 22758.

[285] 64 FR at 22763.

[286] *See* 15 U.S.C. 6502(b)(1)(D).

[287] Attorneys General (Comment 114) at 12; CME/CFA et al. (Comment 80) at 36.

[288] Attorneys General (Comment 114) at 12; CME/CFA et al. (Comment 80) at 36; CDT (Comment 81) at 30.

[289] Attorneys General (Comment 114) at 12; CME/CFA et al. (Comment 80) at 36.

[290] CME/CFA et al. (Comment 80) at 36.

[291] *Id.* at 17.

[292] iCanBuy.com (Comment 101) at 4.

[293] *See* 15 U.S.C. 6502(c).

[294] Seventeen commenters addressed this provision of the proposed Rule. MaMaMedia (Comment 85) at 3–4; IDSA (Comment 103) at 7; ANA (Comment 93) at 2–3; MLG Internet (Comment 119) at 2; AAAA (Comment 134) at 4; Consumers Union (Comment 116) at 6; SNAP/CollegeEdge (Comment 123) at 1; Mars (Comment 86) at 15–16; CBBB (Comment 91) at 27–37; TRUSTe (Comment 97) at 2; Bonnett (Comment 126) at 6; DMA (Comment 89) at 27–29; CME/CFA, et al. (Comment 80) at 37; McGraw-Hill (Comment 104) at 8–9; PrivacyBot.com (Comment 32) (unpaginated); Disney (Comment 82) at 10; EPIC (Comment 115) at 6–7.

[295] 64 FR at 22759.

[296] *Id.*

[297] *Id.*

[298] *Id.*

[299] DMA (Comment 89) at 27 (stating that, rather than prescribe the content of self-regulatory guidelines, the Commission should approve guidelines based upon their ''overall merits''); MLG Internet (Comment 119) at 2 (stating that the Commission should allow self-regulatory groups to create rules that meet the COPPA's goals).

[300] Mars (Comment 86) at 16.

regulatory guidelines may comply with this section by requiring subject operators to implement ''substantially similar requirements that provide the same or greater protections for children as those contained in sections 312.2–312.8 of the Rule.'' [301] Under section 312.10(c) of the Rule, the burden remains with persons seeking Commission approval of guidelines to demonstrate that the guidelines in fact meet this standard.

In a similar vein, some commenters believed that the particular assessment mechanisms and compliance incentives listed as options in sections 312.10(b)(2) and 312.10(b)(3), respectively, of the proposed Rule were, in fact, mandatory practices.[302] In the NPR, the Commission sought to clarify that these sections set out performance standards and that the listed methods were only suggested means for meeting these standards.[303] In light of the confusion evidenced by the comments, the Commission has amended these sections to make this express.[304]

Thus, section 312.10(b)(2) of the Rule makes explicit that its requirement that guidelines include an effective, mandatory mechanism for the independent assessment of subject operators' compliance is a performance standard. Similarly, section 312.10(b)(3) of the Rule states that its requirement that guidelines include effective incentives for subject operators' compliance is a performance standard. Both section 312.10(b)(2) and 312.10(b)(3) of the Rule include suggested means of meeting their respective performance standards and provide that those performance standards may be satisfied by other means if their effectiveness equals that of the listed alternatives. The Commission believes that the Rule therefore provides the flexibility sought by the commenters.

In the NPR, the Commission stated that operators could not rely solely on self-assessment mechanisms to comply with section 312.10(b)(2).[305] Commenters were divided on the issue of whether the Commission should permit self-assessment as a means of measuring operators' compliance with self-regulatory guidelines. Some believed that self-assessment, without more, is not an adequate means of measuring compliance.[306] Others believed that the Commission should not impose an independent assessment requirement on operators that choose not to join third-party compliance programs, as long as their information practices satisfy the COPPA.[307]

On balance, the Commission believes that a performance standard that incorporates independent assessment is appropriate and necessary. Under the safe harbor provision, the Commission looks to the promulgators of guidelines, in the first instance, to ensure that those guidelines are effectively implemented. The Commission believes that independent assessment is the best way to ensure that operators are complying with the guidelines.[308] The Commission notes, however, that the Rule does not prohibit the use of self-assessment as one part of an organization's efforts under section 312.10(b)(2) to measure subject operators' compliance with the Rule, nor does it preclude individual operators who have not joined third-party programs from assessing their own compliance. The Rule does, however, prohibit the use of self-assessment as the *only* means of measuring compliance with self-regulatory guidelines.

Several commenters suggested that the Commission require that self-regulatory guidelines include an array of specific practices not listed in the proposed Rule. Such practices include, for example: comprehensive information practice reviews as a condition of membership in self-regulatory programs,[309] annual compliance affidavits to be submitted by subject operators to self-regulatory organizations,[310] quarterly monitoring of operators' information practices by self-regulatory groups,[311] public reporting of disciplinary actions taken by trade groups against subject operators in publications other than trade publications,[312] and referral to the Commission of all violations of approved guidelines [313] or all failures to comply with a self-regulatory group's disciplinary dictates.[314] Many of these ideas have merit, and self-regulatory groups may wish to include some or all of them in their proposed guidelines. The Commission does not, however, believe that it should require adoption of any specific practice or practices as a prerequisite to certification under the Rule. Self-regulatory groups or other promulgators of guidelines are best suited to determine the appropriateness of such measures, in light of the Rule's requirements. The Commission will review the adequacy of the proposed enforcement programs in considering specific safe harbor requests.

3. Request for Commission Approval of Self-Regulatory Guidelines

Section 312.10(c)(1)(iii) of the proposed Rule required that persons seeking approval of guidelines submit a statement to the Commission demonstrating that their proposed guidelines, including assessment mechanisms and compliance incentives, comply with the proposed Rule.[315] One commenter suggested that the Commission eliminate this requirement.[316] The Commission believes that the burden of demonstrating compliance properly rests on proponents of Commission approval and that the guideline approval process will benefit from proponents' explanations of their rationale for approval. Therefore, the Commission has retained this requirement in the Rule.

Section 312.10 of the proposed Rule did not include a provision governing

[301] Of course, promulgators of guidelines may also require subject operators to implement the precise information practices set forth in the Rule.

[302] DMA (Comment 89) at 28; PrivacyBot.com (Comment 32) (unpaginated). One commenter expressed the view that by requiring self-regulatory groups affirmatively to monitor their members' compliance, rather than take action only in response to consumer complaints, the proposed Rule in effect deputizes industry organizations to police their members on the Commission's behalf. DMA (Comment 89) at 28. However, the Commission believes that, to the contrary, the Rule's safe harbor provisions allow industry to craft effective alternatives to Commission enforcement.

[303] 64 FR at 22759.

[304] One commenter was concerned that section 312.10(b)(2) could be read to require ''manual,'' but not ''automated'' means of independently assessing subject operators' compliance with self-regulatory guidelines. PrivacyBot.com (Comment 32) (unpaginated) and (IRFA comment 03) at 2.

[305] 64 FR at 22759.

[306] CME/CFA et al. (Comment 80) at 37; CBBB (Comment 91) at 31.

[307] McGraw-Hill (Comment 104) at 9. *See also* Mars (Comment 86) at 15 (stating that the Commission should permit self-assessment).

[308] One commenter suggested that the Commission award safe harbor status only to non-profit self-regulatory programs or for-profit groups whose self-regulatory decisions are insulated from owner or investor control. CBBB (Comment 91) at 33–34. The Commission believes it is unnecessary to so limit eligibility for safe harbor status and further believes that the test for eligibility should be the substance of self-regulatory guidelines, rather than the corporate structure of their promulgators.

[309] CBBB (Comment 91) at 29–30.

[310] *Id.* at 32.

[311] E.A. Bonnett (Comment 126) at 6.

[312] CME/CFA et al. (Comment 80) at 37.

[313] *Id.*

[314] CBBB (Comment 91) at 32.

[315] 64 FR at 22759–60. One commenter requested that the Commission clarify the status under the Freedom of Information Act of proprietary information submitted to the Commission under this section. CBBB (Comment 91) at 37. The Commission believes this is unnecessary, as such information would be protected from disclosure under section 6(f) of the Federal Trade Commission Act and Exemption 4 of the Freedom of Information Act, to the extent that it constitutes ''trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.'' FTCA Section 6(f), 15 U.S.C. 46(f); FOIA Exemption 4, 5 U.S.C. 552(b)(4).

[316] CBBB (Comment 91) at 36.

approval of changes in previously approved self-regulatory guidelines. Several commenters suggested that the Commission amend the proposed Rule to include such a provision.[317] Therefore, section 312.10(c)(3) of the Rule now provides that promulgators of approved self-regulatory guidelines must submit proposed changes and all supporting documentation for review and approval by the Commission. The Commission recognizes, however, the need for efficiency in reviewing proposed changes to approved guidelines. Only changes in approved guidelines will be subject to public notice and comment, not the unaffected portions of the guidelines.[318] Section 312.10(c)(3) of the Rule also requires that proponents of changes in approved guidelines submit a statement describing how the proposed changes comply with the Rule and how they affect existing guideline provisions.

Other comments suggested that the Commission should shorten the 180-day period for Commission action on submissions,[319] specify a time period for public comment (e.g., 30–45 days),[320] ''toll'' (rather than restart, as proposed in the NPR) the 180-day period for Commission action in the event of an incomplete submission of supporting documents,[321] and make guidelines effective upon publication of the Commission's decision, rather than 45 days from publication in the **Federal Register** as stated in the NPR.[322] After considering the comments, the Commission agrees that the guidelines should become effective upon publication of Commission approval.[323] However, it declines to adopt a single, specific time period for public comment, as the appropriate period may well vary with the complexity and novelty of the guidelines submitted. Further, the Commission does not believe the 180-day time period should be shortened or tolled during the comment period, but notes that it intends to complete its review within the statutory period.

4. Records

Section 312.10(d)(1) of the proposed Rule required that industry groups or other persons seeking safe harbor treatment maintain consumer complaints for a period not to exceed three years.[324] As one commenter noted, however, the proposed Rule did not specify the length of time required for maintaining the other documents specified in this section, *e.g.*, records of disciplinary actions against subject operators and records of independent assessments of subject operators' compliance.[325] The Commission agrees that this inconsistency is unnecessarily confusing. Therefore, the Rule now clarifies that industry groups or other persons seeking safe harbor treatment must maintain all documents required by this section for a period of three years.

J. Section 312.11: Rulemaking Review

Section 312.11 of the proposed Rule retained the Act's requirement that the Commission initiate a review proceeding to evaluate the Rule's implementation no later than five years after the effective date of the Rule and report its results to Congress.[326] The Commission stated in the NPR that the review will address the Rule's effect on: practices relating to the collection and disclosure of children's information; children's ability to access information of their choice online; and the availability of websites directed to children. In addition, eighteen months after the effective date of the Rule, the Commission will conduct a review of available mechanisms for obtaining verifiable parental consent, as discussed above in Section II.D.

