[**Billing Code: 6750-01S**]

FEDERAL TRADE COMMISSION

16 CFR Part 312

RIN: 3084-AB20

CHILDREN'S ONLINE PRIVACY PROTECTION RULE

AGENCY: Federal Trade Commission ("FTC" or "Commission").

ACTION: Proposed rule; request for comment.

SUMMARY: The Commission proposes to amend the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"), consistent with the requirements of the Children's Online Privacy Protection Act to respond to changes in online technology, including in the mobile marketplace, and, where appropriate, to streamline the Rule. After extensive consideration of public input, the Commission proposes to modify certain of the Rule's definitions, and to update the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbor provisions. In addition, the Commission proposes adding a new provision addressing data retention and deletion.

DATES: Written comments must be received on or before November 28, 2011.

ADDRESSES: Interested parties may file a comment online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write "COPPA Rule Review, 16 CFR Part 312, Project No. P104503" on your comment, and file your comment online at **https://ftcpublic.commentworks.com/ftc/2011copparulereview**, by following the instructions on the web-based form. If you prefer to file your comment on paper, write "COPPA Rule Review, 16 CFR Part 312, Project No. P104503 on your comment, and mail or deliver your comment to the following address: Federal

Trade Commission, Office of the Secretary, Room H-113 (Annex E), 600 Pennsylvania Avenue, NW, Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Phyllis H. Marcus or Mamie Kresses, Attorneys, Division of Advertising Practices, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, (202) 326-2854, or (202) 326-2070.

SUPPLEMENTARY INFORMATION:

I. Background

The COPPA Rule, 16 CFR Part 312, issued pursuant to the Children's Online Privacy Protection Act ("COPPA" or "COPPA statute"), 15 U.S.C. 6501 *et seq.*, became effective on April 21, 2000. The Rule imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age (collectively, "operators"). Among other things, the Rule requires that operators provide notice to parents and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under 13 years of age.[1] The Rule also requires operators to keep secure the information they collect from children and prohibits them from conditioning children's participation in activities on the collection of more personal

[1] *See* Children's Online Privacy Protection Rule, 16 CFR 312.3.

information than is reasonably necessary to participate in such activities.[2] The Rule contains a "safe harbor" provision enabling industry groups or others to submit to the Commission for approval self-regulatory guidelines that would implement the Rule's protections.[3]

The Commission initiated a review of the Rule on April 21, 2005, pursuant to Section 6507 of the COPPA statute, which required the Commission to conduct a review within five years of the Rule's effective date.[4] After considering extensive public comment, the Commission determined in March 2006 to retain the Rule without change.[5]

The Commission remains deeply committed to helping to create a safer, more secure online experience for children and takes seriously the challenge to ensure that COPPA continues to meet its originally stated goals, even as online technologies, and children's uses of such technologies, evolve. In light of the rapid-fire pace of technological change since the Commission's 2005 review, including an explosion in children's use of mobile devices, the proliferation of online social networking and interactive gaming, the Commission initiated review of the COPPA Rule in April 2010 on an accelerated schedule.[6]

---

[2] *See* 16 CFR 312.7 and 312.8.

[3] *See* 16 CFR 312.10; Children's Online Privacy Protection Rule, 64 FR 59888, 59906, 59908, 59915 (Nov. 3, 1999), *available at* **http://www.ftc.gov/os/1999/10/64Fr59888.pdf**.

[4] *See* 15 U.S.C. 6507; 16 CFR 312.11.

[5] *See* Children's Online Privacy Protection Rule, 71 FR 13247 (Mar. 15, 2006) (retention of rule without modification).

[6] The Commission generally reviews each of its trade regulation rules approximately every ten years. Under this schedule, the next COPPA Rule review was

(continued...)

On April 5, 2010, the Commission published a document in the FEDERAL REGISTER seeking public comment on whether technological changes to the online environment over the preceding five years warranted any changes to the Rule.[7] The Commission's request for public comment examined each aspect of the COPPA Rule, posing 28 questions for the public's consideration.[8] The Commission identified several areas where public comment would be especially useful, including examination of whether: the Rule's existing definitions are sufficiently clear and comprehensive, or warrant modification or expansion, consistent with the COPPA statute; additional technological methods to obtain verifiable parental consent should be added to the COPPA Rule, and whether any of the consent methods currently included should be removed; whether the Rule provisions on protecting the confidentiality and security of personal information are sufficiently clear and comprehensive; and the Rule's criteria and process for Commission approval and oversight of safe harbor programs should be modified in any way. The comment period closed on July 12, 2010. During the comment period, on June 2, 2010, the Commission held a public roundtable to discuss in detail several of the areas where public comment was sought, including the application of COPPA's definitions of "Internet," "website," and "online service" to new devices and technologies, the COPPA statute's actual knowledge standard for general audience websites and online services, the definition of "personal

---

[6](...continued)
originally set for 2017.

[7] *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule ("2010 Rule Review"), 75 FR 17089 (Apr. 5, 2010).

[8] *Id.*

information," emerging parental consent mechanisms, and COPPA's exceptions to prior parental consent.[9]

In addition to the dialogue at the public roundtable, the Commission received 70 comments from industry representatives, advocacy groups, academics, technologists, and individual members of the public in response to the April 5, 2010 request for public comment.[10] The comments addressed the efficacy of the Rule generally, and several possible areas for change.

II. COPPA's Definition of "Child"

The COPPA statute, and by extension, the COPPA Rule, defines as a child "an individual under the age of 13."[11] A few commenters suggested that COPPA's protections be broadened to cover a range of adolescents over age 12 and urged the Commission to seek a statutory change from Congress.[12] By contrast, the majority of commenters who addressed this issue expressed

---

[9] Information about the June 2, 2010 COPPA Roundtable is located at **http://www.ftc.gov/bcp/workshops/coppa/index.shtml**.

[10] Public comments in response to the Commission's April 5, 2010 FEDERAL REGISTER document are located at **http://www.ftc.gov/os/comments/copparulerev2010/index.shtm**. Comments have been numbered based upon alphabetical order. Comments are cited herein identified by commenter name, comment number, and, where applicable, page number.

[11] *See* 15 U.S.C. 6502(1).

[12] *See* Andrew Bergen (comment 4); Common Sense Media (comment 12).

concern that expanding COPPA's coverage to teenagers would raise a number of constitutional, privacy, and practical issues.[13]

Recognizing the difficulties of extending COPPA to children ages 13 or older, at least one commenter, the Institute for Public Representation, proposed the need for alternative privacy protections for teenagers. This commenter, while not proposing a statutory change to the definition of "child," called on the Commission to develop a set of privacy protections for teens, consistent with the Fair Information Practices Principles created by the Organisation for Economic Cooperation and Development, that would require understandable notices, limited information collection, an opt-in consent process, and access and control rights to data collected from them.[14]

In the course of drafting COPPA, Congress looked closely at whether adolescents should be covered by the law. Congress initially considered a requirement that operators make reasonable efforts to provide parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under

---

[13] *See* Sharon Anderson (comment 2); Kevin Brook (comment 6); Center for Democracy and Technology ("CDT") (comment 8), at 5; CTIA (comment 14), at 10; Facebook (comment 22), at 2; Elatia Grimshaw (comment 26); Interactive Advertising Bureau ("IAB") (comment 34), at 6-7; Harold Levy (comment 37); Motion Picture Association of America ("MPAA") (comment 42), at 4; National Cable & Television Association (comment 44), at 5 n.16; NetChoice (comment 45), at 2; Promotion Marketing Association ("PMA") (comment 51), at 5; Berin Szoka (comment 59), at 6; Toy Industry Association of America (comment 63), at 5. Five commenters urged the Commission to consider lowering or eliminating COPPA's age to permit younger children access to a variety of educational online offerings. *See* Eric MacDonald (comment 38); Mark Moran (comment 41); Steingreaber (comment 58); Karla Talbot (comment 60); Daniel Widrew (comment 67).

[14] *See* Institute for Public Representation (comment 33), at 42.

the age of 17.[15] Ultimately, however, Congress decided to define a "child" as an individual under age 13.[16] The Commission supported this assessment at the time, based in part on the view that young children under age 13 do not possess the level of knowledge or judgment to make appropriate determinations about when and if to divulge personal information over the Internet.[17] The Commission continues to believe that the statutory definition of a child remains appropriate.[18]

---

[15] *See Children's Online Privacy Protection Act of 1998*, S. 2326, 105th Cong. § 3(a)(2)(iii) (1998).

[16] *See* 15 U.S.C. 6502.

[17] *See Protection of Children's Privacy on the World Wide Web: Hearing on S. 2326 Before the Subcomm. on Communications of the S. Comm. on Commerce, Science & Transportation,* 105th Cong. (1998), at 5 (Statement of Robert Pitofsky, Chairman, Federal Trade Commission), *available at* **www.ftc.gov/os/1998/09/priva998.htm** ("Children are not fully capable of understanding the consequences of divulging personal information online.").

[18] *See Protecting Youths in an Online World: Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science & Transportation,* 111th Cong. 14-15 (2010) (Statement of Jessica Rich, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission), *available at* **http://www.ftc.gov/os/testimony/100715toopatestimony.pdf**.

Although teens face particular privacy challenges online,[19] COPPA's parental notice and consent approach is not designed to address such issues. COPPA's parental notice and consent model works fairly well for young children, but the Commission continues to believe that it would be less effective or appropriate for adolescents.[20] COPPA relies on children providing operators with parental contact information at the outset to initiate the consent process. The COPPA model would be difficult to implement for teenagers, as many would be less likely than young children to provide their parents' contact information, and more likely to falsify this information or lie about their ages in order to participate in online activities. In addition, courts have recognized that as children age, they have an increased constitutional right to access information and express themselves publicly.[21] Finally, given that adolescents are more likely

---

[19] For example, research shows that teens tend to be more impulsive than adults and that they may not think as clearly as adults about the consequences of what they do. *See, e.g.,* Transcript of Exploring Privacy, A Roundtable Series (Mar. 17, 2010), Panel 3: Addressing Sensitive Information, *available at* **http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/031710_sess3.pdf**; Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (April 14, 2010), *available at* **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864**. As a result, they may voluntarily disclose more information online than they should. On social networking sites, young people may share personal details that leave them vulnerable to identity theft. *See* Javelin Strategy and Research, 2010 *Identity Fraud Survey Report* (Feb. 2010), *available at* **https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf**. They may also share details that could adversely affect their potential employment or college admissions. *See e.g.,* Commonsense Media, *Is Social Networking Changing Childhood? A National Poll* (Aug. 10, 2009), *available at* **http://www.commonsensemedia.org/teen-social-media** (indicating that 28 percent of teens have shared personal information online that they would not normally share publicly).

[20] *Id.*

[21] *See*, *e.g., American Amusement Mach. Ass'n v. Kendrick*, 244 F.3d 572 (7th Cir. 2001) (citing *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-14 (1975)); *Tinker v. Des Moines Indep. Sch. Dist.*, 393 U.S. 503, 511-14 (1969).

than young children to spend a greater proportion of their time on websites and online services that also appeal to adults, the practical difficulties in expanding COPPA's reach to adolescents might unintentionally burden the right of adults to engage in online speech.[22] For all of these reasons, the Commission declines to advocate for a change to the statutory definition of "child."

Although the Commission does not recommend that Congress expand COPPA to cover teenagers, the Commission believes that it is essential that teens, like adults, be provided with clear information about uses of their data and be given meaningful choices about such uses. Therefore, the Commission is exploring new privacy approaches that will ensure that teens – and adults – benefit from stronger privacy protections than are currently generally available.[23]

III. COPPA's "Actual Knowledge" Standard

The COPPA statute applies to two types of operators: (1) those who operate websites or online services directed to children and collect personal information, and (2) those who have

---

[22] *See ACLU v. Ashcroft*, 534 F.3d 181, 196 (3d Cir. 2008) (citing *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007) ("Requiring users to go through an age verification process would lead to a distinct loss of personal privacy."); *see also Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 73 (1983) (citing *Butler v. Michigan*, 352 U.S. 380, 383 (1957) ("The Government may not reduce the adult population . . . to reading only what is fit for children."). *See also* Berin Szoka (comment 59), at 6.

[23] *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 36-36 (Dec. 1, 2010), *available at* **http://www.ftc.gov/os/2010/12/101201privacyreport.pdf**; *Protecting Youths in an Online World, supra* note 18, at 14-15 ("The FTC believes that its upcoming privacy recommendations based on its roundtable discussions will greatly benefit teens. The Commission expects that the privacy proposals emerging from this initiative will provide teens both a greater understanding of how their data is used and a greater ability to control such data.").

actual knowledge that they are collecting personal information from a child under age 13.[24] The second prong, commonly known as "the actual knowledge standard," holds operators of websites directed to teenagers, adults, or to a general audience, liable for providing COPPA's protections *only* when they know they are collecting personal information from a COPPA-covered child (*i.e.*, one under age 13). COPPA therefore was never intended to apply to the entire Internet, but rather to a subset of websites and online services.[25]

Congress did not define the term "actual knowledge" in the COPPA statute, nor did the Commission define the term in the Rule. The case law makes clear that actual knowledge does not equate to "knowledge fairly implied by the circumstances"; nor is actual knowledge "constructive knowledge," as that term is interpreted and applied legally.[26] Therefore, the

---

[24] *See* 15 U.S.C. 6503(a)(1).

[25] *See* MPAA (comment 42), at 10 ("Congress deliberately selected the actual knowledge standard because it served the objective of protecting young children without constraining appropriate data collection and use by operators of general audience websites. This standard was selected to serve the goals of COPPA without imposing excessive burdens – including burdens that could easily constrain innovation – on general audience sites and online services").

[26] The original scope of COPPA, as indicated in S. 2326 and H.R. 4667, would have applied to any commercial website or online service used by an operator to "knowingly" collect information from children. *See Children's Online Privacy Protection Act of 1998*, S. 2326, 105th Cong. § 2(11)(A)(iii) (1998); *Electronic Privacy Bill of Rights Act of 1998*, H.R. 4667, 105th Cong. § 105(7)(A)(iii) (1998). Under federal case law, the term "knowingly" encompasses actual, implied, and constructive knowledge. *See Schmitt v. FMA Alliance*, 398 F.3d 995, 997 (8th Cir. 2005); *Freeman United Coal Mining Co. v. Federal Mine Safety and Health Review Comm'n*, 108 F.3d 358, 363 (D.C. Cir. 1997).

Upon the consideration of testimony from various witnesses, Congress modified the knowledge standard in the final legislation to require "actual knowledge." *See Internet Privacy Hearing: Hearing on S. 2326 Before the Subcomm. on Communications of the S. Comm. on Commerce, Science, and Transportation*, 105th Cong. 1069 (1998). Actual knowledge is

(continued...)

Commission has advised that operators of general audience websites are not required to investigate the ages of their users.[27] By contrast, however, operators that ask for – or otherwise collect – information establishing that a user is under the age of 13 trigger COPPA's verifiable parental consent and all other requirements.[28]

In general, commenters to the Rule review expressed widespread support for Congress's retention of the statutory actual knowledge standard. Supporters find that the standard provides necessary certainty regarding the boundaries of operators' legal liability for COPPA violations.[29] Commenters generally felt strongly that a lesser standard, *e.g.*, constructive or

---

[26](...continued)
generally understood from case law to establish a far stricter standard than constructive knowledge or knowledge implied from the ambient facts. *See United States v. DiSanto*, 86 F.3d 1238, 1257 (1st Cir. 1996) (citing *United States v. Spinney*, 65 F.3d 231, 236 (1st Cir. 1995), for the proposition that "when considering the question of "knowledge" [it is helpful] to recall that "the length of the hypothetical knowledge continuum" is marked by "constructive knowledge" at one end and "actual knowledge" at the other with various "gradations," such as "notice of likelihood" in the "poorly charted area that stretches between the poles").

[27] *See* Children's Online Privacy Protection Rule, Statement of Basis and Purpose ("1999 Statement of Basis and Purpose"), 64 FR 59888, 59889 (Nov. 3, 1999), *available at* **http://www.ftc.gov/os/1999/10/64Fr59888.pdf**.

[28] *See id.* at 59892 ("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").

[29] *See* CTIA (comment 14), at 2; Direct Marketing Association ("DMA") (comment 17), at 8; MPAA (comment 42), at 9; Toy Industry Association, Inc. (comment 63), at 5; Jeffrey Greenbaum, Partner, Frankfurt Kurnit Klein & Selz PC, and J. Beckwith ("Becky") Burr, Partner, WilmerHale, Remarks from *The "Actual Knowledge" Standard in Today's Online*
(continued...)

implied knowledge, would cause extreme uncertainty for operators of general audience websites or online services seeking to comply with the law since they would be obliged either to make guesses about the presence of underage children or to deny access to a wide swath of participants, not only young children.[30] According to commenters, such actions would result in greater data collection from all users, including children, in order to determine who should receive COPPA protections (or, alternatively, be denied access to a site). Commenters viewed this result as contradictory to COPPA's goal of minimizing data collection.[31]

A handful of commenters argued for a different standard. One commenter urged the Commission to require commercial website operators to make reasonable efforts to determine if a child is registering online, taking into consideration available technology.[32] According to this commenter, website operators otherwise face minimal legal risk and business incentive to proactively institute privacy protections for children online. Other commenters, such as the Institute for Public Representation and Microsoft, urged the Commission to adopt clearer

---

[29](...continued)
Environment Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 78-79 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**.

[30] *See* Sharon Anderson (comment 2); Boku (comment 5); CDT (comment 9), at 6; CTIA (comment 14), at 2; DMA (comment 17), at 8; Facebook (comment 22), at 7; IAB (comment 34), at 6.

[31] *See* CTIA (comment 14), at 2; DMA (comment 17), at 8; Facebook (comment 22), at 7-8.

[32] *See* Harry A. Valetk (comment 66), at 4.

guidance on when an operator will be considered to have obtained actual knowledge that it has collected personal information from a child.[33]

Despite the limitations of the actual knowledge standard, the Commission is persuaded that this remains the correct standard to be applied to operators of websites and online services that are not directed to children. Accordingly, the Commission does not advocate that Congress amend the COPPA statute's actual knowledge requirement at this time. Actual knowledge is far more workable, and provides greater certainty, than other legal standards that might be applied to the universe of general audience websites and online services. This is because the actual knowledge standard is triggered only at the point at which an operator becomes aware of a child's age. By contrast, imposing a lesser "reasonable efforts" or "constructive knowledge" standard might require operators to ferret through a host of circumstantial information to determine who may or may not be a child.

