
# FEDERAL REGISTER

Vol. 78 Thursday,
No. 12 January 17, 2013

Part II

## Federal Trade Commission

16 CFR Part 312
Children's Online Privacy Protection Rule; Final Rule

**FEDERAL TRADE COMMISSION**

**16 CFR Part 312**

**RIN 3084–AB20**

## Children's Online Privacy Protection Rule

**AGENCY:** Federal Trade Commission (''FTC'' or ''Commission'').

**ACTION:** Final rule amendments.

**SUMMARY:** The Commission amends the Children's Online Privacy Protection Rule (''COPPA Rule'' or ''Rule''), consistent with the requirements of the Children's Online Privacy Protection Act, to clarify the scope of the Rule and strengthen its protections for children's personal information, in light of changes in online technology since the Rule went into effect in April 2000. The final amended Rule includes modifications to the definitions of *operator, personal information,* and *Web site or online service directed to children.* The amended Rule also updates the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbor provisions, and adds a new provision addressing data retention and deletion.

**DATES:** The amended Rule will become effective on July 1, 2013.

**ADDRESSES:** The complete public record of this proceeding will be available at *www.ftc.gov.* Requests for paper copies of this amended Rule and Statement of Basis and Purpose (''SBP'') should be sent to: Public Reference Branch, Federal Trade Commission, 600 Pennsylvania Avenue NW., Room 130, 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:**

### Statement of Basis and Purpose

### I. Overview and Background

*A. Overview*

This document states the basis and purpose for the Commission's decision to adopt certain amendments to the COPPA Rule that were proposed and published for public comment on September 27, 2011 (''2011 NPRM''),[1] and supplemental amendments that were proposed and published for public comment on August 6, 2012 (''2012 SNPRM'').[2] After careful review and consideration of the entire rulemaking record, including public comments submitted by interested parties, and based upon its experience in enforcing and administering the Rule, the Commission has determined to adopt amendments to the COPPA Rule. These amendments to the final Rule will help to ensure that COPPA continues to meet its originally stated goals to minimize the collection of personal information from children and create a safer, more secure online experience for them, even as online technologies, and children's uses of such technologies, evolve.

The final Rule amendments modify the definitions of *operator* to make clear that the Rule covers an operator of a child-directed site or service where it integrates outside services, such as plug-ins or advertising networks, that collect personal information from its visitors; *Web site or online service directed to children* to clarify that the Rule covers a plug-in or ad network when it has actual knowledge that it is collecting personal information through a child-directed Web site or online service; *Web site or online service directed to children* to allow a subset of child-directed sites and services to differentiate among users, and requiring such properties to provide notice and obtain parental consent only for users who self-identify as under age 13; *personal information* to include geolocation information and persistent identifiers that can be used to recognize a user over time and across different Web sites or online services; and *support for internal operations* to expand the list of defined activities.

The Rule amendments also streamline and clarify the direct notice requirements to ensure that key information is presented to parents in a succinct ''just-in-time'' notice; expand the non-exhaustive list of acceptable methods for obtaining prior verifiable parental consent; create three new exceptions to the Rule's notice and consent requirements; strengthen data security protections by requiring operators to take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of such information; require reasonable data retention and deletion procedures; strengthen the Commission's oversight of self-regulatory safe harbor programs; and institute voluntary pre-approval mechanisms for new consent methods and for activities that support the internal operations of a Web site or online service.

*B. 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 Web sites or online services directed to children under 13 years of age, and on operators of other Web sites 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.[3] 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 information than is reasonably necessary to participate in such activities.[4] 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.[5]

The Commission initiated review of the COPPA Rule in April 2010 when it published a document in the **Federal Register** seeking public comment on whether the rapid-fire pace of technological changes to the online environment over the preceding five years warranted any changes to the Rule.[6] The Commission's request for public comment examined each aspect of the COPPA Rule, posing 28 questions for the public's consideration.[7] The Commission also held a public roundtable to discuss in detail several of the areas where public comment was sought.[8]

The Commission received 70 comments from industry representatives, advocacy groups, academics, technologists, and

[1] 2011 NPRM, 76 FR 59804, *available at http://ftc.gov/os/2011/09/110915coppa.pdf.*

[2] 2012 SNPRM, 77 FR 46643, *available at http://ftc.gov/os/2012/08/120801copparule.pdf.*

[3] *See* 16 CFR 312.3.

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

[5] *See* 16 CFR 312.10.

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

[7] *Id.*

[8] Information about the June 2010 public roundtable is located at *http://www.ftc.gov/bcp/workshops/coppa/index.shtml.*

individual members of the public in response to the April 5, 2010 request for public comment.[9] After reviewing the comments, the Commission issued the 2011 NPRM, which set forth several proposed changes to the COPPA Rule.[10] The Commission received over 350 comments in response to the 2011 NPRM.[11] After reviewing these comments, and based upon its experience in enforcing and administering the Rule, in the 2012 SNPRM, the Commission sought additional public comment on a second set of proposed modifications to the Rule.