K. Paperwork Reduction Act

Pursuant to the Paperwork Reduction Act (as amended 44 U.S.C. 3507(d)), the Commission submitted the proposed Rule to the Office of Management and Budget (OMB) for review.[327] The OMB has approved the Rule's information collection requirements.[328] The Commission did not receive any comments that necessitate modifying its cost estimates for the Rule's notice requirements.[329]

L. Final Regulatory Flexibility Analysis

The NPR did not include an initial regulatory flexibility analysis (IRFA) under the Regulatory Flexibility Act[330] based on a certification that the proposed Rule would not have a significant economic impact on a substantial number of small entities. Nonetheless, the Commission invited public comment on the proposed Rule's effect on small entities to ensure that no significant impact would be overlooked.[331] The Commission received two responsive comments suggesting that it publish an IRFA.[332] While the Commission believed that such an analysis was not technically required, it issued an IRFA to provide further information and opportunity for public comment on the small business impact, if any, of the Rule.[333]

This final regulatory flexibility analysis (FRFA) incorporates the Commission's initial findings, as set forth in the NPR; addresses the comments submitted in response to the IRFA notice; and describes the steps the agency has taken in the final Rule to minimize the impact on small entities consistent with the objectives of the COPPA.

Succinct Statement of the Need for, and Objectives of, the Rule

The Rule prohibits unfair or deceptive acts or practices in connection with commercial websites' and online services' collection and use of personal information from and about children by: (1) Enhancing parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) helping to protect the safety of children in online fora such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) maintaining the security of children's personal information collected online; and (4) limiting the collection and disclosures of personal information without parental consent. The Commission was

[317] ANA (Comment 93) at 3; Mars (Comment 86) at 17; and MLG Internet (Comment 119) at 2.

[318] 64 FR at 22760.

[319] CBBB (Comment 91) at 36. This commenter suggested a 90-day review period.

[320] *Id.*

[321] *Id.*; Mars (Comment 86) at 17.

[322] CBBB (Comment 91) at 36.

[323] One commenter requested that the Commission maintain a list of parties interested in being contacted by the Commission when proposed guidelines are published in the **Federal Register** and on the Commission's website. EPIC (Comment 115) at 7. The Commission believes that publication of proposed guidelines is, as a general matter, sufficient notice of their submission for approval.

[324] 64 FR at 22760.

[325] CBBB (Comment 91) at 37.

[326] 15 U.S.C. 6506. Two commenters called for conducting the review in three years rather than five. CME/CFA et al. (Comment 80) at 17; CDT (Comment 81) at 31. The Commission believes that the COPPA's five year requirement is appropriate, but will consider undertaking a review sooner if warranted.

[327] The Commission's Supporting Statement submitted to OMB as part of the clearance process has been made available on the public record of this rulemaking. *See* Supporting Statement for Information Collection Provisions at <http://www.ftc.gov/os/1999/9906/childprivsup.htm>.

[328] The assigned OMB clearance number is 3084–0117.

[329] *See* 64 FR at 22761 (estimating total burden of 18,000 hours for first year, and 1800 hours for subsequent years).

[330] 5 U.S.C. 603.

[331] *See* 64 FR at 22761.

[332] Hons. George Gekas and James Talent, U.S. House of Representatives (Comment 74) at 4; U.S. Small Business Administration (Comment 128) at 4–5.

[333] 64 FR 40525.

required by the COPPA to issue implementing regulations.[334]

Summary of the Significant Issues Raised by the Public Comments in Response to the IRFA; Summary of the Assessment of the Agency of Such Issues; and Statement of Any Changes Made in the Rule as a Result of Such Comments

In the IRFA, the Commission sought comment regarding the impact of the proposed Rule and any alternatives the Commission should consider, with a specific focus on the effect of the Rule on small entities.[335] The Commission received five comments, which discussed issues also addressed in the Statement of Basis and Purpose, above, including notice, verifiable parental consent, security, and safe harbors.

1. New Notice and Request for Consent

One commenter contended that the requirement for new notice and consent for different uses of a child's personal information under the notice and consent sections of the proposed Rule threatened smaller operators that rely on mergers and marketing alliances to help build their business.[336] The commenter recommended that new notice and consent should be required only when there is a material change in intended uses or practices.[337] As explained in Section II.C.4 and II.D.1, above, the Commission has modified its position to require new notice and consent only if there is a material change in the collection, use, or disclosure of personal information from children.

2. Verifiable Parental Consent

Another commenter expressed concern that the proposed Rule's consent requirement would result in high compliance costs and a substantial reduction in traffic to small sites.[338] According to the commenter, a child's use of collaborative educational tools on the Internet should be treated differently from the collection and use of personal contact information by marketers. The commenter, who called for parental notification and opt-out for such collaborative uses, was especially concerned about the loss of business from schools.

The Commission does not have discretion under the statute to waive the requirement of verifiable parental consent.[339] As noted above in Section II.D.4, the Rule does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parent's agent in the process. Thus, the Rule should not hinder businesses that provide services to schools.

The Commission is sensitive to commenters' concerns about increased costs and reduced traffic to sites. Accordingly, the Commission has temporarily adopted a sliding scale approach to verifiable parental consent to minimize burdens and costs for operators while still providing for parental control of children's personal information. As more fully described in Section II.D, inexpensive e-mail mechanisms may be used to obtain parental consent for the collection of information for internal uses, such as an operator's marketing to a child based on information collected about the child's preferences. Only where information is subject to ''disclosure'' under section 312.2 of the Rule will the other methods of consent be required and, even then, operators will have a range of mechanisms from which to choose. Further, even after the sliding scale is phased out two years from the Rule's effective date, operators will be able to choose from a number of consent methods, many of which are expected to be less costly and more widely available at that time.[340] Finally, for certain uses of children's personal information, no consent will be required at all under the exceptions to prior parental consent set forth in section 312.5(c) of the Rule.

3. Confidentiality, Security, and Integrity of Information

One commenter found the security methods identified in section 312.8 of the proposed Rule to be effective, but suggested that small entities should not be held to the same standards as larger entities when evaluating adequate protection under the Rule.[341] As noted earlier, the Rule allows operators flexibility in selecting security procedures in accordance with their particular needs.

4. Safe Harbors

A commenter suggested that section 312.10 of the proposed Rule should more clearly recognize the role automation can play in assessing an operator's compliance with privacy seal programs.[342] As explained above in Section II.I.2, section 312.10(b)(2) includes a performance standard requiring only that assessment mechanisms be effective, mandatory, and independent. In addition to the examples listed in the Rule, that performance standard may be satisfied by other equally effective means. Thus, the Rule does not preclude the use of automated assessment tools that meet the performance standard.

Description and Estimate of the Number of Small Entities to Which the Rule Will Apply or an Explanation of Why No Such Estimate Is Available

The Rule applies to any commercial operator of an online service or website directed to children or any commercial operator that has actual knowledge that it is collecting personal information from a child.[343] A precise estimate of the number of small entities that fall within the Rule is not currently feasible, in part, because the definition of a website directed to children turns on a number of factors that will require a factual analysis on a case-by-case basis.[344] In connection with the NPR, IRFA, and the public workshop on verifiable parental consent, the Commission has not received any comments providing an estimate of the number of small entities to which the Rule will apply.

Description of the Projected Reporting, Recordkeeping and Other Compliance Requirements of the Rule, Including an Estimate of the Classes of Small Entities That Will Be Subject to the Requirement and the Type of Professional Skills Necessary for Preparation of the Report or Record

The Commission incorporates by reference its description of the projected reporting, recordkeeping and other compliance requirements of the Rule, as

[334] 15 U.S.C. 6502.

[335] 64 FR at 40527–28.

[336] KidsOnLine.com (IRFA Comment 02) at 1.

[337] *Id.*

[338] Zeeks.com (IRFA Comment 05) at 2.

[339] *See* 15 U.S.C. 6502; section 312.3 of the Rule. Another commenter suggested that operators be permitted to collect some personal information to establish a relationship with the child in exchange for limited access to the site (such as games) without obtaining consent. KidsOnLine.com (IRFA Comment 02) at 2.

[340] *See supra* note 1868. As described more fully above, the Commission will undertake a review eighteen months after the effective date of the Rule to determine through public comment whether technology has progressed as expected. The impact on small businesses will again be carefully considered.

[341] KidsOnLine.com (IRFA Comment 02) at 1.

[342] PrivacyBot.com (IRFA Comment 03) at 2. This commenter noted that the examples listed the NPR appeared to call for manual assessment mechanisms.

[343] Section 312.3. The Rule does not apply to nonprofit entities. Section 312.2 (definition of ''operator'').

[344] Under section 312.2, in determining whether a commercial website or online service is directed to children, the Commission will consider its subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children.

set forth in the IRFA.[345] The Office of Management and Budget has approved the information collection of the Rule[346] based on the Commission's earlier submission for clearance, which has been made available on the public record of this rulemaking.[347] The Commission has not received any comments that necessitate modifying its previous description of projected compliance requirements.

Description of the Steps the Agency Has Taken To Minimize the Significant Economic Impact on Small Entities, Consistent With the Stated Objectives of Applicable Statutes, Including a Statement of the Factual, Policy, and Legal Reasons for Selecting the Alternative Adopted in the Final Rule and Why Each of the Other Significant Alternatives to the Rule Considered by the Agency Which Affect the Impact on Small Entities Was Rejected

The Rule incorporates the many performance standards set forth in the statute.[348] Thus, operators are free to choose among a number of compliance methods based upon their individual business models and needs. Although the Rule's provisions impose some costs, the requirements of notice, verifiable parental consent, access, and security are mandated by the COPPA itself. The Commission has sought to minimize the burden on all businesses, including small entities, by adopting flexible standards;[349] however, it does not have the discretion to create exemptions from the Act based on an operator's size. Likewise, while the Rule attempts to clarify, consolidate, and simplify the statutory requirements for all entities,[350] the Commission has little discretion, if any, to mandate different methods or schedules for small entities that would undermine compliance with the Act.[351]

Nevertheless, throughout the rulemaking proceeding, the Commission has sought to gather information regarding the economic impact of the COPPA's requirements on all operators, including small entities. The NPR, for example, included a number of questions for public comment regarding the costs and benefits associated with notice and consent.[352] Similarly, the subsequent IRFA notice invited public comment specifically on the issue of small business impact.[353] In addition, the agenda for the public workshop on verifiable parental consent included topics designed to elicit economic impact information. In connection with the workshop, the Commission invited additional public comment.

The Commission has carefully considered responsive comments that suggested a variety of alternatives in developing the final Rule. The discussion below reviews some of the significant alternatives considered and the basis for the Commission's decisions with regard to certain notice, parental consent, access, security, and safe harbor requirements.