As described in detail below, with this Notice of Proposed Rulemaking, the Commission is proposing several modifications to the Rule's definition of "personal information."[34] Were

---

[33] *See* Institute for Public Representation (comment 33), at 34 (urging the Commission to make clear that an operator can gain actual knowledge where it obtains age information from a source other than the child and where it creates a category for behavioral advertising to children under age 13. "Simply, if an operator decides on, or uses, or purports to know the fact that someone is a child, then that operator has actual knowledge that it is dealing with a child."); Microsoft (comment 39), at 8 (asking the Commission to provide clear guidance on how operators can better meet COPPA's objectives of providing access to rich media content while not undermining parental involvement).

[34] For example, the Commission proposes defining as personal information persistent identifiers and screen or user names where they are used for functions other than or in addition to support for the internal operations of a website or online service. The Commission also proposes including identifiers that link the activities of a child across different websites or (continued...)

the Commission to recommend that Congress change COPPA's actual knowledge standard, the changes the Commission proposes to the Rule's definitions might prove infeasible if applied across the entire Internet. The impact of the proposed changes to the definition of personal information are significantly narrowed by the fact that COPPA only applies to the finite universe of websites and online services directed to children and websites and online services with actual knowledge.

IV. COPPA's Coverage of Evolving Technologies

The Commission's April 5, 2010 FEDERAL REGISTER document sought public input on the implications for COPPA enforcement raised by technologies such as mobile communications, interactive television, interactive gaming, and other evolving media.[35] The Commission's June 2, 2010 roundtable featured significant discussion on the breadth of the terms "Internet," "website located on the Internet," and "online service" as they relate to the statute and the Rule.

Commenters and roundtable participants expressed a consensus that both the COPPA statute and Rule are written broadly enough to encompass many new technologies without the need for new statutory language.[36] First, there is widespread agreement that the statute's

---

[34](...continued)
online services, as well as digital files containing a child's image or voice, in the definition. *See infra* Part V.A.(4).

[35] *See* 2010 Rule Review, *supra* note 7, at 17090.

[36] *See* CDT (comment 8), at 2; Edward Felten, Dir. and Professor of Computer Sci. and Pub. Affairs, Princeton Univ. (currently Chief Technologist at the Federal Trade Commission), Remarks from *The Application of COPPA's Definitions of "Internet," "Website,"* (continued...)

definition of "Internet," covering 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," is device neutral.[37]

While neither the COPPA statute nor the Rule defines a "website located on the Internet," the term is broadly understood to cover content that users can access through a browser on an ordinary computer or mobile device.[38] Likewise, the term "online service" broadly covers any service available over the Internet, or that connects to the Internet or a wide-area network.[39] The Commission agrees with commenters that a host of current technologies

---

[36](...continued)
and "Online Service" to New Devices and Technologies Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 13-14 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf** ("[T]his was and still is a spot-on definition of what "Internet" means – worldwide interconnection and the use of TCP or IP or any of that suite of protocols.").

[37] *See* CDT (comment 8), at 2. However, two commenters urged the Commission to consider modifying or expanding the definition of "Internet" so as to expressly acknowledge the convergence of technologies, *e.g.*, mobile devices and other applications that are platform neutral or capable of storing and transmitting data in the manner of a personal computer. *See* Electronic Privacy Information Center ("EPIC") (comment 19), at 7-8; Jayne Hitchcock (comment 29).

[38] *See* AT&T (comment 3), at 5; Spratt (comment 57); Edward Felten, *supra* note 36, at 15.

[39] *See* John B. Morris, Jr., General Counsel and Director, Internet Standards, Technology and Policy Project, CDT, and Angela Campbell, Institute for Public Representation, Georgetown Univ. Law Ctr., Remarks from *The Application of COPPA's Definitions of "Internet," "Website," and "Online Service" to New Devices and Technologies* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 16-17 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**. One commenter mentioned that the terms "Internet" and "online" were seemingly intended by (continued...)

that access the Internet or a wide area network are "online services" currently covered by COPPA and the Rule. This includes mobile applications that allow children to play network-connected games, engage in social networking activities, purchase goods or services online, receive behaviorally targeted advertisements, or interact with other content or services.[40] Likewise, Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location based services, also are online services covered by COPPA and the Rule. The Commission does not believe that the term "online service" needs to be further defined either in the statute or in the Rule.[41]

Although many mobile activities are online services, it is less clear whether all short message services ("SMS") and multimedia messaging services ("MMS") are covered by COPPA.[42] One commenter maintained that SMS and MMS text messages cross wireless

---

[39](...continued)
Congress to be used interchangeably to mean "the interconnected world-wide network of networks." *See* Entertainment Software Association (comment 20), at 15 (citing the legislative history, 144 Cong. Rec. S8482-83, Statement of Sen. Bryan (1998)). *But see* Edward Felten, *supra* note 36, at 19.

[40] *See, e.g.*, Angela Campbell, *supra* note 39, at 30-31.

[41] The FTC has brought a number of cases alleging violations of COPPA in connection with the operation of an online service, including: *United States v. W3 Innovations LLC*, No. CV-11-03958 (N.D. Cal., filed Aug. 12, 2011) (child-directed mobile applications); *United States v. Playdom, Inc*., No. SA CV-11-00724 (C.D. Cal., filed May 11, 2011) (online virtual worlds); *United States v. Sony BMG Music Entertainment*, No. 08 Civ. 10730 (S.D.N.Y, filed Dec. 10, 2008) (social networking service); *United States v. Industrious Kid, Inc.*, No. CV-08-0639 (N.D. Cal., filed Jan. 28, 2008) (social networking service); *United States v. Xanga.com, Inc.*, No. 06-CIV-6853 (S.D.N.Y., filed Sept. 7, 2006) (social networking service); and *United States v. Bonzi Software, Inc*., No. CV-04-1048 (C.D. Cal., filed Feb. 14, 2004) (desktop software application).

[42] *See* 2010 Rule Review, *supra* note 7, at 17090 (Question 11); *see also* Denise (continued...)

service providers' networks and short message service centers, not the public Internet, and therefore that such services are not Internet-based and are not "online services."[43] However, another panelist at the Commission's June 2, 2010 roundtable cautioned that not all texting programs are exempt from COPPA's coverage.[44] For instance, mobile applications that enable users to send text messages from their web-enabled devices without routing through a carrier-issued phone number constitute online services.[45] Likewise, retailers' premium texting and coupon texting programs that register users online and send text messages from the Internet to users' mobile phone numbers are online services.[46]

---

[42](...continued)
Tayloe, President, Privo, Inc., Remarks from *Emerging Parental Verification Access and Methods* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 27 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf** (questioning whether a "text to vote" marketing campaign is covered by COPPA).

[43] *See* CTIA (comment 14), at 2-5 (citing the Federal Communications Commission's rules and regulations implementing the CAN-SPAM Act of 2003 and the Telephone Consumer Protection Act of 1991, finding that phone-to-phone SMS is not captured by Section 14 of CAN-SPAM because such messages do not have references to Internet domains). The Commission agrees that where mobile services do not traverse the Internet or a wide-area network, COPPA will not apply. *See* Michael Altschul, Senior Vice President and Gen. Counsel, CTIA, Remarks from *The Application of COPPA's Definitions of "Internet," "Website," and "Online Service" to New Devices and Technologies* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 19-21 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**.

[44] *See* Edward Felten, *supra* note 36, at 27-28.

[45] For example, online texting services offered by TextFree, Textie, and textPlus+ that permit users to communicate via text message over the Internet.

[46] For example, text alert coupon and notification services offered by retailers such as Target and JC Penney.

The Commission will continue to assess emerging technologies to determine whether or not they constitute "websites located on the Internet" or "online services" subject to COPPA's coverage.

V. Proposed Modifications to the Rule

As discussed above, commenters expressed a consensus that, given its flexibility and coverage, the COPPA Rule continues to be useful in helping to protect children as they engage in a wide variety of online activities. The Commission's experience in enforcing the Rule, and public input received through the Rule review process, however, demonstrate the need to update certain Rule provisions. After extensive consideration, the Commission proposes modifications to the Rule in the following five areas: Definitions, Notice, Parental Consent, Confidentiality and Security of Children's Personal Information, and Safe Harbor Programs. In addition to modifying these provisions, the Commission proposes adding a new Rule section addressing data retention and deletion. Each of these changes is discussed in detail below.

A. Definitions (16 CFR 312.2)

The Commission proposes to modify particular definitions to update the Rule's coverage and, in certain cases, to streamline the Rule's language. The Commission proposes modifications to the definitions of "collects or collection," "online contact information," "personal information," "support for the internal operations of the website or online service," and "website or online service directed to children." The Commission also proposes a minor structural change to the Rule's definition of "disclosure."

(1) *Collects or collection*

Section 312.2 of the Rule defines "collects or collection" as:

> [T]he 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.

The Commission proposes amending paragraph (a) to change the term "requesting that children submit personal information online" to "requesting, prompting, or encouraging a child to submit personal information online" in order to clarify that the Rule covers the online collection of personal information both when an operator mandatorily requires it, and when an operator merely prompts or encourages a child to provide such information.

Section 312.2(b) currently defines "collects or collection" to include enabling children to publicly post personal information (*e.g.*, on social networking sites or on blogs), "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."[47] This aspect of

[47] Operators who offer services such as social networking, chat, bulletin boards and who do not pre-strip (*i.e.*, completely delete) such information are deemed to have "disclosed" (continued...)

COPPA's definition of "collects or collection" has come to be known as the "100% deletion standard."[48] Several commenters indicated that this standard, while well-meaning, serves as an impediment to operators' implementation of sophisticated filtering technologies that might aid in the detection and removal of personal information.[49] Some commenters urged the Commission to revise the Rule to specify the particular types of filtering mechanisms – for example, white lists, black lists, or algorithmic systems – that the Commission believes conform to the Rule's current 100% deletion requirement.[50] One commenter urged the Commission to exercise caution in modifying the Rule to permit the use of automated filtering systems to strip personal information from posts prior to posting; this commenter urged the Commission to make clear that the use of

---

[47](...continued)
personal information under COPPA's definition of "disclosure." *See* 16 CFR 312.2.

[48] *See* Phyllis Marcus, Remarks from *COPPA's Exceptions to Parental Consent* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online 310 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**.

[49] *See* Entertainment Software Association (comment 20), at 13-14; Rebecca Newton (comment 46), at 4; *see also* WiredSafety.org (comment 68), at 15.

[50] *See* Berin Szoka (comment 59), Szoka Responses to Questions for the Record, at 19 ("[T]he FTC could . . . allow operators, at least in some circumstances, to use "an automated system of review and/or posting" to satisfy the existing "deletion exception to the definition of collection." In other words, sites could potentially allow children to communicate with each other through chat rooms, message boards, and other social networking tools *without* having to obtain verifiable parental consent if they had in place algorithmic filters that would automatically detect personal information such as a string of seven or ten digits that seems to correspond to a phone number, a string of eight digits that might correspond to a Social Security number, a street address, a name, or even a personal photo – and prevent children from sharing that information in ways that make the information "publicly available"); *see also* Privo (comment 50), at 5.

an automated system *would not* provide an operator with a safe harbor from enforcement action in the case of an inadvertent disclosure of personal information.[51]

The Commission has undertaken this Rule review with an eye towards encouraging the continuing growth of engaging, diverse, and appropriate online content for children that includes strong privacy protections by design. Children increasingly seek interactive online environments where they can express themselves, and operators should be encouraged to develop innovative technologies to attract children to age-appropriate online communities while preventing them from divulging their personal information. Unfortunately, websites that provide children with only limited communications options often fail to capture their imaginations for very long. After careful consideration, the Commission believes that the 100% deletion standard has set an unrealistic hurdle to operators' development and implementation of automated filtering systems.[52] In its place, the Commission proposes a "reasonable measures" standard whereby operators who employ technologies reasonably designed to capture *all or virtually all* personal information inputted by children should not be deemed to have "collected" personal information. This proposed change is intended to encourage the development of systems, either automated, manual, or a combination thereof, to detect and delete all or virtually all personal information that may be submitted by children prior to its public posting.[53]

---

[51] *See* EPIC (comment 19), at 6-7.

[52] In fact, inquiries about automated filtering systems, and whether they could ever meet the Commission's current 100% deletion standard, are among the most frequent calls to the Commission's COPPA hotline.

[53] In the Commission's experience, establishing a broad standard of reasonableness permits industry to innovate specific security methods that best suit particular needs, and the (continued...)

Finally, the Commission proposes simplifying paragraph (c) of the Rule's definition of "collects or collection" to clarify that it includes all means of passive tracking of a child online, irrespective of the technology used. The proposed paragraph removes the language "or use of any identifying code linked to an individual, such as a cookie" and simply states "passive tracking of a child online."

Therefore, the Commission proposes to amend the definition of "collects or collection" so that it reads:

> *Collects* or *collection* means the gathering of any personal information from a child by any means, including but not limited to:
>
> (a) Requesting, prompting, or encouraging a child to submit personal information online;
>
> (b) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or,
>
> (c) The passive tracking of a child online.[54]

---

[53](...continued)
Commission has set similar "reasonableness" standards in other enforcement arenas. For example, in its law enforcement actions involving breaches of data security, the Commission consistently has required respondents to establish and maintain comprehensive information security programs that are "reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." *See, e.g., Ceridian Corp.*, FTC Dkt. No. C-4325 (June 15, 2011)*; Lookout Servs., Inc.*, FTC Dkt. No. C-4326 (June 15, 2011).

[54] One commenter, EPIC, expressed the opinion that the Rule's reference to information collected "by any means" in the definition of "collects or collection" is ambiguous with regard to information acquired offline that is uploaded, stored, or distributed to third parties
(continued...)

(2) ***Disclosure***

Section 312.2 of the Rule defines "disclosure" as:

> (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.

The Commission proposes making several minor modifications to this definition that are consistent with the statutory definition. First, the Commission proposes broadening the title of this definition from "disclosure" to "disclose or disclosure" to clarify that in every instance in which the Rule refers to instances where an operator "disclose[s]" information, the definition of

---

[54](...continued)
by operators. *See* EPIC (comment 19), at 5. However, Congress limited the scope of COPPA to information that an operator collects *online* from a child; COPPA does not govern information collected offline. *See* 15 U.S.C. 6501(8) (defining the personal information as "individually identifiable information about an individual collected online. . . ."); 144 Cong. Rec. S11657 (Oct. 7, 1998) (Statement of Sen. Bryan) ("This is an online children's privacy bill, and its reach is limited to information collected online from a child.").

disclosure shall apply. In addition, the Commmission proposes moving the definitions of "release of personal information" and "support for the internal operations of the website or online service" contained within the definition of "disclosure" to stand-alone definitions within § 312.2 of the Rule.[55] This change will clarify what is intended by the terms "release of personal information" and "support for the internal operations of the website or online service" where those terms are referenced elsewhere in the Rule and where they are not directly connected with the terms "disclose" or "disclosure."[56]

Therefore, the Commission proposes to amend the definition of "disclosure" to read:

> *Disclose or disclosure* means, with respect to personal information:
>
> (a) The release of personal information collected by an operator from a child in identifiable form 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,
>
> (b) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

---

[55] The Commission also proposes minor changes to the definition of "support for the internal operations of a website or online service," as described in Part V.A(5). below.

[56] For example, the term "support for the internal operations of the website or online service" is included within the proposed revisions to the definition of "personal information." *See infra* Part V.A.(5). The term "release of personal information" is included within the proposed revised provision to § 312.8 regarding "Confidentiality, security, and integrity of personal information collected from children." *See infra* Part V.D.

(3) *"Release of personal information"*

The Commission proposes to define the term "release of personal information" separately from its current inclusion within the definition of "disclosure." Since the term applies to provisions of the Rule that do not relate solely to disclosures,[57] this stand-alone definition will provide greater clarity as to the terms' applicability throughout the Rule. In addition, the Commission proposes technical changes to clarify that the term "release of personal information" primarily addresses business-to-business uses of personal information. Public disclosure of personal information is covered by paragraph (b) of the definition of "disclosure." Therefore, the Commission proposes to revise the definition of "release of personal information" so that it reads:

> *Release of personal information* means the sharing, selling, renting, or transfer of personal information to any third party.

(4) *"Support for the internal operations of the website or online service"*

The Commission also proposes separating out the term "support for the internal operations of the website or online service" from the definition of "disclosure." The Commission recognizes that the term "support for internal operations of the website or online service" – *i.e.*, activities necessary to maintain the technical functioning of the website or online service – is an important limiting concept that warrants further explanation. The Rule recognizes that information that is collected by operators for the sole purpose of support for internal operations should be treated differently than information that is used for broader purposes.

---

[57] *See, e.g.*, discussion regarding 16 CFR 312.8 (confidentiality, security and integrity of children's personal information), *infra* Part V.D.

The term currently is a part of the definitions of "disclosure" and "third party" within the Rule. As explained below, the Commission proposes to expand the definition of "personal information" to include "screen or user names" and "persistent identifiers," when such items are used for functions other than or in addition to "support for the internal operations of the website or online service."[58] In proposing to create a separate definition of "support for the internal operations of a website or online service," the Commission also proposes to expand that definition to include "activities necessary to protect the security or integrity of the website or online service." With this change, the Commission recognizes operators' need to protect themselves or their users from security threats, fraud, denial of service attacks, user misbehavior, or other threats to operators' internal operations.[59] In addition, the Commission proposes adding the limitation that information collected for such purposes may not be used or disclosed for any other purpose, so that if there is a secondary use of the information, it becomes "personal information" under the Rule.

The Commission recognizes that operators use persistent identifiers and screen names to aid the functionality and technical stability of websites and online services and to provide a good user experience, and the Commission does not intend to limit operators' ability to collect such information from children for those purposes. However, the Commission also recognizes that such identifiers may be used in more expansive ways that affect children's privacy. In the

---

[58] *See infra* Part V.(5)(b) and (c).

[59] *See* WiredSafety.org (comment 68), at 17.

sections that follow, the Commission sets forth the parameters within which operators may collect and use screen names and persistent identifiers without triggering COPPA's application.[60]

The Commission proposes to revise the definition of "support for the internal operations of website or online service" so that it states:

> *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, to protect the security or integrity of the website or online service, or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose.