1. New Notice and Request for Consent

Many commenters contended that requiring operators to undertake new notice and consent under sections 312.4(c) and 312.5 for any use not covered by a parent's previous consent was burdensome and unnecessary.[354] The Commission is sensitive to the objections raised, particularly with respect to mergers, which occur often in this industry and which would trigger new notice and consent requirements even where there was no significant change in the operator's information practices. Eliminating this requirement altogether, however, would prevent parents from receiving material information that could affect their decisions regarding their child's online activities.[355]

In response to comments, including those of small businesses,[356] the Commission has modified the Rule to require new notice and consent only if there will be a material change in how the operator collects, uses, or discloses personal information from children.[357] This modification should substantially reduce the costs of compliance.

2. Verifiable Parental Consent

Throughout the rulemaking, the Commission has sought input on what mechanisms may be used to satisfy the COPPA's verifiable parental consent requirement. As described more fully in Section II.D. above, the Commission has temporarily adopted a ''sliding scale'' approach that depends upon the use of the child's personal information. This approach was recommended by many industry members seeking to preserve flexibility for operators while achieving the objectives of the Act.[358] To minimize burdens until more reliable electronic methods become more available and affordable, it allows use of e-mail for internal uses of personal information, as long as additional steps are taken to verify a parent's identity.

Some commenters had contended that use of e-mail alone should be an acceptable method of consent under section 312.5 of the Rule.[359] Commenters also criticized methods such as print-and-send, credit card, toll-free numbers, and digital signatures for the costs and burdens they might impose.[360] Based on the comments and workshop discussion, the Commission does not believe that use of e-mail alone adequately satisfies the statutory requirement that operators make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology.[361] According to many commenters, e-mail is easily subject to circumvention by children.[362] In particular, where a child and parent share the same e-mail account, as is often the case, a child may easily pretend to be a parent and provide consent for himself.[363]

The Commission does not expect that declining to permit use of e-mail alone will impose significant costs in terms of foregone activities. Websites will be able to engage in many activities that do not trigger any prior consent requirements pursuant to the exceptions to parental consent set forth in section 312.5(c).[364] According to a workshop participant, these exceptions cover some of the most popular and common online activities,

---

[345] *See* 64 FR at 40526–27.

[346] The OMB clearance number is 3084–0117.

[347] *See* Supporting Statement for Information Collection Provisions at <http://www.ftc.gov/os/1999/9906/childprivsup.htm>.

[348] *See, e.g.*, sections 312.4(c), 312.5.

[349] *See* 5 U.S.C. 603(c)(3). The notice requirements, for example, have been designed to minimize the burdens on operators in a variety of ways. Section 312.4(b) of the Rule permits operators to post ''links'' to the required notices, rather than state the complete text. Similarly, in response to industry concerns about technical feasibility, the Commission has eliminated the requirement that the link must be seen without having to scroll down from the initial viewing screen. *See* Section II.C.2, *supra*.

[350] *See* 5 U.S.C. 603(c)(2).

[351] For example, the COPPA requires the online posting of privacy policies by websites and online services. A waiver for small entities of that prior notice requirement (*e.g.*, by permitting notice after the fact) would be inconsistent with the statutory mandate. *See* 15 U.S.C. 6502(b)(1)(A)(i).

[352] 64 FR at 22761–63.

[353] 64 FR 40525.

[354] *See supra* note 143.

[355] For example, an operator might initially use a child's information only for internal marketing purposes and then later undertake a new use involving disclosures to third parties. Such a change would likely be important to the parent's consent decision.

[356] *See* KidsOnLine.com (IRFA Comment 02) at 1.

[357] *See also* Section II.C.3.a, *supra* (discussing section 312.4(b)(2)(i) (content of notice)).

[358] *See supra* note 203 and accompanying text.

[359] *See supra* note 197 and accompanying text.

[360] *See supra* notes 187–195 and accompanying text.

[361] *See* 15 U.S.C. 6501(9).

[362] *See supra* note 196 and accompanying text.

[363] *See supra* note 178 and accompanying text.

[364] *See* Section II.D.3, *supra.* Prior parental consent is not required pursuant to these exceptions. However, in some instances, operators must provide parents with notice and an opportunity to opt out. *See* section 312.5(c)(3).

including newsletters, contests, and online magazine subscriptions.[365]

Moreover, where e-mail mechanisms are employed for internal uses under the sliding scale, the additional steps required under section 312.5 (such as sending a confirmatory e-mail to the parent following receipt of consent) should not be especially onerous given the availability and ease of automated technology.[366] Thus, the additional steps required should have no deterrent effect on operators (or parents).

Only for activities that entail ''disclosure'' of a child's personal information, as defined in the Rule, such as chat rooms, message boards, pen-pal services, and personal home pages, will the higher method of consent be triggered.[367] The comments and public workshop discussion provide considerable support for the principle that such activities warrant a higher level of protection, given the heightened safety concerns.[368] In order to ensure maximum flexibility within this upper tier of the sliding scale, a range of mechanisms will be acceptable under the Rule, including postal mail, facsimile, credit card in connection with a transaction, toll-free numbers, and digital signatures.[369] To minimize costs, once a parent has provided consent through one of these methods and obtained a PIN or password, an operator may subsequently obtain consent through an e-mail accompanied by such PIN or password.

In adopting the sliding scale for a two-year period following the Rule's effective date, the Commission has sought to minimize any burdens of compliance until advancements in technology provide more reliable electronic methods at low cost. Based on reports from industry members, the Commission expects that this will occur soon.[370] To assess whether such developments have in fact occurred as expected, the Commission will undertake a review, using notice and comment, approximately eighteen months after the Rule's effective date. All businesses, including small entities, will be given the opportunity to comment on economic impact issues at that time.

If technology progresses as expected, operators should have a wide variety of reasonable and effective options for providing verifiable parental consent. Therefore, phasing out the sliding scale should not impose undue burdens on operators seeking to comply with the Rule. Moreover, the Commission's amendment to the Rule requiring new notice and consent only in the case of Amaterial changes' to an operator's information practices should further reduce operators' burdens.

3. Parental Access to Information

In implementing the COPPA's parental access requirement,[371] the Commission has adopted flexible standards and sought to eliminate any unnecessary provisions in the Rule. For example, section 312.6(a)(3) requires that operators provide a means of review that ensures that the requestor is a parent, taking into account available technology, and that is not unduly burdensome to the parent. In response to comments that the proposed Rule's right to change information went beyond the statute and was onerous, the Commission has omitted that provision from the Rule. To eliminate unnecessary costs, the Rule also no longer requires parental verification for access to the types or categories of personal information collected from the child under section 312.6(a)(1). However, consistent with the COPPA, which recognized the safety concerns inherent in granting access to the child's specific information, proper parental verification will be required for access to that information under section 312.6(a)(3). As with verifiable parental consent, operators may choose from among a variety of verification methods, including both online and offline methods.[372]

4. Confidentiality, Security, and Integrity of Information

As required under the Act, the Rule seeks to ensure a baseline level of protection for children's personal information.[373] The Commission recognizes that certain security procedures may be more costly for smaller entities than larger entities.[374] Accordingly, section 312.8 allows operators flexibility in selecting reasonable procedures in accordance with their business models.[375]

5. Safe Harbors

The safe harbor provisions also utilize performance standards in order to minimize burdens and provide incentives for industry self-regulation, as required by the COPPA.[376] In response to concerns that the proposed Rule appeared inflexible, the Commission has clarified in section 312.10(b)(1) that promulgators of self-regulatory guidelines may comply with the safe harbor provisions by requiring subject operators to implement ''substantially similar requirements that provide the same or greater protections for children'' as those contained in the Rule. The Commission also has adopted performance standards for the assessment mechanisms and compliance incentives in sections 312.10(b)(2) and (b)(3). In addition to the examples listed in the Rule, these performance standards may be satisfied by other equally effective means. In order to maximize efficiency, the Rule further provides that only material changes in approved guidelines will be subject to the public notice and comment required under this section.

Final Rule

List of Subjects in 16 CFR Part 312

Children, Children's online privacy protection, Communications, Computer technology, Consumer protection, Data protection, Electronic mail, E-mail, Information practices, Internet, Online service, Privacy, Record retention, Safety, Trade practices, Website, Youth.

Accordingly, the Federal Trade Commission amends 16 CFR chapter I by adding a new Part 312 to read as follows:

PART 312—CHILDREN'S ONLINE PRIVACY PROTECTION RULE

Sec.

[365] *See supra* note 226.

[366] A number of commenters recognized that taking additional steps would increase the likelihood that it is the parent who is providing consent, and some websites already undertake such measures. *See supra* notes 198–203 and accompanying text.

[367] To minimize burdens on general audience sites, the Commission has revised the Rule so that if a chat room monitor strips any posting of individually identifiable information before it is made public, the operator will not be deemed to have ''collected'' the child's personal information for purposes of the Rule. *See* Section II.A.2, *supra* (discussing section 312.2's definition of ''collects or collection''). Moreover, because the individually identifiable information has been deleted, the operator will not have ''disclosed'' that information under the Rule.

[368] *See supra* note 205 and accompanying text.

[369] *See* section 312.5(b).

[370] *See* Section II.D.2 and note 186, *supra.*

[371] *See* 15 U.S.C. 6502(b)(1)(B)(iii).

[372] The Commission will continue to monitor technological advances that might play a useful role in identifying parents for purposes of granting access. The Commission agrees with comments that it is currently premature to mandate the use of certain mechanisms still under development or not yet widely available. *See* CBBB (Comment 91) at 24.

[373] *See* 15 U.S.C. 6502(b)(1)(D).

[374] *See* KidsOnLine.com (IRFA Comment 02) at 1.

[375] *See* note 284, supra.

[376] *See* 15 U.S.C. 6503.

Authority: Secs. 15 U.S.C. 6501 *et seq.*

§ 312.1 Scope of regulations in this part.

This part implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, *et seq.*,) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. The effective date of this part is April 21, 2000.

§ 312.2 Definitions.

Child means an individual under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(a) Requesting that children submit personal information online;

(b) Enabling children to make personal information publicly available through a chat room, message board, or other means, *except where* the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records; or

(c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclosure means, with respect to personal information:

(a) The release of personal information collected from a child in identifiable form by an operator for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online service and who does not disclose or use that information for any other purpose. For purposes of this definition:

(1) *Release of personal information* means the sharing, selling, renting, or any other means of providing personal information to any third party, and

(2) *Support for the internal operations of the website or online service* means those activities necessary to maintain the technical functioning of the website or online service, or to fulfill a request of a child as permitted by § 312.5(c)(2) and (3); or

(b) Making personal information collected from a child by an operator publicly available in identifiable form, by any means, including by a public posting through the Internet, or through a personal home page posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Online contact information means an e-mail address or any other substantially similar identifier that permits direct contact with a person online.

Operator means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce:

(a) Among the several States or with 1 or more foreign nations;

(b) In any territory of the United States or in the District of Columbia, or between any such territory and

(1) Another such territory, or

(2) Any State or foreign nation; or

(c) Between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(a) A first and last name;

(b) A home or other physical address including street name and name of a city or town;

(c) An e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address;

(d) A telephone number;

(e) A Social Security number;

(f) A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or

(g) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Third party means any person who is not:

(a) An operator with respect to the collection or maintenance of personal information on the website or online service; or

(b) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Obtaining *verifiable consent* means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(a) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(b) Authorizes any collection, use, and/or disclosure of the personal information.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children. *Provided, however,* that a commercial website or online service, or a portion thereof, shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In determining whether a commercial website or online service, or a portion thereof, is targeted to children, the Commission will consider its subject matter, visual or audio content, age of models, language or other characteristics of the website or

online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition; evidence regarding the intended audience; and whether a site uses animated characters and/or child-oriented activities and incentives.

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

General requirements. It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6);

(d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§ 312.7); and

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).

§ 312.4 Notice.

(a) *General principles of notice.* All notices under §§ 312.3(a) and 312.5 must be clearly and understandably written, be complete, and must contain no unrelated, confusing, or contradictory materials.

(b) *Notice on the website or online service.* Under § 312.3(a), an operator of a website or online service directed to children must post a link to a notice of its information practices with regard to children on the home page of its website or online service and at each area on the website or online service where personal information is collected from children. An operator of a general audience website or online service that has a separate children's area or site must post a link to a notice of its information practices with regard to children on the home page of the children's area.

(1) *Placement of the notice.* (i) The link to the notice must be clearly labeled as a notice of the website or online service's information practices with regard to children;

(ii) The link to the notice must be placed in a clear and prominent place and manner on the home page of the website or online service; and

(iii) The link to the notice must be placed in a clear and prominent place and manner at each area on the website or online service where children directly provide, or are asked to provide, personal information, and in close proximity to the requests for information in each such area.

(2) *Content of the notice.* To be complete, the notice of the website or online service's information practices must state the following:

(i) The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service. *Provided that:* the operators of a website or online service may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

(ii) The types of personal information collected from children and whether the personal information is collected directly or passively;

(iii) How such personal information is or may be used by the operator(s), including but not limited to fulfillment of a requested transaction, recordkeeping, marketing back to the child, or making it publicly available through a chat room or by other means;

(iv) Whether personal information is disclosed to third parties, and if so, the types of business in which such third parties are engaged, and the general purposes for which such information is used; whether those third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the operator; and that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties;

(v) That the operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity; and

(vi) That the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

(c) *Notice to a parent.* Under § 312.5, an operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives notice of the operator's practices with regard to the collection, use, and/or disclosure of the child's personal information, including notice of any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(1) *Content of the notice to the parent.* (i) All notices must state the following:

(A) That the operator wishes to collect personal information from the child;

(B) The information set forth in paragraph (b) of this section.

(ii) In the case of a notice to obtain verifiable parental consent under § 312.5(a), the notice must also state that the parent's consent is required for the collection, use, and/or disclosure of such information, and state the means by which the parent can provide verifiable consent to the collection of information.

(iii) In the case of a notice under the exception in § 312.5(c)(3), the notice must also state the following:

(A) That the operator has collected the child's e-mail address or other online contact information to respond to the child's request for information and that the requested information will require more than one contact with the child;

(B) That the parent may refuse to permit further contact with the child and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice.

(iv) In the case of a notice under the exception in § 312.5(c)(4), the notice must also state the following:

(A) That the operator has collected the child's name and e-mail address or other online contact information to protect the safety of the child participating on the website or online service;

(B) That the parent may refuse to permit the use of the information and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose stated in the notice.

§ 312.5 Parental consent.

(a) *General requirements.* (1) An operator is required to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

(b) *Mechanisms for verifiable parental consent.* (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

(2) Methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the verification methods listed in this paragraph. *Provided that:* For the period until April 21, 2002, methods to obtain verifiable parental consent for uses of information other than the ''disclosures'' defined by § 312.2 may also include use of e-mail coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory e-mail to the parent following receipt of consent; or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. Operators who use such methods must provide notice that the parent can revoke any consent given in response to the earlier e-mail.

(c) *Exceptions to prior parental consent.* Verifiable parental consent is required prior to any collection, use and/or disclosure of personal information from a child except as set forth in this paragraph. The exceptions to prior parental consent are as follows:

(1) Where the operator collects the name or online contact information of a parent or child to be used for the sole purpose of obtaining parental consent or providing notice under § 312.4. If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) Where the operator collects online contact information from a child for the sole purpose of responding directly on a one-time basis to a specific request from the child, and where such information is not used to recontact the child and is deleted by the operator from its records;

(3) Where the operator collects online contact information from a child to be used to respond directly more than once to a specific request from the child, and where such information is not used for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that a parent receives notice and has the opportunity to request that the operator make no further use of the information, as described in § 312.4(c), immediately after the initial response and before making any additional response to the child. Mechanisms to provide such notice include, but are not limited to, sending the notice by postal mail or sending the notice to the parent's e-mail address, but do not include asking a child to print a notice form or sending an e-mail to the child;

(4) Where the operator collects a child's name and online contact information to the extent reasonably necessary to protect the safety of a child participant on the website or online service, and the operator usesd reasonable efforts to provide a parent notice as described in § 312.4(c), where such information is:

(i) Used for the sole purpose of protecting the child's safety;

(ii) Not used to recontact the child or for any other purpose;

(iii) Not disclosed on the website or online service; and

(5) Where the operator collects a child's name and online contact information and such information is not used for any other purpose, to the extent reasonably necessary:

(i) To protect the security or integrity of its website or online service;

(ii) To take precautions against liability;

(iii) To respond to judicial process; or

(iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

§ 312.9 Enforcement.

Subject to sections 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Safe harbors.

(a) *In general.* An operator will be deemed to be in compliance with the requirements of this part if that operator complies with self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, that, after notice and comment, are approved by the Commission.

(b) *Criteria for approval of self-regulatory guidelines.* To be approved by the Commission, guidelines must include the following:

(1) A requirement that operators subject to the guidelines (''subject operators'') implement substantially similar requirements that provide the same or greater protections for children as those contained in §§ 312.2 through 312.9;

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the guidelines. This performance standard may be satisfied by:

(i) Periodic reviews of subject operators' information practices conducted on a random basis either by the industry group promulgating the guidelines or by an independent entity;

(ii) Periodic reviews of all subject operators' information practices, conducted either by the industry group promulgating the guidelines or by an independent entity;

(iii) Seeding of subject operators' databases, if accompanied by either paragraphs (b)(2)(i) or (b)(2)(ii) of this section; or

(iv) Any other equally effective independent assessment mechanism; and

(3) Effective incentives for subject operators' compliance with the guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of disciplinary action taken against subject operators by the industry group promulgating the guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the guidelines; or

(v) Any other equally effective incentive.

(4) The assessment mechanism required under paragraph (b)(2) of this section can be provided by an independent enforcement program, such as a seal program. In considering whether to initiate an investigation or to bring an enforcement action for violations of this part, and in considering appropriate remedies for such violations, the Commission will take into account whether an operator has been subject to self-regulatory guidelines approved under this section and whether the operator has taken remedial action pursuant to such guidelines, including but not limited to actions set forth in paragraphs (b)(3)(i) through (iii) of this section.

(c) *Request for Commission approval of self-regulatory guidelines.*

(1) To obtain Commission approval of self-regulatory guidelines, industry groups or other persons must file a request for such approval. A request shall be accompanied by the following:

(i) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(ii) A comparison of each provision of §§ 312.3 through 312.8 with the corresponding provisions of the guidelines; and

(iii) A statement explaining:

(A) How the guidelines, including the applicable assessment mechanism, meet the requirements of this part; and

(B) How the assessment mechanism and compliance incentives required under paragraphs (b)(2) and (3) of this section provide effective enforcement of the requirements of this part.

(2) The Commission shall act upon a request under this section within 180 days of the filing of such request and shall set forth its conclusions in writing.

(3) Industry groups or other persons whose guidelines have been approved by the Commission must submit proposed changes in those guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(1). The statement required under paragraph (c)(1)(iii) must describe how the proposed changes affect existing provisions of the guidelines.

(d) *Records.* Industry groups or other persons who seek safe harbor treatment by compliance with guidelines that have been approved under this part shall maintain for a period not less than three years and upon request make available to the Commission for inspection and copying:

(1) Consumer complaints alleging violations of the guidelines by subject operators;

(2) Records of disciplinary actions taken against subject operators; and

(3) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2) of this section.

(e) *Revocation of approval.* The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory guidelines and their implementation do not, in fact, meet the requirements of this part.

§ 312.11 Rulemaking review.

No later than April 21, 2005, the Commission shall initiate a rulemaking review proceeding to evaluate the implementation of this part, including the effect of the implementation of this part on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and report to Congress on the results of this review.

§ 312.12 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 99–27740 Filed 11–2–99; 8:45 am]

BILLING CODE 6750–01–P

How to Comply With The Children's Online Privacy Protection Rule

November 1999 Kidz Privacy website

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. The new rules spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.

The Federal Trade Commission staff prepared this guide to help you comply with the new requirements for protecting children's privacy online and understand the FTC's enforcement authority.

Who Must Comply

If you operate a commercial Web site or an online service directed to children under 13 that collects personal information from children **or** if you operate a general audience Web site and have *actual knowledge* that you are collecting personal information from children, you must comply with the Children's Online Privacy Protection Act.

- To determine whether a Web site is directed to children, the FTC considers several factors, including the subject matter; visual or audio content; the age of models on the site; language; whether advertising on the Web site is directed to children; information regarding the age of the actual or intended audience; and whether a site uses animated characters or other child-oriented features.
- To determine whether an entity is an "operator" with respect to information collected at a site, the FTC will consider who owns and controls the

information; who pays for the collection and maintenance of the information; what the pre-existing contractual relationships are in connection with the information; and what role the Web site plays in collecting or maintaining the information.

Personal Information

The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information -- for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms -- when they are tied to individually identifiable information.

Basic Provisions

Privacy Notice

Placement

An operator must post a link to a notice of its information practices on the home page of its Web site or online service *and* at each area where it collects personal information from children. An operator of a general audience site with a separate children's area must post a link to its notice on the home page of the children's area.

The link to the privacy notice must be clear and prominent. Operators may want to use a larger font size or a different color type on a contrasting background to make it stand out. A link in small print at the bottom of the page -- or a link that is indistinguishable from other links on your site -- is not considered clear and prominent.

Content

The notice must be clearly written and understandable; it should not include any unrelated or confusing materials. It must state the following information:

- The name and contact information (address, telephone number and email

address) of all operators collecting or maintaining children's personal information through the Web site or online service. If more than one operator is collecting information at the site, the site may select and provide contact information for only one operator who will respond to all inquiries from parents about the site's privacy policies. Still, the names of *all* the operators must be listed in the notice.