(5) *Online Contact Information*

Section 312.2 of the Rule defines "online contact information" as "an e-mail address or any other substantially similar identifier that permits direct contact with a person online." The Commission proposes to clarify this definition to flag that the term covers *all* identifiers that permit direct contact with a person online, and to eliminate any inconsistency between the stand-alone definition of online contact information and the use of the same term within the Rule's definition of "personal information."[61] The revised definition set forth below adds commonly used forms of online identifiers, including instant messaging user identifiers, voice

---

[60] *Id.*

[61] The Rule currently defines as personal information "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." 16 CFR 312.2 (paragraph (c), definition of "personal information"). The Commission also proposes removing the listing of identifiers from the definition of personal information and substituting the simple phrase "online contact information" instead. *See infra* Part V.A.(4)(a). By doing so, the Commission hopes to streamline the Rule's definitions in a way that is useful and accessible for operators.

over internet protocol (VOIP) identifiers, and video chat user identifiers. The proposed definition makes clear, however, that the identifiers included are not intended to be exhaustive, and may include other substantially similar identifiers that permit direct contact with a person online.

Therefore, the Commission proposes to amend the definition of "online contact information" to state:

> *Online contact information* means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

(6) *Personal Information*

The COPPA statute defines personal information as 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;
>
> (D) a telephone number;[62]
>
> (E) a Social Security number;
>
> (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or

---

[62] The term "telephone number" includes landline, web-based, and mobile phone numbers.

> (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.[63]

As explained below, the Commission proposes to use this statutorily granted authority in paragraph (F) to modify, and in certain cases, expand, upon the Rule's definition of "personal information" to reflect technological changes.

a. Online Contact Information (revised paragraph (c))

The Commission proposes to replace existing paragraph (c) of the Rule's definition of "personal information," which refers to "an email 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," with the broader term "online contact information," as newly defined.[64] Moreover, as discussed immediately below, the Commission proposes to move the existing reference to a "screen name" to a separate item within the definition of "personal information."

---

[63] 15 U.S.C. 6502(8). The Federal Trade Commission originally used the authority granted under Section 6502(8)(F) to define personal information under the COPPA Rule to include the following pieces of information not specifically listed in the statute:

- other online contact information, including but not limited to an instant messaging user identifier;
- a screen name that reveals an individual's e-mail address;
- 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; and,
- a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting.

[64] *See supra* Part V.A.(4)(a).

b. Screen or User Names (revised paragraph (d))

Currently, screen names are considered "personal information" under COPPA only when they reveal an individual's email address. The Commission proposes instead that screen (or user) names be categorized as personal information when they are used for functions other than, or in addition to, support for the internal operations of the website or online service. This change reflects the reality that screen and user names increasingly have become portable across multiple websites or online services, and permit the direct contact of a specific individual online regardless of whether the screen or user names contain an email address.[65]

The proposed definition exempts screen or user names that are used solely to maintain the technical functioning of the website or online service. This qualification is intended to retain operators' ability to utilize screen or user names *within* a website or online service (absent the collection, use, or disclosure of *other* personal information) without obtaining prior parental consent. Accordingly, an operator may allow children to establish screen names for use within a site or service. Such screen names may be used for access to the site or service, to identify users to each other, and to recall user settings. However, where the screen or user name is used for purposes other than to maintain the technical functioning of the website or online service, the screen name becomes "personal information" under the proposed Rule.

c. Persistent Identifiers (revised paragraph (g)) and Identifiers Linking a Child's Online Activities (new paragraph (h))

The existing Rule includes as personal information "a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is

---

[65] *See, e.g.*, OpenId, Windows Live ID, and the Facebook Platform.

associated with individually identifiable information."[66] In its 1999 Statement of Basis and Purpose, the Commission discussed persistent identifiers that automatically are collected by websites, such as static IP addresses and processor serial numbers, stating that "unless such identifiers are associated with other individually identifiable personal information, they would not fall within the Rule's definition of 'personal information.'" Moreover, with respect to information stored in cookies, the Commission stated that "[i]f the operator either collects individually identifiable information using the cookie or collects non-individually identifiable information using the cookie that is combined with an identifier, then the information constitutes 'personal information' under the Rule, regardless of where it is stored."[67] Taken together, these statements limit COPPA's coverage of persistent identifiers solely to those identifiers that are otherwise linked to "personal information" as defined by the Rule.

Developments in technology in the intervening twelve years since the COPPA Rule was issued, and the resulting implications for consumer privacy, have led to a widespread reexamination of the concept of "personal information" and of the types of information COPPA should cover.[68] While it is clear that COPPA always was intended to regulate an operator's

---

[66] *See* paragraph (f) to the definition of "personal information." 16 CFR 312.2.

[67] *See* 1999 Statement of Basis and Purpose, 64 FR 59888, 59892-93.

[68] Commission staff recognized in its 2009 online behavioral advertising report that, "in the context of online behavioral advertising, the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data." FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, 21-22 (Feb. 2009), *available at* **http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.** Similarly, the Federal Trade Commission 2010 Staff Privacy Report cited widespread recognition among industry and academics that the traditional distinction between the two categories of data has eroded, and that (continued...)

ability to obtain information from, and market back to, children,[69] methods of marketing online have burgeoned in recent years. In this regard, the Commission sought comment on whether certain identifiers, such as IP address, zip code, date of birth, gender, and information collected in connection with online behavioral advertising, should now be included within the Rule's definition of "personal information."[70]

Numerous comments to the Rule review addressed this question.[71] Several commenters opposed such an expansion, pointing out that the collection of certain identifiers, such as IP addresses, are integral to the delivery of online content.[72] According to these commenters, if an

---

[68](...continued)
information practices and restrictions that rely on this distinction are losing their relevance. *See* Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 23, at 35-36.

[69] *See* 144 Cong. Rec. S8482 (July 17, 1998) (Statement of Sen. Bryan) ("Unfortunately, the same marvelous advances in computer and telecommunication technology that allow our children to reach out to new resources of knowledge and cultural experiences are also leaving them unwittingly vulnerable to exploitation and harm by deceptive marketers and criminals . . . . Much of this information appears to be harmless, but companies are attempting to build a wealth of information about you and your family without an adult's approval – a profile that will enable them to target and to entice your children to purchase a range of products. The Internet gives marketers the capability of interacting with your children and developing a relationship without your knowledge").

[70] *See* 2010 Rule Review, *supra* note 7, at 17090.

[71] *See, e.g.*, BOKU (comment 5); CDT (comment 8); DMA (comment 17), at 6-9; Entertainment Software Association (comment 20), at 17-18; Google, Inc. (comment 24), at 6-7; Institute for Public Representation (comment 33), at 21; IAB (comment 34), at 3-5; Interstate Commerce Coalition (comment 35), at 2; Microsoft Corporation (comment 39), at 9-10; MPAA (comment 42), at 6-7; NetChoice (comment 45), at 6-7; Paul Ohm (comment 48); TechAmerica (comment 61), at 5-6; Toy Industry Association, Inc. (comment 63), at 7-10; TRUSTe (comment 64), at 3-5.

[72] *See* Google, Inc. (comment 24), at 7; Internet Commerce Coalition (comment 35), at 2-3.

IP address, on its own, were to be included within the definition of "personal information," virtually every website or online service directed to children would be subject to COPPA's requirements, regardless of whether any additional information is collected, used, or disclosed, because a browser's communication with a website typically reveals the user's IP address to the website operator. Commenters especially expressed concern about operators' ability to obtain prior verifiable parental consent in such situations.[73] In addition, some commenters noted that an IP address may not lead an operator to a specific individual, but rather, indicate only a particular computer or computing device shared by a number of individuals.[74]

Several other commenters addressed the question of whether identifiers such as cookies or other technologies used to track online activities should be included within the definition of "personal information." As with the comments regarding IP addresses, these commenters maintained that uses of cookies and other tracking devices do not result in the contacting of specific individuals online as contemplated by Congress in the COPPA statute.[75] Moreover, some commenters asserted that these technologies can be used for a number of beneficial purposes, *e.g.*, some operators use cookies to protect children from inappropriate advertising (and conversely, to deliver only appropriate advertising); other operators use cookies to personalize children's online experiences. Finally, these commenters contended that expanding

---

[73] *See, e.g.*, Entertainment Software Association (comment 20), at 18; Interstate Commerce Coalition (comment 35), at 2.

[74] *See* Toy Industry Association, Inc. (comment 63), at 9; TRUSTe (comment 64), at 5.

[75] *See* Facebook (comment 22), at 6; Microsoft Corporation (comment 39), at 9; Toy Industry Association, Inc. (comment 63), at 7.

COPPA to include cookies and other online behavioral advertising technologies is unnecessary because existing self-regulatory principles for online behavioral advertising are sufficient to curtail targeted advertising to children.[76]

By contrast, several commenters asserted that identifiers such as cookies and IP addresses can be used by online operators to track and communicate with *specific* individuals and should be included within COPPA's categories of information considered to be personal.[77]

After careful consideration, the Commission believes that persistent identifiers can permit the contacting of a specific individual, and thus, with the limitations described below, should be included as part of a revised definition of "personal information" in the COPPA Rule. The Commission does not agree with commenters who argue that persistent identifiers only allow operators to contact a specific device or computer. Information that "permits the physical or online contacting of a specific individual" does not mean information that permits the contacting of only a single individual, to the exclusion of all other individuals. For example, the COPPA statute includes within the definition of "personal information" a home address alone or a phone number alone – information that is often applicable to an entire household. The Commission believes this reflects the judgment of Congress that an operator who collects this

---

[76] *See* CDT (comment 8, at 8) (referring to the Network Advertising Initiative's *2008 NAI Principles Code of Conduct*); Entertainment Software Association (comment 20), at 19 (referring to the *Self-Regulatory Principles for Online Behavioral Advertising* issued by the American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus in July 2009); Facebook (comment 22), at 7.

[77] *See* Common Sense Media (comment 12), at 8; EPIC (comment 19), at 9; Institute for Public Representation (comment 33), at 21.

information is reasonably likely to be able to contact a specific individual, even without having collected other identifying information. The Commission believes the same is true of persistent identifiers.

Moreover, increasingly, consumer access to computers is shifting from the model of a single, family-shared, personal computer to the widespread distribution of person-specific, Internet-enabled, handheld devices to each member within a household, including children.[78] Such handheld devices often have one or more unique identifiers associated with them that can be used to persistently link a user across websites and online services, including mobile applications.[79] With this change in computing use, operators now have a better ability to link a particular individual to a particular computing device.

---

[78] *See* Common Sense Media, *Do Smart Phones = Smart Kids? The Impact of the Mobile Explosion on America's Kids, Families, and Schools* (Apr. 2010), *available at* **http://www.commonsensemedia.org/smartphones-smartkids** (citing a study from the NPD Group, Inc. finding that 20% of U.S. children ages 4-14 owned a cell phone in 2008); N. Jackson, "More Kids Can Work Smartphones Than Can Tie Their Own Shoes," The Atlantic (Jan. 24, 2011), *available at* **http://www.theatlantic.com/technology/archive/2011/01/more-kids-can-work-smartphones-than-can-tie-their-own-shoes/70101/**; *see also* S. Smith, "Now It's Personal: Mobile Nears the Privacy Third Rail," Behavioral Insider (Apr. 22, 2011), *available at* **http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=149196** (warning that "[m]any of the arguments used to assuage worries about digital privacy online are simply less effective [in the mobile space]. When data can be tied to specific device IDs, times and location, insistence that the resulting data is 'anonymized' (no matter how true it may be) is very hard for the layman to swallow.").

[79] Sometimes called "processor serial numbers," "device serial numbers," or "unique device identifier," unique identifiers refer to software-readable or physical numbers embedded by manufacturers into individual processors or devices. *See, e.g.*, J. Valentino-DeVries, *Unique Phone ID Numbers Explained*, Wall St. J. (Dec. 19, 2010), *available at* **http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained/**.

At the same time, the Commission is mindful of the concerns raised by commenters that including persistent identifiers within the definition of personal information, without further qualification, would hinder operators' ability to provide basic online services to children. Several commenters indicated that websites and online services must identify and use IP addresses to deliver content to computers; if IP addresses, without more, were treated as "personal information" under COPPA, a site or service would be liable for collecting personal information as soon as a child landed on its home page or screen.[80] The Commission agrees that such an approach is over-broad and unworkable.[81]

The Commission believes that when a persistent identifier is used only to support the internal operations of a website or online service, rather than to compile data on specific computer users, the concerns underlying COPPA's purpose are not present.[82] Accordingly, the Commission proposes to modify the definition of "personal information" by revising paragraph (g), and adding a paragraph (h), as follows:

> (g) A persistent identifier, including but not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier, where such persistent identifier is used

---

[80] *See* CDT (comment 9), at 7-8; DMA (comment 17), at 6; Entertainment Software Association (comment 20), 17-18; Google (comment 24), 7; Internet Commerce Coalition (comment 35), at 2-3; and TechAmerica (comment 61), at 6.

[81] As some commenters noted, it would be impracticable to obtain verifiable parental consent prior to the collection of an IP address for purposes of delivering online content, since website operators would not know at that point in time that the website visitor was a child, and would have no means of obtaining consent from that child's parent. *See, e.g.*, Internet Commerce Coalition (comment 35), at 2.

[82] *See* 144 Cong. Rec. S8482 (July 17, 1998) (Statement of Sen. Bryan).

for functions other than or in addition to support for the internal operations of the website or online service;

(h) an identifier that links the activities of a child across different websites or online services;

Proposed paragraph (g) – which covers persistent identifiers *where they are used for functions other than, or in addition to, support for the internal operations of the website or online service* – is designed not to interfere with operators' ability to deliver content to children within the ordinary operation of their websites or online services. This limitation takes into account the comments expressing concern about the potential for COPPA to interfere with the ordinary operation of websites or online services.[83] The new language in the definition would permit operators' use of persistent identifiers for purposes such as user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft. However, the new language would require parental notification and consent prior to the collection of persistent identifiers where they are used for purposes such as amassing data on a child's online activities or behaviorally targeting advertising to the child. Therefore, operators such as network advertisers may not claim the collection of persistent identifiers as a technical function under the "support for internal operations" exemption.

New paragraph (h) of the definition of "personal information" is intended to serve as a catch-all category covering the online gathering of information about a child over time for the

[83] S*ee* Boku (comment 5) (encouraging the Commission to regulate the use of identifiers such as IP address, device data, or any other data automatically captured during interaction with a user and a web site rather than the data capture itself or the storage of such data; *see also* CDT (comment 8), at 8 (asserting that a prohibition on the *mere collection* of this data would undermine the very functioning of the Internet).

purposes of either online profiling or delivering behavioral advertising to that child.[84] For example, an advertising network or analytics service that tracks a child user across a set of websites or online services, but stores this information in a separate database rather than with the persistent identifier, would be deemed to have collected personal information from the child under this proposed paragraph.

Several commenters stated that industry self-regulatory efforts more effectively address the treatment of online behavioral advertising to children than would regulation in this area. For example, citing the industry's 2009 *Self-Regulatory Principles for Online Behavioral Advertising*, the Direct Marketing Association asserted that "robust self-regulation is the best and most appropriate way to address privacy concerns in connection with online behavioral advertising, including concerns related to children."[85]

The Commission finds this argument unpersuasive. Although self-regulation can play an important role in consumer protection, Congress specifically directed the Commission to promulgate and implement regulations covering the online collection, use, and disclosure of children's personal information. To the extent that children's personal information is collected in connection with behavioral advertising, such information should be protected under the Rule.

---

[84] "Online behavioral advertising" is the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests. *See* Self-Regulatory Principles for Online Behavioral Advertising, *supra* note 68, at *i*.

[85] DMA (comment 17), at 7 (directing the Commission's attention to *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), at 16-17, *available at* **http://www.the-dma.org/government/ven-principles%2007-01-09%20FINAL.pdf**. *See also* Entertainment Software Association (comment 20), at 19; Facebook (comment 22), at 7; IAB (comment 34), at 3; Microsoft (comment 39), at 9-10; Mobile Marketing Association (comment 40), at 3; Toy Industry Association (comment 63), at 9.

While self-regulatory programs can be valuable in promoting compliance, the proposed revision implements the COPPA statute and is enforceable by law.[86]

d. Photographs, videos, and audio files (new paragraph (i))

The Rule's existing definition of "personal information" includes photographs only when they are combined with "other information such that the combination permits physical or online contacting." Given the prevalence and popularity of posting photos, videos, and audio files online, the Commission has reevaluated the privacy and safety implications of such practices as they pertain to children. Inherently, photos can be very personal in nature. Also, photographs of children, in and of themselves, may contain information, such as embedded geolocation data,

---

[86] Although it is unclear from the record before the Commission whether operators currently are directing online behavioral advertising to children (various members of industry have informed Commission staff that they do not believe such activity is occurring while media reports have indicated the widespread presence of tracking tools on children's websites, *see* Steven Stecklow, *On the Web, Children Face Intensive Tracking,* Wall St. J., Sept. 17, 2010), the Commission notes that the self-regulatory guidelines cited by the commenters do not expressly require prior parental consent for such advertising to occur. Rather, operators who adhere to such guidelines are merely cautioned that they should comply with COPPA when engaging in online behavioral advertising. *See Self-Regulatory Principles for Online Behavioral Advertising, supra* note 85, at 16-17 ("Entities should not collect "personal information", as defined in the Children's Online Privacy Protection Act ('COPPA'), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA"). Moreover, the self-regulatory standards cited by commenters do not collectively represent all operators subject to COPPA.

that permits physical or online contact.[87] In addition, facial recognition technology can be used to further identify persons depicted in photos.[88]

The Commission believes that, with respect to the subset of websites and online services directed to children or having actual knowledge of collecting personal information from children, broader Rule coverage of photos is warranted.[89] In addition, the Commission believes that the Rule's definition of "personal information" should be expanded to include the posting of video and audio files containing a child's image or voice, which, similarly to photos, may enable the identification and contacting of a child. Therefore, the Commission proposes to create a new paragraph (i) of the definition of "personal information" that states:

---

[87] In addition to the personal information that may be viewable in a photograph or video, geolocation data is commonly embedded as hidden "metadata" within these digital images. These data usually consist of latitude and longitude coordinates, and may also include altitude, bearing, distance, and place names. Such geolocation information may be used by operators and may also be accessed by the viewing public. The Commission proposes to specifically enumerate "geolocation information" as a separate category of "personal information" under the Rule. *See infra* Part V.A.(4)(e).