- The kinds of personal information collected from children (for example, name, address, email address, hobbies, etc.) and how the information is collected -- directly from the child or passively, say, through cookies.
- How the operator uses the personal information. For example, is it for marketing back to the child? Notifying contest winners? Allowing the child to make the information publicly available through a chat room?
- Whether the operator discloses information collected from children to third parties. If so, the operator also must disclose the kinds of businesses in which the third parties are engaged; the general purposes for which the information is used; and whether the third parties have agreed to maintain the confidentiality and security of the information.
- That the parent has the option to agree to the collection and use of the child's information without consenting to the disclosure of the information to third parties.
- That the operator may not require a child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation.
- That the parent can review the child's personal information, ask to have it deleted and refuse to allow any further collection or use of the child's information. The notice also must state the procedures for the parent to follow.

Direct Notice to Parents

Content

The notice to parents must contain the same information included on the notice

on the Web site. In addition, an operator must notify a parent that it wishes to collect personal information from the child; that the parent's consent is required for the collection, use and disclosure of the information; and how the parent can provide consent. The notice to parents must be written clearly and understandably, and must not contain any unrelated or confusing information. An operator may use any one of a number of methods to notify a parent, including sending an email message to the parent or a notice by postal mail.

Verifiable Parental Consent

Before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent. This means an operator must make reasonable efforts (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator's information practices and consents to those practices.

Until April 2002, the FTC will use a *sliding scale* approach to parental consent in which the required method of consent will vary based on how the operator uses the child's personal information. That is, if the operator uses the information for *internal* purposes, a less rigorous method of consent is required. If the operator *discloses the information to others*, the situation presents greater dangers to children, and a more reliable method of consent is required. The sliding scale approach will sunset in April 2002 subject to a Commission review planned for October 2001.

Internal Uses

Operators may use *email* to get parental consent for all internal uses of personal information, such as marketing back to a child based on his or her preferences or communicating promotional updates about site content, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, operators might seek confirmation from a parent in a delayed confirmatory email, or confirm the parent's consent by letter or phone call.

Public Disclosures

When operators want to disclose a child's personal information to third parties or make it publicly available (for example, through a chat room or message board), the *sliding scale* requires them to use a more reliable method of consent, including:

- getting a signed form from the parent via postal mail or facsimile;
- accepting and verifying a credit card number in connection with a transaction;
- taking calls from parents, through a toll-free telephone number staffed by trained personnel;
- email accompanied by digital signature;

But in the case of a monitored chat room, if all individually identifiable information is stripped from postings before it is made public -- and the information is deleted from the operator's records -- an operator does not have to get prior parental consent.

Disclosures to Third Parties

An operator must give a parent the option to agree to the collection and use of the child's personal information without agreeing to the disclosure of the information to third parties. However, when a parent agrees to the collection and use of their child's personal information, the operator may release that information to others who uses it solely to provide support for the internal operations of the website or service, including technical support and order fulfillment.

Exceptions

The regulations include several exceptions that allow operators to collect a child's email address without getting the parent's consent in advance. These exceptions cover many popular online activities for kids, including *contests*, *online newsletters*, *homework help* and *electronic postcards*.

Prior parental consent is not required when:

- an operator collects a child's or parent's email address to provide notice

and seek consent;

- an operator collects an email address to respond to a *one-time* request from a child and then deletes it;
- an operator collects an email address to respond *more than once to a specific* request -- say, for a subscription to a newsletter. In this case, the operator must notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to a child;
- an operator collects a child's name or online contact information to protect the safety of a child who is participating on the site. In this case, the operator must notify the parent and give him or her the opportunity to prevent further use of the information;
- an operator collects a child's name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, and does not use it for any other purpose.

October 2001/April 2002

In October 2001, the Commission will seek public comment to determine whether technology has progressed and whether secure electronic methods for obtaining verifiable parental consent are widely available and affordable. Subject to the Commission's review, the sliding scale will expire in April 2002. Until then, operators are encouraged to use the more reliable methods of consent for all uses of children's personal information.

New Notice for Consent

An operator is required to send a *new notice and request for consent to parents* if there are material changes in the collection, use or disclosure practices to which the parent had previously agreed. Take the case of the operator who got parental consent for a child to participate in contests that require the child to submit limited personal information, but who now wants to offer the child chat rooms. Or, consider the case of the operator who wants to disclose the child's information to third parties who are in materially different lines of business from those covered

by the original consent -- for example, marketers of diet pills rather than marketers of stuffed animals. In these cases, the Rule requires new notice and consent.

Access Verification

At a parent's request, operators must disclose the general kinds of personal information they collect online from children (for example, name, address, telephone number, email address, hobbies), as well as the specific information collected from children who visit their sites. Operators must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information.

They can use a variety of methods to verify the parent's identity, including:

- obtaining a signed form from the parent via postal mail or facsimile;
- accepting and verifying a credit card number;
- taking calls from parents on a toll-free telephone number staffed by trained personnel;
- email accompanied by digital signature;
- email accompanied by a PIN or password obtained through one of the verification methods above.

Operators who follow one of these procedures acting in good faith to a request for parental access are protected from liability under federal and state law for inadvertent disclosures of a child's information to someone who purports to be a parent.

Revoking & Deleting

At any time, a parent may revoke his/her consent, refuse to allow an operator to further use or collect their child's personal information, and direct the operator to delete the information. In turn, the operator may terminate any service provided to the child, but only if the information at issue is reasonably necessary for the child's participation in that activity. For example, an operator may require children to provide their email addresses to participate in a chat room so the operator can

contact a youngster if he is misbehaving in the chat room. If, after giving consent, a parent asks the operator to delete the child's information, the operator may refuse to allow the child to participate in the chat room in the future. If other activities on the Web site do not require the child's email address, the operator must allow the child access to those activities.

Timing

The Rule covers all personal information collected after April 21, 2000, regardless of any prior relationship an operator has had with a child. For example, if an operator collects the name and email address of a child before April 21, 2000, but plans to seek information about the child's street address after that date, the later collection would trigger the Rule's requirements. In addition, come April 21, 2000, if an operator continues to offer activities that involve the ongoing collection of information from children -- like a chat room -- or begins to offer such activities for the first time, notice and consent are required for all participating children regardless of whether the children had already registered at the site.

Safe Harbors

Industry groups or others can create self-regulatory programs to govern participants' compliance with the Children's Online Privacy Protection Rule [PDF]. These guidelines must include independent monitoring and disciplinary procedures and must be submitted to the Commission for approval. The Commission will publish the guidelines and seek public comment in considering whether to approve the guidelines. An operator's compliance with Commission-approved self-regulatory guidelines will generally serve as a Asafe harbor" in any enforcement action for violations of the Rule.

Enforcement

The Commission may bring enforcement actions and impose civil penalties for violations of the Rule in the same manner as for other Rules under the FTC Act. The Commission also retains authority under Section 5 of the FTC Act to examine information practices for deception and unfairness, including those in use before the Rule's effective date. In interpreting Section 5 of the FTC Act, the

Commission has determined that a representation, omission or practice is *deceptive* if it is likely to:

- mislead consumers; and
- affect consumers' behavior or decisions about the product or service.

Specifically, it is a deceptive practice under Section 5 to represent that a Web site is collecting personal identifying information from a child for one reason (say, to earn points to redeem a premium) when the information will be used for another reason that a parent would find material -- and when the Web site does not disclose the other reason clearly or prominently.
In addition, an act or practice is *unfair* if the injury it causes, or is likely to cause, is:

- substantial;
- not outweighed by other benefits; and
- not reasonably avoidable.

For example, it is likely to be an unfair practice in violation of Section 5 to collect personal identifying information from a child, such as email address, home address or phone number, and disclose that information to a third party without giving parents adequate notice and a chance to control the collection and use of the information.

For More Information

If you have questions about the Children's Online Privacy Protection Rule [PDF], visit the FTC online at www.ftc.gov/kidzprivacy. You also may call the FTC's Consumer Response Center toll-free at 1-877-FTC-HELP (382-4357), or write Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Your Opportunity to Comment

The Small Business and Agriculture Regulatory Enforcement Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about

federal enforcement actions. Each year, the Ombudsman evaluates enforcement activities and rates each agency's responsiveness to small business. To comment on FTC actions, call 1-888-734-3247.

Frequently Asked Questions about the Children's Online Privacy Protection Rule

Volume 1

The following FAQs are intended to supplement the compliance materials available on the FTC's website. To view the Rule and the compliance materials, go to *www.ftc.gov/kidzprivacy*.

INDEX OF HEADINGS

GENERAL QUESTIONS

1. What is the Children's Online Privacy Protection Rule?

The Children's Online Privacy Protection Act (COPPA) was passed by Congress in October 1998, with a requirement that the Federal Trade Commission (FTC) issue and enforce rules concerning children's online privacy. The primary goal of the Act and the Rule is to place parents in control over what information is collected from their children online. The Rule was designed to be strong, yet flexible, to protect children while recognizing the dynamic nature of the Internet.

- The COPPA Rule applies to operators of commercial websites and online services directed to children under 13 that collect personal information from children, and operators of general audience sites with actual knowledge that they are collecting information from children under 13.
- Those operators must:

(1) post clear and comprehensive Privacy Policies on the website describing their information practices for children's personal information;

(2) provide notice to parents, and with limited exceptions, obtain verifiable parental consent **before** collecting personal information from children;

(3) give parents the choice to consent to the operator's collection and use of a child's information while prohibiting the operator from disclosing that information to third parties;

(4) provide parents access to their child's personal information to review and/or have it deleted;

(5) give parents the opportunity to prevent further collection or use of the information

(6) maintain the confidentiality, security, and integrity of information they collect from children.

- In addition, the Rule prohibits operators from conditioning a child's participation in an online activity on the child's providing more information than is reasonably necessary to participate in that activity.

2. Where can I find information about COPPA?

The FTC has a comprehensive website, *www.ftc.gov*, which has information concerning all the activities of the agency. In the upper left section of the home page is a link that says "Privacy Initiatives." If you click on that banner, you will have access to a variety of documents regarding the Children's Rule, including the proposed and final Rules, the public comments received by the Commission in the course of the rulemaking, guides for businesses and parents, safe harbor applications we've received and any public comments on those applications, notice of any cases brought under the Rule, and announcements of future activities. Materials concerning general privacy and financial privacy (including the Gramm-Leach-Bliley rulemaking) are available there as well.

In addition, the FTC has set up a special web page designed for kids, parents, businesses, and educators at *www.ftc.gov/kidzprivacy*. In addition to providing the Rule and compliance materials for businesses and parents, this web page features online safety tips for children and other useful education resources about the Rule and online privacy in general.