[88] *See* M. Geuss, "Facebook Facial Recognition Could Get Creepy: new facial recognition technology used to identify your friends in photos could have some interesting applications – and some scary possibilities," PC World (Apr. 26, 2011), *available at* **http://www.pcworld.com/article/226228/facebook_facial_recognition_its_quiet_rise_and_dangerous_future.html** (discussing Facebook's facial recognition technology, and similar technologies offered by services such as Viewdle, Fotobounce, Picasa, iPhoto, and Face.com).

[89] Although the Commission received little comment on this topic, one individual commenter, as well as the Commission-approved COPPA safe harbor, TRUSTe, strongly supported this approach. *See* Gregory Schiller (comment 47); Office of the State Attorney – 15th Judicial Circuit in and for Palm Beach County, Florida (comment 47); TRUSTe (comment 64), at 4; Maureen Cooney, Chief Privacy Officer, TRUSTe, Remarks from *COPPA's Definition of "Personal Information"* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 191-92 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**.

(i) A photograph, video, or audio file where such file contains a child's image or voice;

This proposed change will ensure that parents are given notice and the opportunity to decide whether the posting of images or audio files is an activity in which they wish their children to engage.

e. Geolocation information (new paragraph (j))

In recent years, geolocation services have become ubiquitous features of the personal electronics market.[90] Numerous commenters raised with the Commission the issue of the potential risks associated with operators' collection of geolocation information from children. Some commenters urged the Commission to expressly modify the Rule to include geolocation information, given the current pervasiveness of such technologies and their popularity among children.[91] Others maintained that geolocation information is already covered by existing paragraph (b) of the Rule's definition of "personal information," which includes "a home or other physical address including street name and name of a city or town."[92]

---

[90] For example, geolocation-based navigation tools help users reach destinations, find local businesses or events, find friends and engage in social networking, "check in" at certain locations, and link their location to other activities. Many users access geolocation services through mobile devices. However, devices such as laptop and desktop computers, tablets, and in-car navigation and assistance systems also may be used to access such services. Geolocation information may be used once for a single purpose, or it may be stored or combined with other information to produce a history of a user's activities or a detailed profile for advertising or other purposes. *See* ACLU, "Location Based Services: Time For a Privacy Check-In" 1, 3 (Nov. 2010) *available at* **http://dotrights.org/sites/default/files/lbs-white-paper.pdf**.

[91] *See*, *e.g.,* EPIC (comment 19), at 8.

[92] *See* Institute for Public Representation (comment 33), at 26; TRUSTe (comment 64), at 4. *See also* Jules Polonetsky, Director, Future of Privacy Forum; Paul Ohm, Professor, (continued...)

Technologies that collect geolocation information can take a variety of forms and can communicate location with varying levels of precision. Generally speaking, most commonly used location tracking technologies are capable of revealing a person's location at least down to the level of a street name and the name of a city or town.[93] In the Commission's view, any geolocation information that provides precise enough information to identify the name of a street and city or town is covered already under existing paragraph (b) of the definition of "personal information." However, because geolocation information may be presented in a variety of formats (*e.g.*, coordinates or a map), and in some instances may be more precise than street name and name of city or town, the Commission proposes making geolocation information a stand-alone category within that definition.

Those commenters who opposed the inclusion of geolocation information within COPPA's definition of "personal information" argued that such information cannot be used to identify a specific individual, but only a device.[94] However, as discussed above, the Commission finds this argument unpersuasive.[95] Physical address, including street name and name of city or town, alone is considered personal information under COPPA. Accordingly, geolocation data

---

[92](...continued)
Univ. of Colorado Law School; Sheila A. Millar, Partner, Keller & Heckman LLP; Matt Galligan, Founder and CEO, SimpleGeo; Heidi C. Salow, Of Counsel, DLA Piper, Remarks from *COPPA's Definition of "Personal Information"* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 195, 205-07 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**.

[93] *See* ACLU, *supra* note 90, at 9.

[94] *See* DMA (comment 17), at 7-8; MPAA (comment 42), at 6-7; Net Choice (comment 45), at 6.

[95] *See supra* Part V.A.(6)(c).

that provides information at least equivalent to "physical address" should be covered as personal information.

f. Date of Birth, Gender, and ZIP Code

Several commenters recommended that the Commission include date of birth, gender, or ZIP code in the definition of "personal information."[96] The Commission gave careful thought to these recommendations, but is not proposing to include these items within the definition because the Commission does not believe that any one of these items of information, alone, permits the physical or online contacting of a specific individual. However, the Commission seeks input as to whether the *combination* of date of birth, gender, and ZIP code provides sufficient information to permit the contacting of a specific individual such that this combination of information should be included in the Rule as "personal information."[97] Moreover, there is a question whether an operator's collection of "ZIP+4" may, in some cases, be the equivalent of a physical address. A ZIP+4 Code consists of the original 5-digit ZIP Code plus a 4-digit add-on code that identifies a geographic segment within the 5-digit delivery area, such as a city block, office building, individual high-volume receiver of mail, or any other unit that would aid

---

[96] *See* EPIC (comment 19), at 8-9; Institute for Public Representation (comment 33), at 33.

[97] *See infra* Part X. at Question 9(b). Commenter Paul Ohm cites to several studies finding that a significant percentage of individuals can be uniquely identified by the combination of these three pieces of information. *See* Paul Ohm (comment 48), at 3, note 7.

efficient mail sorting and delivery.[98] The Commission seeks input on whether ZIP+4 is the equivalent of a physical address and whether it should be added to the Rule.[99]

g. Other Collections of Information

Taking a different view of "personal information," one commenter argued that the Commission should move away from identifying new particular individual items of personal information, and instead add to the definition "any collection of more than twenty-five distinct categories of information about a user."[100] This proposed definition is based on the premise that above a certain quantity threshold, the information an operator holds about a particular user becomes sufficiently identifying so as to be "personal." The Commission recognizes the potential for collections of diverse bits of information to permit the identification of a specific individual; however, the record is not sufficiently developed at this time to support a quantity-based approach to defining personal information. Without greater specificity, a quantity-based approach would not provide operators with sufficient certainty to determine which collections and combinations of information trigger the Rule's requirements and which do not. As a result, this standard would be difficult for operators to implement, as well as for the government to enforce.[101] The Commission believes that setting bright-line categories of personal information,

---

[98] *See* United States Postal Service, Frequently Asked Questions, ZIP Code Information, **http://faq.usps.com/eCustomer/iq/usps/** (search "ZIP Code Information"; then follow "ZIP Code Information" hyperlink) (last visited September 12, 2011).

[99] *See infra* Part X. at Question 9(c).

[100] *See* Paul Ohm (comment 48), at 2.

[101] Professor Ohm acknowledges that "most websites probably do not count their data in this way today, so the regulation will require some websites to expend modest new

(continued...)

while potentially both over- and under-inclusive, provides greater certainty for operators seeking to follow the Rule.

(7) *Website or online service directed to children*

The Commission also considered whether any changes needed to be made to the Rule's definition of "website or online service directed to children." The current definition is largely a "totality of the circumstances" test that provides sufficient coverage and clarity to enable websites to comply with COPPA, and the Commission and its state partners to enforce COPPA.[102] Few commenters addressed the definition. However, one commenter, the Institute for Public Representation, suggested that the Rule be amended so that a website *per se* should be deemed "directed to children" if audience demographics show that 20% or more of its visitors are children under age 13.[103]

The current definition of "website or online service directed to children" already notes that the Commission will consider competent and reliable empirical evidence of audience composition as part of a totality of circumstances analysis. The Commission's experience with

---

[101](...continued)
resources to comply. Moreover, every time a website decides to collect new categories of information from users, it needs to recalculate its count." *Id.* at 8-9.

[102] *See, e.g.*, *United States v. Playdom, Inc.*, No. SA CV-11-00724 (C.D.Ca., filed May 11, 2011) (finding defendants' Pony Stars website to be "directed to children"); *United States v. Industrious Kid, Inc.*, No. CV-08-0639 (N.D. Cal., filed Jan. 28, 2008); *United States v. UMG Recordings, Inc.*, No. CV-04-1050 (C.D. Cal., filed Feb. 17, 2004); *United States v. Bonzi Software, Inc.*, No. CV-04-1048 (C.D. Cal., filed Feb. 17, 2004).

[103] *See* Institute for Public Representation (comment 33), at iii (urging the Commission to adopt the same threshold, 20%, used in the Commission's 2007 food marketing Orders to File a Special Report).

online audience demographic data in both its studies of food marketing to children and marketing violent entertainment to children shows that such data is neither available for all websites and online services, nor is it sufficiently reliable, to adopt it as a *per se* legal standard.[104] Accordingly, the Commission declines to adopt a standard akin to the 20% standard proposed by the Institute for Public Representation.

However, the Commission proposes minor modifications to the definition, as follows. First, as part of the totality of the circumstances analysis, the Commission proposes modifying the term "audio content" to include musical content. In addition, the Commission proposes adding the presence of child celebrities, and celebrities who appeal to children, within the non-exclusive set of indicia it will use to determine whether a website or online service is directed to children. In the Commission's experience, both music and the presence of celebrities are strong indicators of a website or online service's appeal to children. Finally, the Commission proposes reordering the language of the definition so that the terms "animated characters" and "child-oriented activities and incentives" are addressed alongside the other indicia of child-directed content.

Therefore, the proposed definition of "website or online service directed to children" reads:

---

[104] In the context of the Commission's food marketing studies, food marketers were required to identify and report website expenditures targeted to children based on a number of criteria, one of which was whether audience demographic data indicated that 20% or more of visitors to a website were children ages 2-11. *See* Fed. Trade Comm'n, Order to File Special Report, B-3, note 14 (July 31, 2007) *available at* **http://www.ftc.gov/os/6b_orders/foodmktg6b/070731boskovichfarmssixb.pdf**. There, the 20% threshold was not used as a basis to impose legal liability for a Rule violation.

> *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 content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, 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, and evidence regarding the intended audience.

B. Notice (16 CFR 312.4)

The linchpins of the COPPA Rule are its parental notice and consent requirements. Providing parents with clear and complete notice of operators' information practices is the necessary first step in obtaining informed consent from parents. COPPA requires that parents be notified in two ways: on the operator's website or online service (the "online notice," which typically takes the form of a privacy policy), and in a notice delivered directly to a parent whose child seeks to register on the site or service (the "direct notice"). The current Rule requires that operators provide extensive information about their children's privacy practices in their online notice. While the Rule states that the direct notice must contain the information an operator includes in its online notice as well as certain additional information, in the past, the Commission has indicated that operators may truncate the information in the direct notice by providing a hyperlink to their online privacy policy.[105]

---

[105] *See* 1999 Statement of Basis and Purpose, 64 FR 59888, 59897.

Outside the COPPA context, in recent years, the Commission has begun to urge industry to provide consumers with notice and choice about information practices at the point consumers enter personal data or before accepting a product or service.[106] The analogous point of entry under COPPA would be the direct notice, which has the potential to provide parents with the best opportunity to consider an operator's information practices and to determine whether to permit children's engagement with such operator's website or online service. Therefore, the Commission proposes to revise the notice requirements to reinforce COPPA's goal of providing complete and clear information in the direct notice, and to rely less heavily on the online notice or privacy policy as a means of providing parents with information about operators' information practices.[107]

(1) ***Notice on the website or online service (revised paragraph (b))***

The Commission proposes to streamline § 312.4(b),[108] regarding the placement and content of the notice of information practices that operators must provide on their websites or in their online services. The language regarding the required placement of this online notice has been shortened and clarified, thereby making the provision more instructive to operators. The revised language more succinctly requires that the online notice be clearly labeled and

---

[106] *See* Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 23, at 57-59.

[107] The proposed changes to the direct notice provision, discussed in Part V.B.(2) *infra*, would reverse the Commission's guidance that operators may truncate the information in the direct notice by providing a hyperlink to their online privacy policy. *See* note 105 and accompanying text.

[108] No changes are proposed to § 312.4(a) ("general principles of notice").

prominently located, and be posted on an operator's home page or home screen and at each location where the operator collects personal information from children.[109]

With respect to the content of the online notice, the Commission proposes several improvements to the Rule's current list of requirements. First, the Commission proposes requiring operators to provide contact information, including, at a minimum, the operator's name, physical address, telephone number, and email address. In contrast to the current Rule, this proposal would apply to *all* operators of a website or online service, rather than permitting the designation of a single operator as the contact point. Given the possibility of a child interacting with multiple operators on a single website or online service (*e.g.*, in the case of a mobile application that grants permission to an advertising network to collect user information from within the application), the Commission believes that the identification of each operator will aid parents in finding the appropriate party to whom to direct any inquiry.

Second, the Commission proposes eliminating the Rule's current lengthy – yet potentially under-inclusive – recitation of an operator's information collection, use, and disclosure practices in favor of a simple statement of: (1) what information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available, (2) how the operator uses such information, and (3) the operator's disclosure practices for such information.[110] In the Commission's experience, privacy policies are often long

---

[109] The Commission poses a question whether the Rule should be modified to require operators to post a link to their online notice in any location where their mobile applications can be purchased or otherwise downloaded. *See infra* Part X. at Question 14.

[110] This language mirrors the statutory requirements for the online notice. *See* 15 (continued...)

and difficult to understand, and may no longer be the most effective way to communicate salient information to consumers, including parents.[111] By streamlining the Rule's online notice requirements by reverting to the language of the COPPA statute, the Commission hopes to encourage operators to provide clear, concise descriptions of their information practices, which may have the added benefit of being easier to read on smaller screens (*e.g.,* those on Internet-enabled mobile devices).

The Commission also proposes eliminating the requirement, articulated in § 312.4(b)(2)(v), that an operator's privacy policy state that the operator may not condition a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity. In the Commission's experience, this blanket statement, often parroted verbatim in operators' privacy policies, detracts from the key information of operators' actual information practices, and yields little value to a parent trying to determine whether to permit a child's participation. In proposing to delete this requirement in the privacy notice, however, the Commission does not propose deleting § 312.7 of the Rule, which still prohibits 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.[112]

---

[110](...continued)
U.S.C. 6503(b)(1)(A)(i).

[111] *See* Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 23, at 7.

[112] *See* 16 CFR 312.7.

Therefore, the Commission proposes to revise paragraph (b) of § 312.4 so that it states:

> (b) *Notice on the website or online service.* Pursuant to § 312.3(a), each operator of a website or online service directed to children must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its website or online service, *and,* at each area of the website or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. 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 or landing page or screen of the children's area. To be complete, the online notice of the website or online service's information practices must state the following:
>
> (1) Each operator's contact information, which at a minimum, must include the operator's name, physical address, telephone number, and email address;
>
> (2) A description of what information each operator collects from children, including whether the website or online service enables a child to make personal information publicly available; how such operator uses such information, and; the operator's disclosure practices for such information; and,
>
> (3) 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.[113]

---

[113] No change is proposed to the Rule's requirement that operators disclose that a parent may review and have deleted a child's personal information and refuse to permit further collection or use of that child's information. Although one commenter observed that parents seldom exercise these rights, *see* WiredSafety.org (comment 68), at 28, the Commission believes that requiring operators to provide such rights to parents remains an important element of the Rule. In the context of its broader inquiry into how to best protect privacy in today's marketplace, Commission staff is exploring methods of ensuring consumer access to data as a means of increasing the transparency of companies' data practices. *See* Protecting Consumer

(continued...)

(2) ***Direct notice to a parent (revised paragraph (c))***

As described above, the Commission proposes refining the Rule requirements for the direct notice to ensure that this notice works as an effective "just-in-time" message to parents about an operator's information practices. Specifically, the Commission proposes to reorganize and standardize the direct notice requirement to set forth the precise items of information that must be disclosed in each type of direct notice required under the Rule. These specific notice requirements correspond to the requirements for obtaining parental consent under § 312.5 of the Rule. The proposed reorganization is intended to make it easier for operators to determine what information they must include in the direct notice to parents, based upon operators' particular information collection practices.

The proposed revised language of § 312.4(c) specifies, for each different form of direct notice required by the Rule, the precise information that operators must provide to parents regarding: the items of personal information the operator already has obtained from the child (the parent's online contact information either alone or together with the child's online contact information); the purpose of the notification; action that the parent must or may take; and, what use, if any, the operator will make of the personal information collected. The proposed revised provision also makes clear that each form of direct notice must provide a hyperlink to the operator's online notice of information practices. The Commission believes the proposed revisions will help ensure that parents receive key information up front, while directing them online to view any additional information contained in the operator's online notice.

---

[113](...continued)
Privacy in an Era of Rapid Change, *supra* note 23, at 72-76.

The Commission also proposes adding a new paragraph, § 312.4(c)(2), setting out the requirements for a direct notice when an operator chooses to collect a parent's online contact information from the child in order to provide parental notice about a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. This new form of parental notice corresponds to a newly proposed exception to the parental consent requirement for the collection of a parent's online contact information when done to inform the parent of a child's participation in a website or online service that does not otherwise collect personal information from the child.[114]

Therefore, the Commission proposes to revise paragraph (c) of § 312.4 so that it reads:

> (c) *Direct notice to a parent*. An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of the child's personal information, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.
>
> (1) *Content of the direct notice to the parent required under § 312.5(c)(1) (Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information).* This direct notice shall set forth:
>
> (i) That the operator has collected the parent's online contact information from the child in order to obtain the parent's consent;
>
> (ii) That the parent's consent is required for the child's participation in the website or online service, and that the operator will not collect, use, or disclose any personal

---

[114] *See infra* Part V.C.(4).

information from the child if the parent does not provide such consent;

(iii) The additional items of personal information the operator intends to collect from the child, if any, and the potential opportunities for the disclosure of personal information, if any, should the parent consent to the child's participation in the website or online service;

(iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(b);

(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and,

(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

(2) *Content of the direct notice to the parent allowed under § 312.5(c)(2) (Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information).* This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to the parent of a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information; and,

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the operator to allow the child to participate in the website or online service and may

require the deletion of the parent's online contact information, and how the parent can do so; and,

(iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

(3) *Content of the direct notice to the parent required under § 312.5(c)(4) (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times)*. This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

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

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and,

(vi) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

(4) *Content of the direct notice to the parent required under § 312.5(c)(5) (Notice to a Parent In Order to Protect a Child's Safety)*. This direct notice shall set forth:

(i) That the operator has collected the child's name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

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

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and,

(v) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

C. Parental Consent (16 CFR 312.5)

A central element of COPPA is its requirement that operators seeking to collect, use, or disclose personal information from children first obtain verifiable parental consent.[115] "Verifiable

---

[115] Paragraph (a) of § 312.5 reads:

(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.

parental consent" is defined in the statute as "any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure, described in the notice."[116] In paragraph (b)(1), the Rule provides that operators:

> 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.

The Rule then sets forth a non-exclusive list of methods that meet the standard of verifiable parental consent.[117] Specifically, paragraph (b)(2) states:

> 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.[118]

---

116 15 U.S.C. 6501(9).

117 *See* 16 CFR 312.5(b).

118 Paragraph (b)(2) continues:

> *Provided that:* Until the Commission otherwise determines, 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

(continued...)

The Rule's enumerated consent mechanisms were discussed in-depth at the Commission's June 2, 2010 COPPA roundtable and also were addressed by a number of commenters.[119] While several persons acknowledged that no one method provides complete certainty that the operator has reached and obtained consent from a parent, they generally agreed that the listed methods continue to have utility for operators and should be retained.[120] A great number of commenters also urged the Commission to expand the list of acceptable mechanisms to incorporate newer technologies.[121] After careful consideration, the Commission proposes several significant changes to the mechanisms of verifiable parental consent set forth in paragraph (b) of § 312.5, including: adding several newly recognized mechanisms for parental consent; eliminating the sliding scale approach to parental consent; and, adding two new processes for evaluation and pre-clearance of parental consent mechanisms.

---

[118](...continued)
methods must provide notice that the parent can revoke any consent given in response to the earlier e-mail.

A discussion of paragraph (b)(2) follows in Part V.C.(2).

[119] *See* Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 195, 208-71 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**.

[120] *See* DMA (comment 17), at 10, 12; Microsoft (comment 39), at 7; Toy Industry Association, Inc. (comment 63), at 3; WiredSafety.org. (comment 68), at 18;

[121] *See, e.g.*, Boku (comment 5); DMA (comment 17), at 11-12; EchoSign, Inc. (comment 18); Entertainment Software Association (comment 20), at 7-9; Facebook (comment 22), at 2); Janine Hiller (comment 27), at 447-50; Mary Kay Hoal (comment 30); Microsoft (comment 39), at 4; MPAA (comment 42), at 12; RelyID (comment 53), at 3; TRUSTe (comment 64), at 3; Harry Valetk (comment 66), at 6; WiredSafety.org (comment 68), at 53; Susan Wittlief (comment 69).

(1) *Mechanisms for Verifiable Parental Consent (paragraph (b)(2))*

A number of commenters made suggestions for strengthening, modernizing, and simplifying the Rule's mechanisms for parental consent. For example, commenters asked the Commission to recognize additional methods of obtaining parental consent, such as by sending a text message to the parent's mobile phone number,[122] offering online payment services other than credit cards,[123] offering parental controls in gaming consoles,[124] offering a centralized parents' opt-in list,[125] and permitting electronic signatures.[126] Upon consideration of each proposal in light of the existing record, the Commission determines that the record is sufficient to justify certain proposed mechanisms, but insufficient to adopt others.

First, the Commission notes that the collection of a parent's mobile phone number to effectuate consent via an SMS text message would require a statutory change, as the COPPA statute currently permits only the collection of a parent's "online contact" information for such purposes, and a phone number does not fall within the statute's definition of "online contact information," *i.e.*, "an e-mail address or another substantially similar identifier that permits

---

[122] *See* BOKU (comment 5); Entertainment Software Association (comment 20), at 11-12; TRUSTe (comment 64), at 3; Harry A. Valetk (comment 66), at 6-7. *See* discussion *supra* Part IV. regarding COPPA's application to mobile communications via SMS messaging.

[123] *See* WiredSafety.org (comment 68), at 24 (noting that operators are considering employing online financial accounts such as iTunes for parental consent).

[124] *See* Entertainment Software Association (comment 20), at 9-10; Microsoft (comment 39), at 7.

[125] *See* Entertainment Software Association (comment 20), at 12; Janine Hiller (comment at 27), at 31.

[126] *See* DMA (comment 17), at 12; EchoSign (comment 18); Entertainment Software Association (comment 20), at 10; Toy Industry Association (comment 63), at 11.

direct contact with a person online."[127] There are advantages to using SMS texting as a method of contacting the parent and obtaining consent – among them that parents typically do not have multiple mobile phone numbers, and generally have their mobile phones with them at all times. Some commenters opined that this method was as reliable as use of a credit card or fax;[128] others compared the use of SMS text messaging to the "email plus" method permitted under the Rule's sliding scale approach to parental consent.[129] The Commission believes the more apt analogy is to the email plus method in that the operator sends a notice to the parent via the parent's mobile phone number and requests opt-in consent by a return message in some form. In this way, the use of SMS text messaging for parental consent would suffer from the same inadequacies as does email plus, which, as described below, the Commission proposes to eliminate. Just as with an email address, there is no way to verify that the phone number provided by a child is that of the parent rather than that of the child. For these reasons, the Commission declines to add use of SMS text messaging to the enumerated list of parental consent mechanisms.

With respect to expanding the Rule to permit the use of online payment services for verifying consent in lieu of a credit card, the Commission finds that the record is insufficient to warrant adding online payment services as a consent mechanism. The Commission notes that no commenters provided any analysis of how online payment services might meet the requirements of § 312.5(b)(1); however, one commenter cautioned the Commission against embracing such technologies at this time, noting that alternative payment systems may not be as well-regulated

---

127 15 U.S.C. 6502(12).

128 *See, e.g.*, Entertainment Software Association (comment 20), at 11-12.

129 *See* Boku (comment 5).

as the credit card industry and thereby may provide even less assurance of parental consent than use of a credit card.[130] The Commission also is mindful of the potential for children's easy access to and use of alternative forms of payments (such as gift cards, debit cards, and online accounts), and would expect to see a fuller discussion of the risks presented in any future application to the Commission for recognition of these consent methods.

Several commenters asked the Commission to consider whether, and in what circumstances, parental control features in game consoles could be used to verify consent under COPPA.[131] Parental control settings often permit parents to limit or block functions such as Internet access, information sharing, chat, and interactive game play, and require parental approval before a child adds friends.[132] Parental control features appear to offer parents a great deal of control over a child's gaming experience, and, as commenters acknowledged, can serve as a *complement* to COPPA's parental consent requirements.[133] As acknowledged in the comments, at present, such systems are not designed to comply with COPPA's standards for verifiable parental consent,[134] and the record currently is insufficient for the Commission to

---

[130] *See* EPIC (comment 19), at 5. ("Alternative methods may not be as heavily regulated as more traditional systems. As a result, the use of alternative methods in gaining parental consent or payment remain inadvisable, although that may change as such methods come under stronger regulation.").

[131] *See* Entertainment Software Association (comment 20), at 4; Microsoft (comment 39), at 7.

[132] *See* Entertainment Software Association (comment 20), at 4-6.

[133] *Id.* at 6.

[134] *See id.* at 9 ("Therefore, it makes sense to consider how these tools could be harnessed for the related task of acquiring verifiable parental consent under the COPPA Rule"); Microsoft (comment 39), at 7 (describing how a hypothetical parental controls method might be (continued...)

determine whether a hypothetical parental consent mechanism would meet COPPA's verifiable parental consent standard. The Commission encourages continued exploration of the concept of using parental controls in gaming consoles (and, presumably, on a host of handheld devices) to notify parents and obtain their prior verifiable consent.

Several commenters also asked the Commission to accept electronic signatures as a form of verifiable consent.[135] The term "electronic signature" has many meanings, and can range from "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record,"[136] to an electronic image of the stylized script associated with a person. Although the law recognizes electronic signatures for the assertion that a document has been signed,[137] electronic signatures do not necessarily confirm the underlying identity of the individual signing the document. Therefore, their use, without more indicia of reliability, is problematic in the context of COPPA's verifiable parental consent requirement.

The Entertainment Software Association proposed that the Commission incorporate a "sign and send" method, given that Internet-enabled mobile devices increasingly include technologies that allow a user to input data by touching or writing on the device's screen. The

---

[134](...continued)
structured in the future to notify a parent and obtain parental consent).

[135] *See* DMA (comment 17), at 12; EchoSign (comment 18); Entertainment Software Association (comment 20), at 10; Toy Industry Association (comment 63), at 11.

[136] *See* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7006(5).

[137] 15 U.S.C. 7001(a).

Commission agrees that such sign-and-send methods are substantially analogous to the print-and-send method already recognized by § 312.5(b)(2) of the Rule.[138] However, because of the proliferation of mobile devices among children and the ease with which children could sign and return an on-screen consent, the Commission is concerned that such mechanisms may not "ensure that the person providing consent is the child's parent."[139] The Commission welcomes further comment on how to enhance the reliability of these convenient methods.

Several commenters urged the Commission to recognize the submission of electronically scanned versions of signed parental consent forms and the use of video verification methods.[140] The Commission agrees that now commonly-available technologies such as electronic scans and video conferencing are functionally equivalent to the written and oral methods of parental consent originally recognized by the Commission in 1999. Therefore, the Commission proposes to recognize these two methods in the proposed Rule.

The Commission also proposes allowing operators to collect a form of government-issued identification – such as a driver's license, or a segment of the parent's social security number – from the parent, and to verify the parent's identity by checking this identification against databases of such information, provided that the parent's identification is deleted by the

---

138 *See* Entertainment Software Association (comment 20), at 10.

139 16 CFR 312.5(b)(1).

140 *See* Denise Tayloe, *supra* note 42, at 227; Phyllis B. Spaeth, Assoc. Dir., Children's Adver. Review Unit, Council of Better Bus. Bureaus, Remarks from *The "Actual Knowledge" Standard in Today's Online Environment* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 269 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**; DMA (comment 17), at 11; EPIC (comment 19), at 3.

operator from its records promptly after such verification is complete. The Commission recognizes that information such as social security number, driver's license number, or other record of government-issued identification are sensitive data.[141] In permitting operators to use government-issued identification as an approved method of parental verification, the Commission emphasizes the importance of limiting the collection of such identification information to only those segments of information needed to verify the data.[142] For example, the Commission notes that the last four digits of a person's social security number are commonly used by verification services to confirm a person's identity.[143] The requirement in the proposed Rule that operators immediately delete parents' government-issued identification information upon completion of the verification process provides further protection against operators' unnecessary retention of the information, use of the information for other purposes, and potential compromise of such information.[144]

---

[141] The COPPA statute itself lists social security number among the items considered to be personal information. *See* 16 CFR 312.2. In other contexts, driver's licenses and social security numbers, among other things, have traditionally been considered by Commission staff to be personal, or sensitive, as well. *See* Self-Regulatory Principles for Online Behavioral Advertising, *supra* note 68, at 20, 42, 44.

[142] The use of a driver's license to verify a parent, while not specifically enumerated in the Final Rule as an approved method of parental consent, was addressed in the Statement of Basis and Purpose in connection with a discussion of the methods to verify the identity of parents who seek access to their children's personal information under § 312.6(a)(3) of the Rule. *See* 1999 Statement of Basis and Purpose, 64 FR 59888, 59905. There, the Commission concluded that the use of a driver's license was an acceptable method of parental verification.

[143] *See, e.g.*, Privo, Inc., "Request for Safe Harbor Approval by the Federal Trade Commission for Privo, Inc.'s Privacy Assurance Program under Section 312.10 of the Children's Online Privacy Protection Rule," 25 (Mar. 3, 2004), *available at* **http://www.ftc.gov/os/2004/04/privoapp.pdf**.

[144] The Commission poses a question whether operators should be required to maintain a record that parental consent was obtained. *See infra* Part X., at Question 17.

Finally, the Commission proposes including the term "monetary" to modify "transaction" in connection with use of a credit card to verify parental consent. This added language is intended to make clear the Commission's long-standing position that the Rule limits use of a credit card as a method of parental consent to situations involving actual monetary transactions.[145]

(2) ***The Sliding Scale Approach to Parental Consent***

In conducting the Rule review, the Commission sought comment on whether the sliding scale set forth in § 312.5(b)(2) remains a viable approach to verifiable parental consent.[146] Under the sliding scale, an operator, when collecting personal information only for its *internal* use, may obtain verifiable parental consent through an email from the parent, so long as the email is coupled with an additional step. Such additional steps have included: obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call, or sending a delayed confirmatory email to the parent after receiving consent. The purpose of the additional step is to provide greater assurance that the person providing consent is, in fact, the parent.[147] This consent method is often called "email plus." In contrast, for uses of personal

---

[145] *See* Children's Online Privacy Protection Rule, 71 FR 13247, 13253, 13254 (Mar. 15, 2006) (retention of rule without modification) (requirement that the credit card be used in connection with a transaction provides extra reliability because parents obtain a transaction record, which is notice of the purported consent, and can withdraw consent if improperly given); Fed. Trade Comm'n., Frequently Asked Questions about the Children's Online Privacy Protection Rule, Question 33, *available at* **http://www.ftc.gov/privacy/coppafaqs.shtm#consent**.

[146] *See* 2010 Rule Review, *supra* note 7, at 17091.

[147] The Commission was persuaded by commenters' views that internal uses of information, such as marketing to children, presented less risk than external disclosures of the (continued...)

information that involve disclosing the information to the public or third parties, the sliding scale approach requires operators to use more reliable methods of obtaining verifiable parental consent. These methods have included: using a print-and-send form that can be faxed or mailed back to the operator; 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 email accompanied by a PIN or password obtained through one of the above methods.

In adopting the sliding scale approach in 1999, the Commission recognized that the email plus method was not as reliable as the other enumerated methods of verifiable parental consent.[148] However, it believed that this lower cost option was acceptable as a temporary option, in place only until the Commission determined that more reliable (and affordable) consent methods had adequately developed.[149] In 2006, the Commission extended use of the sliding scale indefinitely, stating that the agency would continue to monitor technological

---

[147](...continued)
information to third parties or through public postings. *See* 1999 Statement of Basis and Purpose, 64 FR 59888, 59901. Other internal uses of children's personal information may include sweepstakes, prize promotions, child-directed fan clubs, birthday clubs, and the provision of coupons.

[148] *See id.* at 59,902 ("[E]mail alone does not satisfy the COPPA because it is easily subject to circumvention by children.").

[149] *See id.* at 59,901 ("The Commission believes it is 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").

developments and modify the Rule should an acceptable electronic consent technology develop.[150]

Email plus has enjoyed wide appeal among operators, who credit its simplicity.[151] Numerous commenters, including associations who represent operators, support the continued retention of this method as a low-cost means to obtain parents' consent.[152] At the same time, several commenters, including safe harbor programs and proponents of new parental consent mechanisms, challenged the method's reliability, given that operators have no real way of determining whether the email address provided by a child is that of the parent, and there is no requirement that the parent's email response to the operator contain any additional information providing assurance that it is from a parent.[153]

---

[150] *See* Children's Online Privacy Protection Rule, 71 FR 13247, 13255, 13254 (Mar. 15, 2006) (retention of rule without modification).

[151] *See* WiredSafety.org (comment 68), at 21 ("We all assumed [email plus] would be phased out once digital signatures became broadly used. But when new authentication models and technologies failed to gain in parental adoption, it was continued and is in broad use for one reason – it's simple").

[152] *See* Rebecca Newton, Chief Cmty. & Safety Officer, Mind Candy, Inc., Remarks from *Emerging Parental Verification Access and Methods* Panel at the Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 211-13 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf** (email plus is as reliable as any other method); DMA (comment 17), at 10; IAB (comment 34), at 2; Rebecca Newton (comment 46), at 3; PMA (comment 51), at 4-5; Toy Industry Association, Inc. (comment 63), at 8.

[153] *See* Privo, Inc. (comment 50), at 5 ("the presentation of a verified email is much less reliable if there is virtually no proofing or analyzing that goes on to determine who the email belongs to"); RelyId (comment 53), at 3 ("The email plus mechanism does not obtain verifiable parental consent at all. It simply does not ensure that a parent 'authorizes' anything required by the COPPA statute. The main problem with this approach is that the child can create an email address to act as the supposed parent's email address, send the email from that address, and receive the confirmatory email at that address"). S*ee also* Denise Tayloe, *supra* note 42, at 215-

(continued...)

The Commission believes that the continued reliance on email plus has inhibited the development of more reliable methods of obtaining verifiable parental consent.[154] In fact, the Commission notes that few, if any, new methods for obtaining parental consent have emerged since the sliding scale was last extended in 2006. The Commission limited the use of email plus to instances where operators only collect children's personal information for internal uses. Although internal uses may pose a lower risk of misuse of children's personal information than the sharing or public disclosure of such information, all collections of children's information merit strong verifiable parental consent. Indeed, children's personal information is one of the most sensitive types of data collected by operators online. In light of this, therefore, the Commission believes that email plus has outlived its usefulness and should no longer be a recognized approach to parental consent under the Rule.

Therefore, the Commission proposes to amend § 312.5(b)(2) so that it reads:

> (2) Existing 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, facsimile, or an electronic scan; permitting a parent to use a credit card in connection with a monetary transaction; having a parent call a toll-free telephone number staffed by trained personnel; having a parent connect to trained personnel via video-conference; or, verifying a parent's identity by checking a form of government-issued identification against databases of such information, *provided that* the

---

[153](...continued)
17; Phyllis Spaeth, *supra* note 140, at 215-17 (email plus is very unreliable).

[154] *See* Privo (comment 50), at 4 ("[Extending the sliding scale mechanism] had the effect of giving industry absolutely no reason to create, innovate, adopt or make use of any other method for the for the internal use of children's personal data.")

parent's identification is deleted by the operator from its records promptly after such verification is complete.

However, as explained below, given the proposed discontinuance of email plus, and in the interest of spurring innovation in parental consent mechanisms, the Commission proposes a new process by which parties may voluntarily seek Commission approval of a particular consent mechanism, as explained below.

(3) ***Commission and Safe Harbor Approval of Parental Consent Mechanisms (new paragraphs (b)(3) and (b)(4))***

Under the Rule, methods 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."[155] This standard provides operators with the opportunity to craft consent mechanisms that meet this standard but otherwise are not enumerated in paragraph (b)(2) of § 312.5. Nevertheless, whether out of concern for potential liability, ease of implementation, or lack of technological developments, operators have been reluctant to utilize consent methods

[155] *See* 16 CFR 312.5(b)(1).

other than those specifically set forth in the Rule.[156] As a result, there appears to be little technical innovation in any area of parental consent.[157]

To encourage the development of new consent mechanisms, and to provide transparency regarding consent mechanisms that may be proposed, the Commission proposes to establish a process in the Rule through which parties may, on a voluntary basis, seek Commission approval of a particular consent mechanism. Applicants who seek such approval would be required to present a detailed description of the proposed parental consent mechanism, together with an analysis of how the mechanism meets the requirements of § 312.5(b)(1) of the Rule. The Commission would publish the application in the FEDERAL REGISTER for public comment, and approve or deny the applicant's request in writing within 180 days of the filing of the request.