All educational materials on our website are also available free by calling the FTC's Consumer Response Center's toll free number at (877) FTC-HELP.

3. What do I do if I have questions about the COPPA Rule?

The first thing you should do is read the educational materials available on our website *www.ftc.gov* and through our toll free telephone number (877) FTC-HELP. If you still have questions, you can email us at kidsprivacy@ftc.gov or contact our Consumer Response Center at toll free (877) FTC-HELP. The FTC also has an online form to file complaints or request information at the website.

4. When did COPPA and its implementing Rule go into effect?

The Act and the Rule went into effect on April 21, 2000.

5. COPPA applies to "websites directed to children." What determines whether or not a website is targeted to children?

The Rule sets out a number of factors in determining whether a website is targeted to children, such as its subject matter, language, whether it uses animated characters, and whether advertising appearing on the site is directed to children. The Commission will also consider empirical evidence regarding the ages of the site's visitors. These standards are very similar to those previously established for TV, radio, and print advertising.

6. Does COPPA apply to information about children collected from parents or other adults?

No. COPPA and the Rule only apply to personal information collected from children, not their parents or other adults. The Rule's Statement of Basis and Purpose, however, notes that the Commission expects that operators will keep confidential any information obtained from parents in the course of obtaining parental consent or providing for parental access pursuant to COPPA. *See* Rule n. 213.

7. Why does COPPA apply only to children under 13? What about protecting the online privacy of teens?

Young children may not understand the safety and privacy issues created by the online collection of personal information, and are therefore particularly vulnerable. Children under 13 has often been the standard for distinguishing adolescents from young children who may need special protections. As a general matter, however, the FTC encourages operators to afford teens privacy protections, given the risks inherent in the disclosure of personal information for all ages. The FTC has recommended that Congress pass legislation to ensure the fair information principles be implemented for all consumers. In the interim, websites' information practices are still subject to Section 5 of the FTC Act, which prohibits deceptive or unfair trade practices. *See* July 15, 1997 Staff Opinion Letter to Center for Media Education for guidance on how Section 5 applies to information practices involving children and teens.

8. Does the Rule apply to information collected prior to the its effective date?

No, but if a site collects new information after the effective date of the Rule, even for existing registrants, they must comply. For example, if an operator collected a child's email address prior to April 21 and now wishes to collect the child's postal address to send a premium or prize, the operator must comply with COPPA prior to collecting the mailing address.

Similarly, if a child registered at a website prior to April 21, 2000 for an online newsletter and the website invites the child to sign up for a new chat room, the fact that the child was already registered with the site does not obviate the need for the operator to comply with COPPA for purposes of enabling the child to register for the chat room.

9. Are there any protections that apply to information collected before COPPA went into effect?

Yes. Although the Rule covers only information collected after its effective date, previously collected information is still subject to the protections afforded by Section 5 of the FTC Act. Thus, if an operator engaged in deceptive or unfair practices when collecting, using or disclosing information from kids, the operator could face FTC action. *See* Staff Opinion Letter to Center for Media Education issued July 15, 1997, outlining

what would be deceptive and/or unfair practices with regard to the collection and use of children's information.

10. I know the Rule is triggered by the collection of personal information from children, but the information I collect at my site is voluntary and not mandatory. Does the Rule still apply?

Yes. Whether your information collection is voluntary or mandatory, it still constitutes collection and triggers the Rule.

11. Hasn't the Children's Online Privacy Protection Act been declared unconstitutional?

No. The *Children's Online Privacy Protection Act* (COPPA), has not been challenged and went into effect on April 21, 2000. Enforcement of the *Children's Online Protection Act* (COPA), which sought to regulate the dissemination of material harmful to minors on the Internet, was preliminarily enjoined by the U.S. District Court for the Eastern District of Pennsylvania, *ACLU v. Reno*, 31 F.Supp.2d 473 (E.D. Pa.1999). That decision was affirmed by the Third Circuit, 217 F.3d 162 (3d Cir. 2000). For information on COPA and the work of the Commission on Child Online Protection, which is studying methods and technologies to help reduce access by minors to such materials visit *www.copacommission.org*.

12. Will the COPPA Rule keep my child from accessing pornography?

No, not directly. COPPA is meant to give parents control over the *collection of their children's personal information* and does not limit children's access to information publicly available on the Internet. COPPA may help keep your child off email lists. Information about COPA, which does address dissemination of pornography to minors, is available at *www.copacommission.org*. If you are concerned about your children accessing pornography or other inappropriate materials on the Internet, you may want to look for a *filtering program* or an Internet Service Provider that offers such tools. Information about such tools is available at *www.getnetwise.org* and *www.safekids.com*.

COPPA ENFORCEMENT

13. How will the FTC enforce the Rule?

The FTC will monitor the Internet for compliance with the Rule and bring law enforcement actions where appropriate to deter violations. Parents and others can

submit complaints to the FTC through our website *www.ftc.gov* and our toll-free number (877) FTC-HELP. We will also investigate referrals from consumer groups, industry, and approved safe harbor programs, as appropriate.

14. What are the penalties for violating the Rule?

Website operators who violate the Rule could be liable for civil penalties of up to $11,000 *per violation*. The level of penalties assessed may turn on a number of factors including egregiousness of the violation, *e.g.*, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties and the size of the company.

15. Do the states or other government agencies have jurisdiction over this issue?

Yes. COPPA also gives states and certain federal agencies authority to enforce compliance with the Act with respect to entities in their jurisdiction. For example, the Office of the Comptroller of the Currency will handle compliance by national banks and the Department of Transportation will handle air carriers.

16. Have any cases ever been brought for deceptive collection of online information from children?

Yes. Even prior to COPPA, the FTC brought enforcement actions in this area under Section 5 of the FTC Act. In the agency's first Internet privacy case, Geocities agreed to settle charges of deceptively collecting personal information from children and adults. *Geocities*, FTC Dkt. No. C-3849 (Feb. 12, 1999). The Liberty Financial case involved the "Young Investors" website which deceptively promised to maintain only anonymous information from children and teens. *Liberty Financial Companies, Inc.*, FTC Dkt. No. C-3891 (Aug. 12, 1999). In Toysmart, the FTC alleges that the defendants collected personal information from children without obtaining prior parental consent in violation of COPPA, 16 C.F.R. § 312.5(c)(2). *FTC. v. Toysmart.com LLC and Toysmart.com, Inc.*, No. 00-11341-RGS, (D. Mass. filed July 10, 2000, amended July 21, 2000). Commission cases are available on its website via the Privacy Initiatives link from the home page or via its search engine.

17. What do I do if my site isn't in compliance with the Rule?

If you are not collecting any personal information from children, then you are not subject to the Rule. So the quickest thing to do until you can get your site into compliance is to stop collecting personal information from children under 13. In fact, many sites that we have talked to have realized that collection of such information is not necessary.
Then, review your website, your privacy policy, and the Rule carefully. The materials on the Commission's website can provide you with helpful guidance. Take a close look at: what information you collect; how you collect it; how you use it; whether the information you seek to collect is necessary for the activities on your site; whether you have adequate mechanisms for providing parents with notice and obtaining consent; and whether you have adequate methods for parents to review their children's information and for verifying that the people requesting access to kids' information really are their parents.

18. Are websites run by nonprofit entities subject to the Rule?

The Act and the Rule expressly state that they apply to *commercial* websites and not to nonprofits that would otherwise be exempt from coverage under Section 5 of the FTC Act. Thus, in general, most non-profits are not subject to the Rule. However, nonprofits that operate for the profit of their for-profit members may be subject to the Rule. *See FTC v. California Dental Association* 526 U.S. 756 (1999), for additional guidance on when nonprofits are subject to FTC jurisdiction. Although true nonprofits are not subject to COPPA, we encourage them to set an example by posting privacy policies and providing the protections set forth in COPPA to children providing personal information at their sites.

19. Does COPPA apply to websites operated by the Federal Government?

It is federal policy that all Federal websites and contractors when operating on behalf of agencies comply with the standards set forth in COPPA. *See* *www.whitehouse.gov/OMB/memoranda/m00-13.html*

20. The Internet is truly a global medium. Do websites set up and run abroad have to comply with the Rule?

Yes. Foreign-run websites must comply with COPPA if they are directed to children in the U.S. or knowingly collect information from children in the U.S. For example, foreign-

run kid-oriented websites would be subject to COPPA if they advertised in offline media in the U.S. or on popular U.S. websites. The Rule's definition of an "operator" - who is subject to the Act - includes foreign websites that are involved in commerce in the United States or its territories.

PRIVACY POLICIES AND NOTICE TO THE PARENT

21. My site does not collect any personally identifiable information. Do I still need to post a privacy policy?

No. COPPA only applies to those websites that collect personal information from children. However, the FTC recommends that *all* websites post privacy policies, so visitors have an easily recognizable place to go to find out about the operator's information practices. Surveys show that most parents are uncomfortable with their children giving out any personal information on the Internet, so as a practical matter, parents will be pleased to read your privacy policy and find out quickly that you do not collect personally identifiable information.

22. What information must I include in my privacy policy and in the direct notice to parents?

The Rule identifies the information that must be disclosed in the privacy policy and in the direct notice - the notice sent directly to the parent. *See* §312.4(b) for information regarding the content of the privacy policy and §312.4(c) for information regarding the content of the direct notice to the parent. Remember, that in addition to including the content required in the privacy policy, the direct notice to parents needs to tell the parent that you wish to collect personal information from the child, that consent is required for you to do so, and how the parent may provide consent. The Rule also requires that the privacy policy be posted clearly and prominently on the home page and that a hyperlink to the policy be provided at each area where personal information is collected.

23. Do I have to disclose my use of cookies, GUIDS, IP addresses, or the use of other passive information collection technology?

Yes, when such information is combined with "personal information." The Rule defines personal information to include individually identifiable information about an individual

collected online, including any persistent identifier that is tied to identifying information. Where such passive forms of information collection are tied to identifying information, including a persistent identifier that can be used to identify, contact, or locate an individual, then it is considered personal information under the Rule.

24. Can I include in my privacy policy materials promoting products, services, and/or websites of mine and my partners?

No. The Rule requires that privacy policies must be "clearly and understandably written, be complete, and contain no unrelated, confusing, or contradictory materials." *See* §312.4(a). The more complicated and confusing a policy is, the more likely it will be that parents won't understand or even read the policy. And remember, parents who find your policy confusing or difficult to comprehend may be less likely to grant you consent.

25. I run a general audience site, but I offer a specific children's section. Is it acceptable for me to structure my privacy policy so that information about my children's practices and non-children's practices are mixed in together, or do I have to have a separate privacy policy about my practices with respect to children?