The Commission believes that this new approval process, aided by public input, will allow the Commission to give careful consideration, on a case-by-case basis, to new forms of consent as they develop in the marketplace. The new process also will increase transparency by publicizing approvals or rejections of particular consent mechanisms and should encourage

---

[156] The June 2, 2010 Roundtable and the public comments reflect a tension between operators' desire for new methods of parental verification and their hesitation to adopt consent mechanisms other than those specifically enumerated in the Rule. *See* Remarks from Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 226-27 (June 2, 2010), *available at* **http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf**; CDT (comment 8), at 3 ("innovation in developing procedures to obtain parental consent has been limited as websites choose to use the methods suggested by the FTC out of fear that a more innovative method could lead to liability").

[157] *See* Children's Online Privacy Protection Rule, 71 FR 13247, 13250 (Mar. 15, 2006) (retention of rule without modification).

operators who may previously have been tentative about exploring technological advancements to come forward and share them with the Commission and the public.

Several commenters urged the Commission to permit Commission-approved safe harbor programs to serve as laboratories for developing new consent mechanisms.[158] The Commission agrees that establishing such a system may aid the pace of development in this area, and given the strengthened oversight of safe harbor programs described in Part F. below, will not result in the loosening of COPPA's standards for parental consent. Therefore, the Commission proposes adding a provision to the Rule stating that operators participating in a Commission-approved safe harbor program may use any parental consent mechanism deemed by the safe harbor program to meet the general consent standard set forth in § 312.5(b)(1).

Therefore, the Commission proposes to amend § 312.5(b) to add two new paragraphs, (3) and (4) that read:

> (3) *Commission approval of parental consent mechanisms.* Interested parties may file written requests for Commission approval of parental consent mechanisms not currently enumerated in paragraph (b)(2). To be considered for approval, parties must provide a detailed description of the proposed parental consent mechanism, together with an analysis of how the mechanism meets paragraph (b)(1). The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the request. The Commission shall issue a

---

[158] *See* MPAA (comment 42), at 12; Rebecca Newton (comment 46), at 2; Privo (comment 50), at 2; PMA (comment 51), at 5; Berin Szoka (comment 59), Szoka Responses to Questions for the Record, at 56; TRUSTe (comment 64), at 3). *See also generally* WiredSafety.org (comment 68), at 31-32.

written determination within 180 days of the filing of the request.

(4) *Safe harbor approval of parental consent mechanisms.* A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent mechanism not currently enumerated in paragraph (b)(2) where the safe harbor program determines that such parental consent mechanism meets the requirements of paragraph (b)(1).

(4) *Exceptions to Prior Parental Consent (paragraph (c))*

Congress anticipated that certain situations would arise in which it was not necessary or practical for an operator to obtain consent from parents prior to engaging with children online. Accordingly, the COPPA statute and Rule contain five scenarios in which an operator may collect limited pieces of personal information (*i.e.*, name and online contact information) from children prior to, or sometimes without, obtaining consent.[159] These exceptions permit operators to communicate with the child to: initiate the parental consent process, respond to the child once or multiple times, and protect the child's safety or the integrity of the website.[160]

The Commission proposes adding one new exception to parental consent in order to give operators the option to collect a parent's online contact information for the purpose of providing notice to or updating the parent about a child's participation in a website or online service that

---

[159] *See* 15 U.S.C. 6503(b)(2); 16 CFR 315.5(c).

[160] The Act and the Rule currently permit the collection of a parent's email address for the limited purposes of: (1) obtaining verified parental consent; (2) providing parents with a right to opt-out of an operator's use of a child's email address for multiple contacts of the child; and (3) to protect a child's safety on a website or online service. *See* 15 U.S.C. 6503(b)(2); 16 CFR 312.5(c)(1), (2), and (4).

does not otherwise collect, use, or disclose children's personal information.[161] The parent's online contact information may not be used for any other purpose, disclosed, or combined with any other information collected from the child. The Commission believes that collecting a parent's online contact information for the limited purpose of notifying the parent of a child's online activities in a site or service that does not otherwise collect personal information is reasonable and should be encouraged.[162]

Therefore, the Commission proposes to amend § 312.5(c) to add a new subsection, § 312.4(c)(2), that reads:

> Where the sole purpose of collecting a parent's online contact information is to provide notice to, and update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2).

The Commission also proposes minor technical corrections to the Rule's current exceptions provisions. First, in § 312.4(c)(1), the Rule permits an operator to collect "the name or online contact information of a parent or child" to be used for the sole purpose of obtaining parental consent. The clear intent of this provision is to allow for the collection of the *parent's*

---

[161] At least a few online virtual worlds directed to very young children already follow this practice. Because the Rule does not currently include such an exception, these operators technically are in violation of COPPA.

[162] This proposed new exception is mirrored in the proposed revisions to the direct notice requirement of § 312.4. *See supra* Part V.B.(2).

online contact information in order to reach the parent to initiate the consent process. Therefore, the Commission proposes to amend § 312.5(c)(1) to clarify the language so that it reads:

> Where the sole purpose of collecting a parent's online contact information and the name of the child or the parent is to provide notice and obtain parental consent under § 312.4(c)(1). 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.

Second, § 312.5(c)(3) provides that an operator may notify a parent of the collection of a child's online contact information for multiple contacts via email or postal address. The Commission proposes to eliminate the option of collecting a parent's postal address for notification purposes. The collection of postal address is not provided for anywhere else in the Rule's notice requirements, and is clearly outmoded at this time. Therefore, the Commission proposes to amend § 312.5(c)(3), now renumbered as § 312.5(4), so that it reads:

> Where the sole purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered.

Finally, in various places in § 312.5(c), the Commission proposes to emphasize that the collection of online contact information is to be used for the limited purpose articulated within each paragraph, and not for any other purpose.

Therefore, the Commission proposes to amend § 312.5(c) so that it reads in its entirety:

> (c) *Exceptions to prior parental consent.* Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child *except* as set forth in this paragraph:
>
> (1) Where the sole purpose of collecting a parent's online contact information and the name of the child or the parent is to provide notice and obtain parental consent under § 312.4(c)(1). 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 sole purpose of collecting a parent's online contact information is to provide notice to, and update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);
>
> (3) Where the sole purpose of collecting a child's online contact information is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;[163]
>
> (4) Where the sole purpose of collecting a child's and a parent's online contact information is to respond

---

[163] This "one time use" exception does not require an operator to provide notice to a parent.

directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the sole purpose of collecting a child's name, and a child's and a parent's online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the sole purpose of collecting a child's name and online contact information is to: (i) protect the security or integrity of its website or online service; (ii) take precautions against liability; (iii) 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; and, where such information is not be used for any other purpose.[164]

D. Confidentiality, Security, and Integrity of Personal Information Collected From Children (16 CFR 312.8)

The Commission proposes to amend § 312.8 to strengthen the provision for maintaining the confidentiality, security, and integrity of personal information. To accomplish this, the Commission proposes adding a requirement that operators take reasonable measures to ensure

---

[164] This exception does not require an operator to provide notice to a parent.

that any service provider or third party to whom they release children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information.

COPPA requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children, but is silent on the data security obligations of third parties.[165] The COPPA Rule mirrors the statutory language but also requires covered operators to disclose in their online privacy policies whether third parties to whom personal information is disclosed have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the operator.[166]

Under the Commission's proposed amendment to § 312.8, an operator must take reasonable measures to ensure that any service provider or third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information. This provision is intended to address security issues surrounding business-to-business releases of data.[167]

The proposed requirement that operators must take reasonable measures to ensure that third parties and service providers keep the shared information confidential and secure is a logical and necessary extension of the statutory requirement that operators themselves keep such

---

[165] 15 U.S.C. 6503(b)(1)(D).

[166] *See* 16 CFR 312.4(b)(2)(iv) and 312.8.

[167] *See supra* Part V.A.(3).

information confidential and secure. Therefore, the Commission proposes to amend § 312.8 to add a second sentence so that it reads:

> The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must take reasonable measures to ensure that any service provider or any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information.

E. Data Retention and Deletion Requirements (proposed 16 CFR 312.10)

As noted above, COPPA authorizes the Commission to promulgate regulations requiring operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[168] Deleting unneeded information is an integral part of any reasonable data security strategy. Accordingly, the Commission proposes adding a new data retention and deletion provision to become § 312.10.[169]

The proposed provision states that operators shall retain children's personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. In addition, it states that an operator must delete such information by taking reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

---

[168] 15 U.S.C. 6503(b)(1)(D).

[169] The Commission proposes moving the current § 312.10 (Safe Harbors) to § 312.11, and deleting as obsolete the current § 312.11 (Rulemaking review).

Although the current Rule does not contain a data retention and deletion requirement, the Commission has long encouraged such practices. According to its 1999 Notice of Proposed Rulemaking: "[t]he Commission encourages operators to establish reasonable procedures for the destruction of personal information once it is no longer necessary for the fulfillment of the purpose for which it was collected. Timely elimination of data is the ultimate protection against misuse or unauthorized disclosure."[170] More recently, the Commission has testified that companies should adopt a "privacy by design" approach, including by building data retention and disposal protections into their everyday business practices.[171]

The proposed new data retention and deletion provision (§ 312.10) reads:

> An operator of a website or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against

---

[170] *See* Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking, 64 FR 22750, 22758-59 (Apr. 27, 1999), *available at* **http://www.ftc.gov/os/fedreg/1999/april/990427childrensonlineprivacy.pdf**.

[171] *See, e.g., Internet Privacy: The Views of the FTC, the FCC, and NTIA: Hearing Before the Subcomms. on Commerce, Manufacturing, & Trade and Communications & Technology of the H.R. Comm. on Energy and Commerce*, 112th Cong., at 14 (2011) (Statement of Edith Ramirez, Commissioner, Federal Trade Commission), *available at* **http://www.ftc.gov/os/testimony/110714internetprivacytestimony.pdf**; *Privacy and Data Security: Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science & Transportation*, 112th Cong., at 12 (2011) (Statement of Julie Brill, Commissioner, Federal Trade Commission), *available at* **http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf**; *Data Security: Hearing Before the Subcomm. on Commerce, Manufacturing & Trade, H.R. Comm. on Energy and Commerce*, 112th Cong., at 9 (2011) (Statement of Edith Ramirez, Commissioner, Federal Trade Commission), *available at* **http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf**. *See also* Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 23, at 44.

unauthorized access to, or use of, the information in connection with its deletion.

F. Safe Harbors (current 16 CFR 312.10, proposed 16 CFR 312.11)

The COPPA statute established a "safe harbor" for participants in Commission-approved COPPA self-regulatory programs.[172] With the safe harbor provision, Congress intended to encourage industry members and other groups to develop their own COPPA oversight programs, thereby promoting efficiency and flexibility in complying with COPPA's substantive provisions.[173] COPPA's safe harbor provision also was intended to reward operators' good faith efforts to comply with COPPA. The Rule therefore provides that operators fully complying with an approved safe harbor program will be "deemed to be in compliance" with the Rule for purposes of enforcement. In lieu of formal enforcement actions, such operators instead are subject first to the safe harbor program's own review and disciplinary procedures.[174]

Current § 312.10 of the Rule sets forth the criteria the Commission uses to approve applications for safe harbor status under COPPA. First, the self-regulatory program must contain guidelines that protect children's online privacy to the same or greater extent as the Rule and ensure that each potential participant complies with these guidelines.[175] Second, the program

---

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

[173] *See* 1999 Statement of Basis and Purpose, 64 FR 59888, 59906 ("[T]his 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").

[174] *See* 16 CFR 312.10(a) and (b)(4).

[175] *See* 16 CFR 312.10(b)(1).

must monitor the participant's practices on an ongoing basis to ensure that the participant continues to comply with both the program's guidelines and the participant's own privacy notices.[176] Finally, the safe harbor program must contain effective incentive mechanisms to ensure operators' compliance with program guidelines.[177]

Several comments supported strengthening the Commission's oversight of participating safe harbor programs. TRUSTe, a Commission-approved COPPA safe harbor program, asked the Commission to develop better criteria for the approval of safe harbor programs that reflect the principles of reliability, accountability, transparency, and sustainability.[178] Another commenter urged the Commission regularly to audit the Commission-approved COPPA safe harbor programs to ensure compliance with the Rule.[179] The Commission finds merit in the calls to strengthen the Safe Harbor provisions of the Rule, and accordingly, proposes three substantive changes: requiring that applicants seeking Commission approval of self-regulatory guidelines submit comprehensive information about their capability to run an effective safe harbor program; establishing more rigorous baseline oversight by Commission-approved safe harbor programs of their members; and, requiring Commission-approved safe harbor programs to submit periodic reports to the Commission. The Commission also proposes several structural and linguistic changes to the Safe Harbors section to increase the Rule's clarity.

---

[176] *See* 16 CFR 312.10(b)(2)(i)-(iv).

[177] *See* 16 CFR 312.10(b)(3)(i)-(v). Effective incentives include mandatory public reporting of disciplinary action taken against participants by the safe harbor program; consumer redress; voluntary payments to the United States Treasury; referral of violators to the Commission; or any other equally effective incentive. *Id.*

[178] *See* TRUSTe (comment 64), at 6.

[179] *See* Harry A. Valetk (comment 66), at 4.

(1) *Criteria for approval of self-regulatory guidelines (paragraph (b))*

Paragraph (b) of the Rule's safe harbor provisions set forth the criteria the Commission will use to review an application for safe harbor status. Among other things, safe harbor applicants must demonstrate that they have an effective mandatory mechanism for the independent assessment of their members' compliance. The Rule outlines possible, non-exclusive, methods applicants may employ to conduct this independent review, including periodic comprehensive or random checks of members' information practices, seeding members' databases if coupled with random or periodic checks,[180] or "any other equally effective independent assessment mechanism."[181]

The Commission proposes maintaining the standard that safe harbor programs implement "an effective, mandatory mechanism for the independent assessment of subject operators' compliance." Rather than provide a set of alternative mechanisms that safe harbor programs can use to carry out this requirement, the Commission proposes to mandate that, at a minimum, safe harbor programs conduct annual, comprehensive reviews of each of their members' information practices. In the Commission's view, this baseline benchmark for oversight will improve the accountability and transparency of Commission-approved COPPA safe harbor programs.

Therefore, the Commission proposes to amend paragraph (b)(2) of the safe harbor provisions of the Rule to read:

---

[180] "Seeding" a participant's database means registering as a child on the website or online service and then monitoring the site or service to ensure that it complies with the Rule's requirements.

[181] *See* 16 CFR 312.10(b)(2).

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator's information policies, practices, and representations. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(2) ***Request for Commission approval of self-regulatory program guidelines (paragraph (c))***

Paragraph (c) of the Rule's current safe harbor provision sets forth the application requirements for safe harbor status. Among other things, an applicant must include the full text of the guidelines for which approval is sought and any accompanying commentary, a statement explaining how the applicant's proposed self-regulatory guidelines meet COPPA, and how the independent assessment mechanism and effective incentives for subject operators' compliance (required under paragraphs (b)(2) and (3)) provide effective enforcement of COPPA.[182]

To enhance the reliability and sustainability of programs granted safe harbor status,[183] the Commission proposes adding a requirement that program applicants include with their application a detailed explanation of their business model and the technological capabilities and mechanisms they will use for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program. This requirement will enable the Commission to better evaluate the qualifications of a safe harbor program applicant.

---

[182] *See* 16 CFR 312.10(c).

[183] *See* TRUSTe (comment 64), at 6.

Therefore, the Commission proposes adding a new requirement to paragraph (c) (paragraph (c)(1)) that reads:

> (c) *Request for Commission approval of self-regulatory program guidelines.* To obtain Commission approval of self-regulatory program guidelines, proposed safe harbor programs must file a request for such approval. A request shall be accompanied by the following:
>
> (1) A detailed explanation of the applicant's business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program.[184]

(3) *Safe harbor reporting and recordkeeping requirements (paragraph (d))*

Paragraph (d) of the current safe harbor provision requires Commission-approved safe harbor programs to maintain records of consumer complaints, disciplinary actions, and the results of the independent assessments required under paragraph (b)(2) for a period of at least three years. Such records shall be made available to the Commission for inspection and copying at the Commission's request.[185]

One commenter urged the Commission to make greater use of its inspection powers under paragraph (d) to audit safe harbor programs in order to "give the Commission a better understanding of actual marketplace practices, and inspire commercial operators to improve

---

[184] The Commission will consider applicants' requests that certain materials submitted in connection with an application for safe harbor should receive confidential treatment. *See* FTC Operating Manual, 15.5.1, and 15.5.2.

[185] *See* 16 CFR 312.10(d).

online practices."[186] The Institute for Public Representation went further, asking the Commission to "assess the effectiveness of the safe harbor programs by requiring annual reports about their enforcement efforts."[187] The Commission believes that instituting a periodic reporting requirement, in addition to retaining the right to access program records, will better ensure that all safe harbor programs maintain sufficient records and that the Commission is routinely apprised of key information about approved safe harbor programs and their members. Therefore, the Commission proposes modifying paragraph (d) to require, within one year of the effective date of the Final Rule amendments, and every eighteen months thereafter, the submission of reports to the Commission containing, at a minimum, the results of an independent audit described in revised paragraph (b)(2), and the reporting of any disciplinary action taken against any member operator within the relevant reporting period.

Therefore, the Commission proposes modifying paragraph (d) to read:

> (d) *Reporting and recordkeeping requirements.* Approved safe harbor programs shall:
>
> (1) Within one year after the effective date of the Final Rule amendments, and every eighteen months thereafter, submit a report to the Commission containing, at a minimum, the results of the independent assessment conducted under paragraph (b)(2), a description of any disciplinary action taken against any subject operator under paragraph (b)(3), and a description of any approvals of member operators' use of

---

186 *See* Harry A. Valetk (comment 66), at 4.

187 *See* Institute for Public Representation (comment 33), at 37.

parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to requests by the Commission for additional information; and,

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

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

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

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

(4) ***Revisions to increase the clarity of the safe harbor provisions***

The Commission also proposes a general reorganization of the safe harbor provision to provide a clearer roadmap of the requirements for obtaining and maintaining safe harbor status. This reorganization includes consolidating into separate paragraphs: the criteria for approval of self-regulatory program guidelines; the application requirements for Commission approval; reporting and recordkeeping requirements; post-approval modifications to self-regulatory program guidelines; and revocation of approval of self-regulatory program guidelines.[188] In addition, the Commission proposes adding language to the revocation of approval paragraph to require currently approved safe harbor programs to propose modifications to their guidelines

[188] The Commission also proposes deleting the requirement that the Commission must determine "in fact" that approved self-regulatory program guidelines or their implementation do not meet the requirements of the Rule's safe harbor provisions prior to revoking their approval.

within 60 days of publication of the Final Rule amendments in order to come into compliance or face revocation.[189] Finally, the proposed revision would move to the end of this section the Rule's provision on the effect of an operators' participation in a safe harbor program.

VI. Request for Comment

The Commission invites interested persons to submit written comments on any issue of fact, law, or policy that may bear upon the proposals under consideration. Please include explanations for any answers provided, as well as supporting evidence where appropriate. After evaluating the comments, the Commission will determine whether to issue specific amendments.

Comments should refer to "COPPA Rule Review: FTC File No. P104503" to facilitate the organization of comments. Please note that your comment – including your name and your state – will be placed on the public record of this proceeding, including on the publicly accessible FTC website, at **http://www.ftc.gov/os/publiccomments.shtm**. Comments must be received on or before the deadline specified above in the DATES section in order to considered by the Commission.

---

[189] Therefore, the Commission proposes to amend paragraph (f) of the safe harbor provisions of the Rule to read:

> (f) *Revocation of approval of self-regulatory program guidelines*. The Commission reserves the right to revoke any approval granted under this Section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs that were approved prior to the publication of the Final Rule amendments must, within 60 days of publication of the Final Rule amendments, submit proposed modifications to their guidelines that would bring them into compliance with such amendments, or their approval shall be revoked.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before November 28, 2011. Write "COPPA Rule Review, 16 CFR Part 312, Project No. P104503" on your comment. Your comment – including your name and your state – will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission website, at **http://www.ftc.gov/os/publiccomments.shtm**. As a matter of discretion, the Commission tries to remove individuals' home contact information from comments before placing them on the Commission website.

Because your comment will be made public, you are solely responsible for making sure that your comment doesn't include any sensitive personal information, such as anyone's Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or credit or debit card number. You are also solely responsible for making sure that your comment doesn't include any sensitive health information, like medical records or other individually identifiable health information. In addition, don't include any "[t]rade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential," as provided in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2). In particular, don't include competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

If you want the Commission to give your comment confidential treatment, you must file it in paper form, with a request for confidential treatment, and you must follow the procedure

explained in FTC Rule 4.9(c), 16 CFR 4.9(c).[190] Your comment will be kept confidential only if the FTC General Counsel, in his or her sole discretion, grants your request in accordance with the law and the public interest.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it at **https://ftcpublic.commentworks.com/ftc/ 2011copparulereview**, by following the instructions on the web-based form. If this document appears at **http://www.regulations.gov/#!home,** you also may file a comment through that website.

If you file your comment on paper, write "COPPA Rule Review, 16 CFR Part 312, Project No. P104503" on your comment and on the envelope, and mail or deliver it to the following address: Federal Trade Commission, Office of the Secretary, Room H-113 (Annex E), 600 Pennsylvania Avenue, NW, Washington, DC 20580. If possible, submit your paper comment to the Commission by courier or overnight service.

Visit the Commission website at **http://www.ftc.gov** to read this document and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or

---

[190] In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c), 16 CFR 4.9(c).

before November 28, 2011.[191] You can find more information, including routine uses permitted by the Privacy Act, in the Commission's privacy policy, at **http://www.ftc.gov/ftc/privacy.htm**.

Comments on any proposed recordkeeping, disclosure, or reporting requirements subject to review under the Paperwork Reduction Act should additionally be submitted to OMB. If sent by U.S. mail, they should be addressed to Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: Desk Officer for the Federal Trade Commission, New Executive Office Building, Docket Library, Room 10102, 725 17th Street, N.W.,Washington, D.C. 20503. Comments sent to OMB by U.S. postal mail, however, are subject to delays due to heightened security precautions. Thus, comments instead should be sent by facsimile to (202) 395-5167.

VII. Regulatory Flexibility Act

The Regulatory Flexibility Act of 1980 ("RFA"), 5 U.S.C. 601 *et seq.*, requires a description and analysis of proposed and final rules that will have significant economic impact on a substantial number of small entities. The RFA requires an agency to provide an Initial Regulatory Flexibility Analysis ("IRFA") with the proposed Rule, and a Final Regulatory Flexibility Analysis ("FRFA"), if any, with the final Rule.[192] The Commission is not required to make such analyses if a Rule would not have such an economic effect.[193]

---

[191] Questions for the public regarding proposed revisions to the Rule are found at Part X., *infra.*

[192] *See* 5 U.S.C. 603-04.

[193] *See* 5 U.S.C. 605.

Although, as described below, the Commission does not anticipate that the proposed changes to the Rule will result in substantially more websites and online services being subject to the Rule, it will result in greater disclosure, reporting, and compliance responsibilities for all entities covered by the Rule. The Commission believes that a number of operators of websites and online services potentially affected by the revisions are small entities as defined by the RFA. It is unclear whether the proposed amended Rule will have a significant economic impact on these small entities. Thus, to obtain more information about the impact of the proposed Rule on small entities, the Commission has decided to publish the following IRFA pursuant to the RFA and to request public comment on the impact on small businesses of its proposed amended Rule.

A. Description of the Reasons That Agency Action Is Being Considered

As described in Part I above, the Commission commenced a voluntary review of the COPPA Rule in early April 2010, seeking public comment on whether technological changes to the online environment warranted any changes to the Rule.[194] After careful review of the comments received, the Commission concludes that there is a need to update certain Rule provisions. Therefore, it proposes modifications to the Rule in the following five areas: Definitions, Notice, Parental Consent, Confidentiality and Security of Children's Personal Information, and Safe Harbor Programs. In addition, the Commission proposes adding a new Section to the Rule regarding data retention and deletion.

---

[194] *See* 75 FR 17089 (Apr. 5, 2010).

B. Succinct Statement of the Objectives of, and Legal Basis for, the Revised Proposed Rule

The objectives of the amendments are to update the Rule to ensure that children's online privacy continues to be protected, as directed by Congress, even as new online technologies evolve, and to clarify existing obligations for operators under the Rule. The legal basis for the proposed amendments is the Children's Online Privacy Protection Act, 15 U.S.C. 6501 *et seq.*

C. Description and Estimate of the Number of Small Entities to Which the Revised Proposed Rule Will Apply

The proposed amendments to the Rule will affect operators of websites and online services directed to children, as well as those operators that have actual knowledge that they are collecting personal information from children. The proposed Rule amendments will impose costs on entities that are "operators" under the Rule.

The Commission staff is unaware of any empirical evidence concerning the number of operators subject to the Rule. However, based on our compliance monitoring efforts in the area of children's privacy, data received by the Commission in connection with preparing its most recent studies of food marketing to children and marketing of violent entertainment to children, and the recent growth in interactive mobile applications that may be directed to children, the Commission staff estimates that approximately 2,000 operators may be subject to the Rule's requirements.

Under the Small Business Size Standards issued by the Small Business Administration, "Internet publishing and broadcasting and web search portals" qualify as small businesses if they

have fewer than 500 employees.[195] The Commission staff estimates that approximately 80% of operators potentially subject to the Rule qualify as small entities. The Commission staff bases this estimate on its experience in this area, which includes its law enforcement activities, oversight of safe harbor programs, conducting relevant workshops, and discussions with industry and privacy professionals. The Commission seeks comment and information with regard to the estimated number or nature of small business entities on which the proposed Rule would have a significant economic impact.

D. Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements

The proposed amended Rule would impose reporting, recordkeeping, and other compliance requirements within the meaning of the Paperwork Reduction Act, as set forth in Part VIII. of this Notice of Proposed Rulemaking. Therefore, the Commission is submitting the proposed requirements to OMB for review before issuing a final rule.

The proposed Rule likely would increase the recordkeeping, reporting, and other compliance requirements for covered operators. In particular, the proposed requirement that the direct notice to parents include more specific details about an operator's information collection practices, pursuant to a revised § 312.4 (Notice), would impose a one-time cost on operators. The Commission's proposed elimination of the sliding scale for acceptable mechanisms of obtaining parental consent, pursuant to a revised § 312.5 (consent mechanisms for verifiable

---

[195] *See* U.S. Small Business Administration Table of Small Business Size Standards Matched to North American Industry Classification System Codes, *available at* **http://www.sba.gov/sites/default/files/Size_Standards_Table.pdf**.

parental consent), would require those operators who previously used the email plus method to now use a more reliable method for obtaining parental consent. The addition of proposed language in § 312.8 (confidentiality, security, and integrity of personal information collected from children) would require operators to take reasonable measures to ensure that service providers and third parties to whom they release children's personal information have in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information. Finally, the proposed Rule contains additional reporting requirements for entities voluntarily seeking approval to be a COPPA safe harbor self-regulatory program, and additional reporting and recordkeeping requirements for all Commission-approved safe harbor programs. Each of these proposed improvements to the Rule may entail some added cost burden to operators, including those that qualify as small entities.

The estimated burden imposed by these proposed amendments is discussed in the Paperwork Reduction Act section of this document, and there should be no difference in that burden as applied to small businesses. While the Rule's compliance obligations apply equally to all entities subject to the Rule, it is unclear whether the economic burden on small entities will be the same as or greater than the burden on other entities. That determination would depend upon a particular entity's compliance costs, some of which may be largely fixed for all entities (*e.g.*, website programming) and others variable (*e.g.*, Safe Harbor participation), and the entity's income or profit from operation of the website itself (*e.g.*, membership fees) or related sources (*e.g.*, revenue from marketing to children through the site). As explained in the Paperwork Reduction Act section, in order to comply with the rule's requirements, website operators will require the professional skills of legal (lawyers or similar professionals) and technical (*e.g.*,

computer programmers) personnel. As explained earlier, the Commission staff estimates that there are approximately 2,000 website or online services that would qualify as operators under the proposed Rule, and that approximately 80% of such operators would qualify as small entities under the SBA's Small Business Size standards. The Commission invites comment and information on these issues.

E. Identification of Other Duplicative, Overlapping, or Conflicting Federal Rules

The Commission has not identified any other federal statutes, rules, or policies that would duplicate, overlap, or conflict with the proposed Rule. The Commission invites comment and information on this issue.

F. Description of Any Significant Alternatives to the Proposed Rule

In drafting the proposed amended Rule, the Commission has made every effort to avoid unduly burdensome requirements for entities. The Commission believes that the proposed amendments are necessary in order to continue to protect children's online privacy in accordance with the purposes of COPPA. For each of the proposed amendments, the Commission has attempted to tailor the provision to any concerns evidenced by the record to date. On balance, the Commission believes that the benefits to children and their parents outweigh the costs of implementation to industry.

The Commission considered, but decided against, providing an exemption for small businesses. The primary purpose of COPPA is to protect children's online privacy by requiring verifiable parental consent before an operator collects personal information. The record and the

Commission's enforcement experience have shown that the threats to children's privacy are just as great, if not greater, from small businesses or even individuals than from large businesses.[196] Accordingly, any exemption for small businesses would undermine the very purpose of the Statute and Rule.

Nonetheless, the Commission has taken care in developing the proposed amendments to set performance standards that will establish the objective results that must be achieved by regulated entities, but do not mandate a particular technology that must be employed in achieving these objectives. For example, the Commission has retained the standard that verifiable parental consent may be obtained via a means reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. The proposed new requirements for maintaining the security of children's personal information and deleting such information when no longer needed do not mandate any specific means to accomplish those objectives. The Commission also proposes to make it easier for operators to avoid the collection of children's personal information by adopting a "reasonable measures" standard enabling operators to use competent filtering technologies to prevent children's public disclosure of information.

---

[196] *See, e.g., United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal., filed Aug. 12, 2011); *United States v. Industrious Kid, Inc.*, No. CV-08-0639 (N.D. Cal., filed Jan. 28, 2008); *United States v. Xanga.com, Inc.*, No. 06-CIV-6853 (S.D.N.Y., filed Sept. 7, 2006); *United States v. Bonzi Software, Inc.*, No. CV-04-1048 (C.D. Cal., filed Feb. 17, 2004); *United States v. Looksmart, Ltd.*, Civil Action No. 01-605-A (E.D. Va., filed Apr. 18, 2001); *United States v. Bigmailbox.Com, Inc.*, Civil Action No. 01-606-B (E.D. Va., filed Apr. 18, 2001).

The Commission seeks comments on ways in which the Rule could be modified to reduce any costs or burdens for small entities.

VIII. Paperwork Reduction Act

The existing Rule contains recordkeeping, disclosure, and reporting requirements that constitute "information collection requirements" as defined by 5 CFR 1320.3(c) under the OMB regulations that implement the Paperwork Reduction Act ("PRA"), 44 U.S.C. 3501 *et seq.* OMB has approved the Rule's existing information collection requirements through July 31, 2014 (OMB Control No. 3084-0117).

The proposed amendments to the COPPA Rule would change the definition of "personal information," potentially increasing the number of operators subject to the Rule. The proposed amendments also would eliminate email plus as an acceptable method for obtaining parental consent, require operators to provide parents with a more detailed direct notice, and increase reporting and recordkeeping requirements for Commission-approved safe harbor programs. Accordingly, the Commission is providing PRA burden estimates for the proposed amendments, which are set forth below.

The Commission invites comments on: (1) whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (2) the accuracy of the FTC's estimate of the burden of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of collecting

information on those who respond, including through the use of automated collection techniques or other forms of information technology.

Estimated Additional Annual Hours Burden:

A. Number of Respondents

As noted in the Regulatory Flexibility Section of this NPR, Commission staff estimates that there are currently approximately 2,000 operators subject to the Rule. The Commission believes that the number of operators subject to the Rule's requirements will not change significantly as a result of the proposed revisions to the definition of personal information. Even though altering the definition of personal information potentially expands the pool of covered operators, other proposed changes in the Rule should offset much of this potential expansion. Specifically, these offsets include provisions allowing the use of persistent identifiers to support the internal operations of a website or online service, and permitting the use of reasonable measures such as automated filtering to strip out personal information before posting children's content in interactive venues. The Commission also anticipates many of these potentially new operators will make adjustments to their information collection practices so that they will not be collecting personal information from children, as defined by the Rule.

For this burden analysis, the Commission staff retains its recently published estimate of 100 new operators per year[197] for a prospective three-year PRA clearance period.[198] The Commission staff also retains its estimate that no more than one additional safe harbor applicant will submit a request within the next three years.

B. Recordkeeping Hours

The proposed Rule amendments do not impose any new significant recordkeeping requirements on operators. The proposed amendments do impose additional recordkeeping requirements on safe harbor programs, however. Commission staff estimates that in the year of implementation ("Year 1"), the four existing safe harbor programs will require no more than 100 hours to set up and implement a new recordkeeping system to comply with the proposed amendments.[199] In later years, once compliant systems are established, the burden for these entities should be negligible – no more than one hour each year.[200] Thus, annualized burden per year for a prospective three-year clearance for existing safe harbor programs is 34 hours per safe harbor program (100 + 1 + 1 = 102 hours; 102 hours ÷ 3 = 34 hour per year). Accordingly, for

---

[197] *See* Agency Information Collection Activities; Submission for OMB Review; Comment Request; Extension, 76 FR 31334 (May 31, 2011) ("FTC COPPA PRA Extension").

[198] Under the PRA, agencies may seek a maximum of three years' clearance for a collection of information. 44 U.S.C. 3507(g). Recordkeeping, disclosure, and reporting requirements are all forms of information collection. *See* 44 U.S.C. 3502(3).

[199] *See, e.g.*, Telemarketing Sales Rule ("TSR"), Notice of Proposed Rulemaking, 74 FR 41988, 42013 (Aug. 19, 2009). Arguably, this estimate conservatively errs upward in the instant context.

[200] *Id*.

the four existing safe harbor programs, cumulative annualized recordkeeping burden would be 136 hours.

For a new entrant, the initial burden of establishing recordkeeping systems and the burden of maintenance thereafter should be no more than for the existing safe harbors. Assuming, as noted above, that there will be one new safe harbor entrant per a given three-year PRA clearance period, the incremental annualized recordkeeping burden for the entrant under the proposed amendments would be 34 hours.

Thus, cumulative annualized recordkeeping burden for new and existing safe harbor applicants would be 170 hours.

C. Disclosure Hours

(*1) New Operators' Disclosure Burden*

Under the existing OMB clearance for the Rule, the Commission staff has already accounted for the time that new operators will spend to craft a privacy policy (approximately 60 hours per operator), design mechanisms to provide the required online privacy notice and, where applicable, direct notice to parents in order to obtain verifiable consent. The proposed amendments should no more than minimally add to, if at all, the time required to accomplish this task because their effect primarily is to transfer required information from the privacy policy to the direct notice.

(2) Existing Operators' Disclosure Burden

In Year 1, operators would have a one-time burden to re-design their existing privacy policies and direct notice procedures that would not carry over to the second and third years of prospective PRA clearance. In addition, existing operators that currently use the email plus method would incur burden in Year 1 for converting to a more reliable method of parental verification. Commission staff believes that an existing operator's time to make these changes would be no more than that estimated for a new entrant to craft a privacy policy for the first time, *i.e.*, 60 hours. Annualized over three years of PRA clearance, this amounts to 20 hours ((60 hours + 0 + 0) ÷ 3) per year. Aggregated for the 2,000 existing operators, annualized disclosure burden would be 40,000 hours.

D. Reporting Hours

The FTC previously has estimated that a prospective safe harbor organization requires 265 hours to prepare and submit its safe harbor proposal.[201] The proposed Rule amendments, however, require a safe harbor applicant to submit a more detailed proposal than what the current Rule mandates. Existing safe harbor programs will thus need to submit a revised application and new safe harbor applicants will have to provide greater detail than they would under the current Rule. The FTC estimates this added information would entail approximately 60 additional hours for safe harbors to prepare. Accordingly, the aggregate incremental burden

---

[201] For PRA purposes, annualized over the course of three years of clearance, this averages roughly 100 hours per year given that the 265 hours is a one-time, not recurring, expenditure of time for an applicant.

for this added one-time preparation is 300 hours (60 hours x 5 safe harbors) or, annualized for an average single year per three-year PRA clearance, 100 hours.