In the commentary of the Final Rule, the Commission noted that "[o]perators are free to combine the privacy policies into one document, as long as the link for the children's policy takes visitors directly to the point in the document where the operator's policies with respect to children are discussed, or it is clearly disclosed at the top of the statement that there is a specific section discussing the operator's information practices with respect to children." 64 Fed. Reg. 59894 at n.98. In addition, the link for the privacy policy pertaining to the children's area must appear on the home page of the children's area and at each area where personal information is collected from children. Sites may also wish to post it as part of their general privacy policy.

26. Is it okay for the link to my privacy policy to be at the very bottom of my home page?

As long as the link is "clear and prominent" it is okay to have it at the bottom of the home page. The Rule requires that the link to your privacy policy "be placed in a clear and prominent place and manner on the home page of the website or online service" and at each area where children provide, or are asked to provide, personal information. *See* §§312.4(b)(1)(ii) and (iii). In its explanation of this requirement, the Commission

noted that "'[c]lear and prominent' means that the link must stand out and be noticeable to the site's visitors through use, for example, of a larger font size in a different color on a contrasting background. The Commission does not consider 'clear and prominent' a link that is in small print at the bottom of the page, or a link that is indistinguishable from a number of other, adjacent links." 64 Fed. Reg. 59894.

27. When I send the notice to parents, can I simply email them a link to the privacy policy?

Yes. You may send your direct notice to parents via email, and you may include in that email a link to your privacy policy. Remember that the direct notice to the parent also needs to tell the parents that you wish to collect personal information from the child, that the parent's consent is required for you to do so, and how the parent may provide consent.

It is also important to remember that the notices must not contain unrelated, confusing, or contradictory information. For example, your notice to parents may not include so much additional information that the message about needing consent or the link to the privacy policy is obscured.

28. Do I have to list the names, addresses, phone numbers, etc. of all of the operators at my site? This will make my privacy policy very long and confusing.

Under the Rule, if there are multiple operators collecting information through your site, you may list the name, address, phone number, and email address of *one* operator who will respond to all inquiries from parents regarding all of the operators' privacy policies and uses of children's information, as long as the *names* of all the operators are also listed in the notice. *See* §312.4(b)(2)(i).

If you wish to list the contact information of all the operators but still keep your privacy policy and notice simple, you can include a link in the privacy policy or notice to the list of operators. Just make sure that when you send the notice to parents to request consent, they can access that list.

VERIFIABLE PARENTAL CONSENT

29. When do I have to get verifiable parental consent?

The general rule is that an operator must obtain verifiable parental consent before collecting personal information from a child unless the collection fits into one of the exceptions for the collection of online contact information. As described below, the method for obtaining such consent will vary with the use of the information.

30. Can I first collect information from children and then get consent from parents as long as I don't use the information until I get consent?

In most cases, no. COPPA clearly states that operators must get verifiable parental consent *before* collecting personal information from children under 13. There are several exceptions to this requirement which allow an operator:

(1) to collect a child's name and parent's email address for purposes of providing the required *notice and obtaining consent*;

(2) to collect a child's email address to respond *once* to a specific request from a child, as long as the email address is deleted immediately after responding;

(3) to collect a child's email address to respond *more than once* to a specific request of a child (for example, requesting a subscription to an online newsletter or requesting site updates), as long as, after the first communication with the child, the operator sends notice to the parent's email address to provide an opportunity for the parent to *opt-out* of the information collection and order the operator to delete the email address and stop contacting the child. With this *multiple-contact exception*, the parent needs only to contact the operator to discontinue the communication; affirmative consent is not required so that a non-response will be presumed to be parental consent. Of course, at any time the parent may contact the operator and request that the information be deleted and the contact halted. *See* §§312.3(c) and 312.6(a)(2).)

(4) to collect a child's name and email address where necessary to protect the *safety of a child* participating on the site or online service. The operator must give notice to the parent, use it only for such safety purpose, and not disclose it on the site or service.

(5) to collect a child's name and email address for the sole purpose of protecting the security or integrity of the site, take precautions against liability, respond to judicial process or for law enforcement on a matter related to public safety.

All of these exceptions are described in §312.5(c) of the Rule.

31. I collect personal information from children on my website but I only use it for internal purposes and never give it to third parties. Do I still need to get parental consent before collecting that information?

Yes, unless the information collection fits within one of the Rule's limited exceptions. If you are only using the information internally, and do not make it publicly available through such activities as chat rooms or bulletin boards, then you can get parental consent through the Rule's "email plus" methods until April 2002 *See* §312.5(b)(2) and below.

32. How do I get parental consent?

You can use one or more of a number of methods of obtaining parental consent. Until April 2002, the methods you may use will depend on how you use the information you collect.

If you are going to use the information only for internal purposes, that is, you will not be giving the information to third parties or making it publicly available through such activities as chat rooms or bulletin boards, then you can use what is being called the "email plus" method of obtaining consent. You may send an email to the parent containing the required notice, and request that the parent provide consent by responding in an email - as long as you take some additional, confirmatory step after receiving the parent's email. For example, after a reasonable time delay, you can send another email to the parent to confirm consent and let the parent know that he or she can revoke the consent if they wish. You may also request in your initial email that the parent include a phone number or mailing address in his or her reply so that you can follow up to confirm via telephone or postal mail.

If you are going to disclose children's information to third parties or make it publicly available through such activities as a chat room, message board, personal home page, pen pal service, or email service, then you must use the most reliable methods available

to obtain parental consent. You can: provide a form for the parent to sign and mail or fax back to you; ask a parent to use a credit card in connection with a transaction (perhaps a fee just to cover the cost of processing the credit card); maintain a toll-free telephone number staffed by trained personnel for parents to call in their consent, or you can accept emails from parents where those emails contain a digital signature or other digital certificate that uses public key technology.

33. Am I required to obtain prior parental consent if I collect the personal information through software that is downloaded from my website or from a CD-ROM that I sell at retail outlets?

If personal information is collected by or through any website or online service, such collection would be covered by COPPA regardless of how the collection was initiated. For example, if children to your site are invited to download software that tracks their online activities and the information sent back to the website is personal information as defined under the Rule, then such collection would require prior parental consent. It is important to note, however, that where the information collection does not take place on the Internet, it is not subject to COPPA, but such collection would still be subject to Section 5 of the FTC Act, which prohibits deceptive or unfair trade practices.

34. I would like to get consent by collecting a credit card number from the parent, but I don't want to charge a fee. Is this ok?

Not unless the card issuer is willing to verify the card number without a transaction. The verifiability of the credit card transaction comes from the card issuer's verification that the number is from a real credit card. Most credit card companies have told us that they do not approve of using credit card numbers without a transaction, and some say they won't verify numbers in the absence of a transaction. Website operators should check with the credit card companies first; if they are willing to work with you to verify a credit card without completing a transaction, then you may use this method of obtaining consent.

35. What do I do if some parents cannot or will not use the consent method I've chosen? For example, some parents can't use email consent because they don't have

an email account. Other parents do not have credit cards or do not like to give out credit card numbers on the Internet.

We recommend that operators have a *readily available backup method* of providing consent for those parents who cannot or will not use your primary consent mechanism. One practical backup method to use is the print-and-send form. This method makes it easy for parents without access to email or a credit card to provide consent.

36. Should I give out passwords or PIN numbers to parents to confirm their identity in any future contact with them?

Yes. This is a good way to confirm a parent's identity for future contacts. Remember that if, after obtaining consent from a parent, you change your information practices in a material way, you will have to send a new notice to the parent and obtain consent all over again. If you have given the parent a password in your initial consent process, then getting new consent will be much easier.

In addition, COPPA requires you to give parents access to any information you have collected from their children. Before you give out that information, you will need to confirm that the person requesting the information really is the child's parent. Again, giving the parent a password during the initial consent process makes it easier to confirm the identity of that parent if access is later requested.

37. I know that I must allow parents to consent to my collection and use of their children's information, while giving them the option of prohibiting me from disclosing that information to third parties. Does that mean that if I have chat rooms or bulletin boards, I have to offer "choice" about those as well?

No. If chat or bulletin boards are bundled together with other online activities, you don't have to offer parents choice regarding the collection of personal information necessary for chat or the bulletin board; but prior parental consent is still required before permitting children to participate in chat rooms or bulletin boards that enable a child to make their personal information publicly available. The Rule only requires parental choice as to *disclosures to third parties.* There are many parents, however, who do not want their children participating in unmonitored chat rooms or bulletin boards because they can raise safety concerns. Those parents may not give consent for their child to provide

personal information for participation in other site activities if the activities are bundled together with chat and bulletin boards. Therefore, while not required, sites may wish to offer parents a broader range of choices in order to address their concerns.

GENERAL AUDIENCE AND TEEN SITES

38. I operate a general audience site and don't ask visitors to reveal their ages. However, I do have a number of chat rooms.

(a) What happens if a child visits my site and posts personal information in a chat room but doesn't reveal his age?

The Rule is not triggered. It applies to general audience websites if they have *actual knowledge* that a particular visitor is a child. If such a site knows that a particular visitor is a child, then the Rule must be followed with respect to that child. If a child posts personal information on a general audience site, but doesn't reveal his or her age and you have no other information that would lead you to know that the visitor is a child, then you would not have "actual knowledge" under the Rule and would not be subject to its requirements. Collecting a child's age, however, does provide "actual knowledge."

(b) What happens if a child visits my chat room and announces his or her age?

If your site has a chat room and no one in your organization sees or is alerted to the post, then you do not have the requisite actual knowledge under the Rule. You may be considered to have actual knowledge with respect to that child: (1) if someone from your operations sees the post in a chat room; or (2) if someone alerts you to the post. At that point, you should delete any personal information that has been posted and either ask the child for a parent's email address for purposes of providing notice and obtaining consent to future postings, or take reasonable steps to block that child from returning to the chat area of the site, whether through screen name blocking, a cookie, or some other means.

If you have monitored chat rooms where the monitors can delete information from posts *before* they are made public, then your monitors can simply strip the child's posts of any personal information before they are publicly posted, thus permitting children to participate in the chat room without the need for obtaining parental consent. This

practice is easily applied to "auditorium" style chat in which children pose questions which are screened to a moderator or guest celebrity.

39. I have a website that targets teens. How does COPPA affect my practices?

Although your site targets teens, you may still attract a substantial number of children protected by COPPA. The Commission has urged all sites to provide fair information practices for all consumers, so personal information collected from even your older children should be given such protections. At a minimum, however, you should identify which visitors are under 13 -- for example, simply ask age (or birth year) when you invite visitors to provide personal information or to create their log-in user ID. Most importantly, ask age in such a way as not to invite falsification. You can also use a session cookie to prevent children from back clicking to change their age once they realize that parental consent is required to collect their information for the activity.

Once you identify those under 13, you have a number of options. First, you can collect their parent's email address to provide direct notice and implement the COPPA parental consent requirements; or, if you are only collecting an email address, it may fall within one of the email exceptions to prior parental consent. (Note that several of the email exceptions do require that you provide notice to the parent and an opportunity to opt-out.) Alternatively, if you do not wish to implement the COPPA protections for your younger visitors, then your data system could be configured to automatically delete the personal information of those visitors under 13, and simply direct those children to content that does not involve information collection.