The proposed amendments to the Rule require safe harbor programs to audit their members at least annually and to submit periodic reports to the Commission on the results of their audits of members. As such, this will increase currently cleared burden estimates pertaining to safe harbor applicants. The burden for conducting member audits and preparing these reports will likely vary for each safe harbor program depending on the number of members. The Commission staff estimates that conducting audits and preparing reports will require approximately 100 hours per program per year. Aggregated for five safe harbor programs, this amounts to an increased disclosure burden of 500 hours per year. Accordingly, cumulative yearly reporting burden for five safe harbor applicants to provide the added information proposed and to conduct audits and prepare reports is 600 hours.

E. Labor Costs

(*1*) *Recordkeeping*

Based on the above estimate of 170 hours for existing and new safe harbor programs, annualized for an average single year per three-year PRA clearance, and applying a skilled labor rate of $26/hour,[202] associated labor costs are $4,420 per year.

---

[202] This rounded figure is derived from the mean hourly earnings shown for computer support specialists found in the Bureau of Labor Statistics National Compensation Survey: Occupational Earnings in the United States, 2010, at Table 3, *available at* **http://www.bls.gov/ncs/ocs/sp/nctb1477.pdf** ("National Compensation Survey Table 3").

(2) Disclosure

The Commission staff assumes that the time spent on compliance for operators would be apportioned five to one between legal (lawyers or similar professionals) and technical (*e.g.*, computer programmers) personnel.[203] As noted above, the Commission staff estimates a total of 40,000 hours disclosure burden, annualized, for 2,000 existing operators. Thus, apportioned five to one, this amounts to, rounded, 33,333 hours of legal, and 6,667 hours of technical, assistance. Applying hourly rates of $150 and $36, respectively, for these personnel categories,[204] associated labor costs would total approximately $5,240,000.

(3) Reporting

The Commission staff assumes that the task to prepare safe harbor program applications will be performed primarily by lawyers at a mean labor rate of $150 an hour. Thus, applied to an assumed industry total of 500 hours per year for this task, associated yearly labor costs would total $75,000.

---

[203] *See* FTC COPPA PRA Extension, 76 FR at 31335 n. 1.

[204] The estimated rate of $150 per hour is roughly midway between Bureau of Labor Statistics (BLS) mean hourly wages for lawyers (approximately $54) in the most recent whole-year data (2010) available online and what Commission staff believes more generally reflects hourly attorney costs ($250) associated with Commission information collection activities. The $36 estimate of mean hourly wages for computer programmers also is based on the most recent whole-year BLS data. *See* National Compensation Survey Table 3.

The Commission staff assumes periodic reports will be prepared by compliance officers, at a labor rate of $28.[205] Applied to an assumed industry total of 500 hours per year for this task, associated yearly labor costs would be $14,000.

Cumulatively, labor costs for the above-noted reporting requirements total approximately $89,000 per year.

F. Non-Labor/Capital Costs

Because both operators and safe harbor programs will already be equipped with the computer equipment and software necessary to comply with the Rule's notice requirements, the proposed amendments to the Rule should not impose any additional capital or other non-labor costs.

IX. Communications by Outside Parties to the Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding, from any outside party to any Commissioner or Commissioner's advisor, will be placed on the public record. *See* 16 CFR 1.26(b)(5).

X. Questions For the Proposed Revisions to the Rule

The Commission is seeking comment on various aspects of the proposed Rule, and is particularly interested in receiving comment on the questions that follow. These questions are designed to assist the public and should not be construed as a limitation on the issues on which public comment may be submitted. Responses to these questions should cite the numbers and

---

[205] *See* National Compensation Survey Table 3.

subsection of the questions being answered. For all comments submitted, please submit any relevant data, statistics, or any other evidence, upon which those comments are based.

General Questions

1. Please provide comment on any or all of the provisions in the proposed Rule. For each provision commented on please describe (a) the impact of the provision(s) (including any benefits and costs), if any, and (b) what alternatives, if any, the Commission should consider, as well as the costs and benefits of those alternatives.

Definitions (§ 312.2)

2. Do the changes to the definition of "collects or collection" sufficiently encompass all the ways in which information can be collected online from children?

3. Does the "reasonable measures" standard articulated in the proposed definition of "collects or collection" adequately protect children while providing sufficient guidance to operators?

4. Are there identifiers that the Commission should consider adding to the list of "online contact information"?

5. Proposed § 312.2 would define personal information to include a "screen or user name."

a. What would be the impact of including "screen or user name" in the definition of personal information?

b. Is the limitation "used for functions other than or in addition to support for the internal operations of the website or online service" sufficiently clear to provide notice of the circumstances under which screen or user name is covered by the Rule?

6. Proposed § 312.2 would define personal information to include a "persistent identifier."

a. What would be the impact of the changes to the term "persistent identifier" in the definition of personal information?

b. Is the limitation "used for functions other than or in addition to support for the internal operations of the website or online service" sufficiently clear to provide notice of the circumstances under which a persistent identifier is covered by the Rule?

c. Are there additional identifiers that the Commission should consider adding to the list of "persistent identifiers"?

7. Proposed § 312.2 would define personal information to include a "an identifier that links the activities of a child across different websites or online services." Is the language sufficiently clear to provide notice of the types of identifiers covered by this paragraph?

8. Proposed § 312.2 would define personal information to include "photograph, video, or audio file where such file contains a child's image or voice" and no longer requires that photographs (or similar items) be combined with "other information such that the combination permits physical or online contacting." What would be the impact of expanding the definition of personal information in this regard?

9. Are there identifiers that the Commission should consider adding to § 312.2's definition of "personal information"?

a. Should paragraph (e) of the definition of personal information include other forms of government-issued identification in addition to Social Security Number?

b. Does the combination of date of birth, gender, and ZIP code provide sufficient information to permit the contacting of a specific individual such that this combination of identifiers should be included as an item of personal information?

c. Should the Commission include "ZIP + 4" as an item of personal information?

10. Proposed § 312.2 would define "release of personal information" as "the sharing, selling, renting, or transfer of personal information to any third party." Is this definition sufficient to cover all potential secondary uses of children's personal information?

11. Proposed § 312.2 would define "support for the internal operations of the website or online service" as "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)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose."

a. Is the term "activities necessary to maintain the technical functioning" sufficiently clear to provide notice of the types of activities that constitute "support for the internal operations of the website or online service"? For example, is it sufficiently clear that the mere collection of an IP address, which is a necessary technical step in providing online content

to web viewers, constitutes an "activity necessary to maintain the technical functioning of the website or online service"?

b. Should activities other than those necessary to maintain the technical functioning or to fulfill a request of a child under §§ 312.5(c)(3) and (4) be included within the definition of "support for the internal operations of the website or online service"?

Notice (§ 312.4)

12. Do the proposed changes to the "notice on the website or online service" requirements in § 312.4(b) clarify or improve the quality of such notice?

13. Do the proposed changes to the "direct notice to the parent" requirements in § 312.4(c) clarify or improve the quality of such notices?

14. Should the Commission modify the notice requirement of the Rule to require that operators post a link to their online notice in any location where their mobile applications can be purchased or otherwise downloaded (*e.g.*, in the descriptions of their applications in Apple's App Store or in Google's Android Market)?

15. Are there other effective ways of placing notices that should be included in the proposed revised Rule?

Parental Consent (§ 312.5)

16. Do the additional methods for parental consent set forth in proposed § 312.5(b)(2) sufficiently reflect available technologies to ensure that the person providing consent is the child's parent?

17. Should the Commission require operators to maintain records indicating that parental consent was obtained, and if so, what would constitute a sufficient record? What burdens would be imposed on operators by such a requirement?

18. Is there other information the Commission should take into account before declining to adopt certain parental consent mechanisms discussed in Part V.C.(1). of the Notice of Proposed Rulemaking?

19. The Commission proposes eliminating the "email plus" mechanism of parental consent from § 312.5(b)(2). What are the costs and benefits to operators, parents, and children of eliminating this mechanism?

20. Proposed § 312.5(b)(3) would provide that operators subject to Commission-approved self-regulatory program guidelines may use a parental consent mechanism determined by such safe harbor program to meet the requirements of § 312.5(b)(1). Does proposed § 312.5(b)(3) provide a meaningful incentive for the development of new parental consent mechanisms? What are the potential downsides of this approach?

Confidentiality, Security and Integrity of Personal Information Collected From Children (§ 312.8)

21. Proposed § 312.8 would add the requirement that an operator "take reasonable measures to ensure that any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information."

a. What are the costs and benefits to operators, parents, and children of adding this requirement?

b. Does the language proposed by the Commission provide sufficient guidance and flexibility to operators to effectuate this requirement?

Data Retention and Deletion (§ 312.10)

22. The Commission proposes adding a requirement that an operator retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

a. Does the language proposed by the Commission provide sufficient guidance and flexibility to operators to effectuate this requirement?

b. Should the Commission propose specific time frames for data retention and deletion?

c. Should the Commission more specifically delineate what constitutes "reasonable measures to protect against unauthorized access to or use of the information"?

Safe Harbors (§ 312.11)

23. Proposed § 312.11(b)(2) would require safe harbor program applicants to conduct a comprehensive review of all member operators' information policies, practices, and representations at least annually. Is this proposed annual review requirement reasonable? Would it go far enough to strengthen program oversight of member operators?

24. Proposed § 312.11(c)(1) would require safe harbor program applicants to include a detailed explanation of their business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of member operators' fitness for membership in the safe harbor program. Is this proposed requirement reasonable? Would it

provide the Commission with useful information about an applicant's ability to run a safe harbor program?

25. Proposed § 312.11(d) would require Commission-approved safe harbor programs to submit periodic reports to the Commission regarding their oversight of member websites.

a. Should the Commission consider requiring safe harbor programs to submit reports on a more frequent basis, *e.g.*, annually?

b. Should the Commission require that safe harbor programs report to the Commission a member's violations of program guidelines immediately upon their discovery by the safe harbor program?

Paperwork Reduction Act

26. The Commission solicits comments on whether the changes to the notice requirements (§ 312.4) and to the safe harbor requirements (§ 312.11), as well as the new data retention and deletion requirement (§ 312.10), constitute "collections of information" within the meaning of the Paperwork Reduction Act. The Commission requests comments that will enable it to:

a. Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

b. Evaluate the accuracy of the agency's estimate of the burden of the proposed collections of information, including the validity of the methodology and assumptions used;

c. Enhance the quality, utility, and clarity of the information to be collected; and,

d. Minimize the burden of the collections of information on those who must comply, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

XI. Proposed Revisions to the Rule

List of Subjects in 16 CFR Part 312

Children, Communications, Consumer Protection, Electronic Mail, E-mail, Internet, Online Service, Privacy, Record Retention, Safety, Science and Technology, Trade Practices, Website, Youth.

For the reasons discussed above, the Commission proposes to amend Part 312 of Title 16, Code of Federal Regulations, as follows:

Part 312 — CHILDREN'S ONLINE PRIVACY PROTECTION RULE

1. The authority citation for Part 312 continues to read as follows:

AUTHORITY: 15 U.S.C. 6501-6508.

2. Amend § 312.2 by revising the following definitions:

§ 312.2 Definitions.

* * * * *

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

(a) Requesting, prompting, or encouraging a child to submit personal information online;

(b) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or,

(c) Passive tracking of a child online.

* * * * *

Disclose or disclosure means, with respect to personal information:

(a) The release of personal information collected by an operator from a child in identifiable form 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,

(b) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

* * * * *

Online contact information means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

* * * * *

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) Online contact information as defined in this Section;

(d) A screen or user name where such screen or user name is used for functions other than or in addition to support for the internal operations of the website or online service;

(e) A telephone number;

(f) A Social Security number;

(g) A persistent identifier, including but not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier, where such persistent identifier is used for functions other than or in addition to support for the internal operations of, or protection of the security or integrity of, the website or online service;

(h) An identifier that links the activities of a child across different websites or online services;

(i) A photograph, video, or audio file where such file contains a child's image or voice;

(j) Geolocation information sufficient to identify street name and name of a city or town; or,

(k) 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.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

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, to protect the security or integrity of the website or online service, or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose.

* * * * *

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 content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, 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, and evidence regarding the intended audience.

3. Amend § 312.4 by revising paragraphs (b) and (c) as follows:

§ 312.4 Notice.

* * * * *

(b) *Notice on the website or online service.* Pursuant to § 312.3(a), each operator of a website or online service directed to children must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its website or online service, *and,* at each area of the website or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. 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 or landing page or screen of the children's area. To be complete, the online notice of the website or online service's information practices must state the following:

(1) Each operator's contact information, which at a minimum, must include the operator's name, physical address, telephone number, and email address;

(2) A description of what information each operator collects from children, including whether the website or online service enables a child to make personal information publicly available; how such operator uses such information, and; the operator's disclosure practices for such information; and,

(3) 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) *Direct notice to a parent*. An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of the child's personal information, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(1) *Content of the direct notice to the parent required under § 312.5(c)(1) (Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information).* This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to obtain the parent's consent;

(ii) That the parent's consent is required for the child's participation in the website or online service, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The additional items of personal information the operator intends to collect from the child, if any, and the potential opportunities for the disclosure of personal information, if any, should the parent consent to the child's participation in the website or online service;

(iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(b);

(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and,

(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

(2) *Content of the direct notice to the parent allowed under § 312.5(c)(2) (Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information).* This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to the parent of a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information; and,

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the operator to allow the child to participate in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and,

(iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

(3) *Content of the direct notice to the parent required under § 312.5(c)(4) (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times)*. This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

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

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and,

(vi) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

(4) *Content of the direct notice to the parent required under § 312.5(c)(5) (Notice to a Parent In Order to Protect a Child's Safety)*. This direct notice shall set forth:

(i) That the operator has collected the child's name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

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

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and,

(v) A hyperlink to the operator's online notice of its information practices required under § 312.4(b).

4. Amend § 312.5 by revising paragraph (b)(2), by adding new paragraphs (b)(3) and (b)(4), and by revising paragraph (c), to read as follows:

§ 312.5 Parental consent.

* * * * *

(b) * * *

(2) Existing 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, facsimile, or an electronic scan; requiring a parent to use a credit card in connection with a monetary transaction; having a parent call a toll-free telephone number staffed by trained personnel; having a parent connect to trained personnel via video-conference; or, verifying a parent's identity by checking a form of government-issued identification against databases of such information, *provided that* the parent's identification is deleted by the operator from its records promptly after such verification is complete.

(3) *Commission approval of parental consent mechanisms.* Interested parties may file written requests for Commission approval of parental consent mechanisms not currently enumerated in paragraph (b)(2). To be considered for approval, parties must provide a detailed description of the

proposed parental consent mechanism, together with an analysis of how the mechanism meets paragraph (b)(1). The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the request. The Commission shall issue a written determination within 180 days of the filing of the request.

(4) *Safe harbor approval of parental consent mechanisms.* A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent mechanism not currently enumerated in paragraph (b)(2) where the safe harbor program determines that such parental consent mechanism meets the requirements of paragraph (b)(1).

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

(1) Where the sole purpose of collecting a parent's online contact information and the name of the child or the parent is to provide notice and obtain parental consent under § 312.4(c)(1) of this part. 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 sole purpose of collecting a parent's online contact information is to provide notice to, and update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting a child's online contact information is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

(4) Where the sole purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts,

taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(4). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the sole purpose of collecting a child's name, and a child's and a parent's online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the sole purpose of collecting a child's name and online contact information is to: (i) protect the security or integrity of its website or online service; (ii) take precautions against liability; (iii) 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; and, where such information is not be used for any other purpose.

5. Revise § 312.8 to read as follows:

§ 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. The operator must take reasonable measures to ensure that any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information.

6. Revise §312.10 to read as follows:

§ 312.10 Data retention and deletion requirements.

An operator of a website or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

7. Revise § 312.11 to read as follows:

§ 312.11 Safe harbor programs.

(a) *In general.* Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines ("safe harbor programs"). The application shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the application. The Commission shall issue a written determination within 180 days of the filing of the application.

(b*) Criteria for approval of self-regulatory program guidelines.* Proposed safe harbor programs must demonstrate that they meet the following performance standards:

(1) Program requirements that ensure operators subject to the self-regulatory program guidelines ("subject operators") provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and 312.10.

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator's information policies, practices, and representations. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(3) Disciplinary actions for subject operators' non-compliance with self-regulatory program guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of any action taken against subject operators by the industry group issuing the self-regulatory guidelines;

(ii) Consumer redress;

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

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

(v) Any other equally effective action.

(c) *Request for Commission approval of self-regulatory program guidelines.* A proposed safe harbor program's request for approval shall be accompanied by the following:

(1) A detailed explanation of the applicant's business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program.

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

(3) A comparison of each provision of §§ 312.2 through 312.8, and 312.10 with the corresponding provisions of the guidelines; and,

(4) A statement explaining: (i) how the self-regulatory program guidelines, including the applicable assessment mechanisms, meet the requirements of this part; and, (ii) how the assessment mechanisms and compliance consequences required under paragraphs (b)(2) and (b)(3) provide effective enforcement of the requirements of this part.

(d) *Reporting and recordkeeping requirements.* Approved safe harbor programs shall:

(1) Within one year after the effective date of the Final Rule amendments, and every eighteen months thereafter, submit a report to the Commission containing, at a minimum, the results of the independent assessment conducted under paragraph (b)(2), a description of any disciplinary action taken against any subject operator under paragraph (b)(3), and a description of any approvals of member operators' use of parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to Commission requests for additional information; and,

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

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

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

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

(e) *Post-approval modifications to self-regulatory program guidelines.* Approved safe harbor programs must submit proposed changes to their guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(2). The statement required under paragraph (c)(4) must describe how the proposed changes affect existing provisions of the guidelines.

(f) *Revocation of approval of self-regulatory program guidelines*. The Commission reserves the right to revoke any approval granted under this Section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs that were approved prior to the publication of the Final Rule amendments must, within 60 days of publication of the Final Rule amendments, submit proposed modifications to their guidelines that would bring them into compliance with such amendments, or their approval shall be revoked.

(g) *Operators' participation in a safe harbor program.* An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8, and 312.10 if that operator complies with Commission-approved safe harbor program guidelines. In considering whether to initiate an investigation or bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator's participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator's non-compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3).

By direction of the Commission.

Donald S. Clark
Secretary.