It is very important to design your information collection in such a way that children are not encouraged to provide a false age. For example, if the log-in registration only permits the visitor to enter birth years starting with age 13, children may be encouraged to falsify their ages. In addition, telling visitors that children under 13 should not provide their information or that they must ask their parents first, may only encourage children to provide their information. If your site does not invite falsification, however, then it will not be responsible if a child misstates his or her age.

40. Can I block children under 13 from my site?

Blocking all children under 13 from accessing your site is not in the spirit of COPPA and probably not good business in the long run. Many sites have found creative ways both to provide rich content for children and comply with COPPA: (1) offering activities that do not require personal information; (2) using screen names to personalize activities on the site; (3) using the email exceptions to prior parental consent (see below) ; and (4) limiting the collection of personal information to only those activities that require it, *e.g.*, collecting the parent's and child's email address to ensure safety of the child participating in a chat room.

41. I operate a general audience site and don't ask visitors to reveal their ages. I do have a button that users can click to send feedback, comments, or questions by email. What are my responsibilities if I get an email that says, "Hi, I am Steve, age 10, and I really like your site. When do you think you will add some more games?"

Under the Rule's one-time contact exception, you can reply to the child (once) without sending notice to the parent or obtaining prior parental consent as long as you do not re-contact the child and you delete the personal information from your records.

EXCEPTIONS TO PRIOR PARENTAL CONSENT

42. I want to have a contest on my site. Can I use the one-time contact exception to prior parental consent?

Yes, as long as you only collect children's email addresses to enter them in the contest and only contact them to notify them of the winner(s). However, if you will be contacting the child more than once, then you will have to use the multiple-contact "notice and opt out" exception. In either case, you must delete those email addresses as soon as the contest ends. In addition, the Rule prohibits operators from using the email addresses for any other purpose and requires them to ensure the security of this information, which is particularly important if the contest runs for any length of time.

If you wish to collect any information from children online beyond an email address in connection with contest entries - for example a home address to mail a prize - you must provide parental notice and obtain prior parental consent (opt-in) as you would for any other type of personal information collection. You may ask the child to provide the parent's email address to notify the parent if the child wins. In the prize notification

email, you can ask the parent to provide the home mailing address to ship the prize, or invite the parent to call a telephone number to provide the mailing information. Remember, the exception to prior parental consent only applies to collection of an email address, and in the case of providing notice or to ensure the safety of a child participating at the site in an activity such as chat, you can also collect the child's name. All other personal information collection will require prior parental consent.

43. I have a site that has an "Ask the Author" corner where kids can send questions via email to featured authors. Do I need to provide notice and obtain parental consent?

No. This feature will likely fall under the one-time contact exception. If your site simply sends children's email to the author and doesn't maintain or store them in any form, then you fall into the one-time contact exception and do not need to obtain parental consent.

44. I want to offer electronic post cards. Can I take advantage of one of the email exceptions?

Yes, if you design your system to either delete the email address immediately after the e-card is sent (a one time exception) or, if you retain the email address for a period of time, you must give parents notice and opportunity to opt-out. *See* Rule n.222.

PARENTAL ACCESS

45. Do I have to keep all information I've collected from children in case a parent may want to see it in the future?

No. As we noted in the discussion on the Final Rule, "if a parent seeks to review his child's personal information after the operator has deleted it, the operator may simply reply that it no longer has any information concerning that child." 64 Fed. Reg. 59904.

46. What if, despite all my most careful efforts, I mistakenly give out a child's personal information to someone who isn't that child's parent or guardian?

Under the Rule, if you act in good faith and follow reasonable procedures to verify the identity of someone seeking access to a child's information, then you will not be liable under any Federal or State law if you mistakenly give out a child's information. *See* §312.6(b).

Acceptable verification methods for access include obtaining parental consent by mail, a toll- free number staffed by trained personnel, a credit card in conjunction with a transaction, digital signatures, and use of an email accompanied by a PIN number or password obtained through one of the verification methods listed above.

46. If a parent revokes his or her consent, can an operator maintain the child's email address so that it can prevent the child from contacting or registering at the site in the future?

Yes, where a parent requests that their child be blocked from providing personal information in the future, the site can obtain the parent's express authorization to retain an email address for such purpose. Otherwise, the Rule does not permit the operator to maintain email addresses collected from children for a "Do Not Contact List." Rather, the site is free to begin the notice and consent process anew if the child returns to the site and registers for an activity.

REQUIREMENT TO LIMIT INFORMATION COLLECTION

47. I know that I can't condition a child's participation in a game or the offering of a prize on the child giving out more information than is reasonably necessary to participate in those activities, but does that limitation apply to other activities?

Yes. The relevant rule provision is: "An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, *or another activity* on the child's disclosing more information than is reasonably necessary to participate in such activity." *See* §312.7. Therefore, you must be careful to examine the information you collect in connection with *each activity* you offer on your site to ensure that you are only collecting information that is reasonably necessary to participate in that activity.

48. If I operate a chat room and a parent revokes their consent to my maintaining the child and parent's email addresses, can I block that child from my chat room?

Yes. If a parent revokes their consent and directs you to delete the personal information you had collected that was necessary for the activity, you may terminate that service. *See* §312.6(c). If your site has activities for which such information collection is not required, however, then you should allow the child to continue to participate in those activities.

SAFE HARBORS

49. How can organizations with self-regulatory guidelines qualify for safe harbor treatment?

The organization must submit its guidelines to the FTC for approval. The Commission will publish submitted guidelines for public comment and then make a determination whether the guidelines meet the criteria set forth in the Rule. The key criteria are that the guidelines (1) provide "substantially similar requirements that provide the same or greater protections" as those in the Rule, and (2) include effective mechanisms for independent assessment of operators' compliance with the guidelines and for enforcement of the guidelines.

50. What should I do if I am interested in submitting my self-regulatory program to the FTC for approval under the safe harbor provisions?

Information about applying for FTC certification of a safe harbor program is provided in §312.10 of the Rule and at our website at *www.ftc.gov/privacy/safeharbor/shp.htm*. In addition, you may call (202) 326-3090, and you will be connected to someone who can help you with your questions.

51. How can I learn about what safe harbor programs have been approved under the Rule?

Applications for safe harbor status are posted on the FTC website, along with the comments on the application. The Commission has 180 days to issue a decision on an application. The applications and comments are available at *www.ftc.gov/privacy/safeharbor/shp.htm*. The Commission's decisions on these submissions will be announced in the Federal Register and on the FTC website.

SCHOOLS AND LIBRARIES

52. Will the Rule limit children's use of the Internet in schools and libraries?

No, the Rule does not limit children's access to information or ability to surf. Rather, it sets forth protections with respect to the personal information collected from children by commercial operators.

53. What role can schools play?

The Rule notes that COPPA does not preclude schools from acting as intermediaries in the notice and consent process, or from serving as agents of parents. Where a school has an agency relationship with an operator that explicitly authorizes information collection, the Rule allows the operator to presume parental consent. Schools can also help to educate students and parents about online privacy issues and safe surfing practices. The FTC is currently working with the Department of Education to develop educational materials on COPPA for teachers and school administrators.

How to Protect Kids' Privacy Online

February 2000 Kidz Privacy website

Whether playing, shopping, studying or just surfing, today's kids are taking advantage of all that the web has to offer. But when it comes to their personal information online, who's in charge? In an effort to put parents in the catbird seat, the Federal Trade Commission has established new rules for website operators to make sure that kids' privacy is protected while they're online. These rules are part of the 1998 Children's Online Privacy Protection Act. Here's a look at what the law requires, starting April 21, 2000.

Website Operators Must:	Parents Should:
Post their privacy policy. Websites directed to children or that knowingly collect information from kids under 13 must post a notice of their information collection practices that includes: • types of personal information they collect from kids- for example, name, home address, email address or hobbies. • how the site will use the information - for example, to market to the child who supplied the information, to notify contest winners or to make the information available through a child's participation in a chat room. • whether personal information is forwarded to advertisers or other third parties. • a contact at the site.	**Look for a privacy policy on any website directed to children.** The policy must be available through a link on the website's homepage and at each area where personal information is collected from kids. Websites for general audiences that have a children's section must post the notice on the homepages of the section for kids. Read the policy closely to learn the kinds of personal information being collected, how it will be used, and whether it will be passed on to third parties. If you find a website that doesn't post basic protections for children's personal information, ask for details about their information collection practices.

Get parental consent. In many cases, a site must obtain parental consent before collecting, using or disclosing personal information about a child. Consent is not required when a site is collecting an email address to: • respond to a one-time request from the child. • provide notice to the parent. • ensure the safety of the child or the site. • send a newsletter or other information on a regular basis as long as the site notifies a parent and gives them a chance to say no to the arrangement.	**Decide whether to give consent.** Giving consent authorizes the website to collect personal information from your child. *You can give consent and still say no to having your child's information passed along to a third party.* Your consent isn't necessary if the website is collecting your child's email address simply to respond to a one-time request for information.
Get new consent when information-practices change in a "material" way. Website operators need to notify parents and get consent again if they plan to change the kinds of information they collect, change how they use the information or offer the information to new and different third parties. For example, new parental consent would be required if the website decides to: • send information from children to marketers of diet pills instead of only marketers of stuffed animals, as covered in the original consent. • give a child access to a chat room if the parent's original consent covered only sending a newsletter.	**Decide whether to approve information collection from your kids based on new uses for the information.** Website operators will let you know about the need for new consent by sending you a new notice and request. They will do this when they are changing the terms-of-use of the information in a "material" or significant way.
Allow parents to review personal information collected from their children. To do this, website operators must verify the identity of the requesting parent.	**Ask to see the information your child has submitted.** The site will ask you to verify your identity to ensure that your child's information isn't given out improperly.

Allow parents to revoke their consent, and delete information collected from their children at the parents' request. Parents can revoke their consent and ask that information about their children be deleted from the site's database. When a parent revokes consent, the website must stop collecting, using or disclosing information from that child. The site may end a child's participation in an activity if the information it collected was necessary for participation in the website's activity.	**Understand that you may revoke your consent at any time and have your child's information deleted.** To stop a website from collecting additional information from your child, you can revoke your consent. You also may ask a site to delete any personal information it has already collected from your child.

If you want more information about privacy online or if you suspect a violation of the Children's Online Privacy Protection Rule, contact the FTC's Consumer Response Center or visit the Kidz Privacy website.

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint, or to get free information on any of 150 consumer topics, call toll-free, **1-877-FTC-HELP** (1-877-382-4357), or use the online complaint form. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies worldwide.

FEDERAL TRADE COMMISSION	**FOR THE CONSUMER**
1-877-FTC-HELP	**www.ftc.gov**