The 2012 SNPRM proposed modifying the definitions of both *operator* and *Web site or online service directed to children* to allocate and clarify the responsibilities under COPPA when independent entities or third parties, *e.g.,* advertising networks or downloadable software kits (''plug-ins''), collect information from users through child-directed sites and services. In addition, the 2012 SNPRM proposed to further modify the definition of *Web site or online service directed to children* to permit Web sites or online services that are directed both to children and to a broader audience to comply with COPPA without treating all users as children. The Commission also proposed modifying the definition of *screen or user name* to cover only those situations where a screen or user name functions in the same manner as *online contact information.* Finally, the Commission proposed to further modify the revised definitions of *support for internal operations* and *persistent identifiers.* The Commission received 99 comments in response to the 2012 SNPRM.[12] After reviewing these additional comments, the Commission now announces this final amended COPPA Rule.

## II. Modifications to the Rule

### *A. Section 312.2: Definitions*

#### 1. Definition of Collects or Collection

#### a. Collects or Collection, Paragraph (1)

In the 2011 NPRM, the Commission proposed amending paragraph (1) to change the phrase ''requesting that children submit personal information online'' to ''requesting, prompting, or encouraging a child to submit personal information online.'' The proposal was to clarify that the Rule covers the online collection of personal information both when an operator requires it to participate in an online activity, and when an operator merely prompts or encourages a child to provide such information.[13] The comments received divided roughly equally between support of and opposition to the proposed change to paragraph (1). Those in favor cited the increased clarity of the revised language as compared to the existing language.[14]

Several commenters opposed the revised language of paragraph (1). For example, the National Cable and Telecommunications Association (''NCTA'') expressed concern that the revised language suggests that ''COPPA obligations are triggered even without the actual or intended collection of personal information.'' [15] NCTA asked the Commission to clarify that ''prompting'' or ''encouraging'' does not trigger COPPA unless an operator *actually* collects personal information from a child.[16]

The Rule defines *collection* as ''the gathering of any personal information from a child by any means,'' and the terms ''prompting'' and ''encouraging'' are merely exemplars of the means by which an operator gathers personal information from a child.[17] This change to the definition of *collects or collection* is intended to clarify the longstanding Commission position that an operator that provides a field or open forum for a child to enter personal information will not be shielded from liability merely because entry of personal information is not mandatory to participate in the activity. It recognizes the reality that such an operator must have in place a system to provide notice to and obtain consent from parents to deal with the moment when the information is ''gathered.'' [18] Otherwise, once the child posts the personal information, it will be too late to obtain parental consent.

After reviewing the comments, the Commission has decided to modify paragraph (1) of the definition of *collects or collection* as proposed in the 2011 NPRM.

#### b. Collects or Collection, Paragraph (2)

Section 312.2(b) of the Rule defines ''collects or collection'' to cover 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.'' [19] This exception, often referred to as the ''100% deletion standard,'' was designed to enable sites and services to make interactive content available to children, without providing parental notice and obtaining consent, provided that all personal information was deleted prior to posting.[20]

The 2010 FRN sought comment on whether to change the 100% deletion standard, whether automated systems used to review and post child content could meet this standard, and whether

[9] Public comments in response to the Commission's 2010 FRN are located at *http://www.ftc.gov/os/comments/copparulerev2010/index.shtm.* Comments cited herein to the **Federal Register** Notice are designated as such, and are identified by commenter name, comment number, and, where applicable, page number.

[10] *See supra* note 1.

[11] Public comments in response to the 2011 NPRM are located at *http://www.ftc.gov/os/comments/copparulereview2011/.* Comments cited herein to the 2011 NPRM are designated as such, and are identified by commenter name, comment number, and, where applicable, page number.

[12] Public comments in response to the 2012 SNPRM are available online at *http://ftc.gov/os/comments/copparulereview2012/index.shtm.* Comments cited herein to the SNPRM are designated as such, and are identified by commenter name, comment number, and, where applicable, page number.

[13] One commenter, Go Daddy, expressed concern that the definition of *collects or collection* is silent as to personal information acquired from children offline that is uploaded, stored, or distributed to third parties by operators. Go Daddy (comment 59, 2011 NPRM), at 2. However, Congress limited the scope of COPPA to information that an operator collects *online* from a child; COPPA does not govern information collected by an operator 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.'').

[14] *See* Institute for Public Representation (comment 71, 2011 NPRM), at 19; kidSAFE Seal Program (comment 81, 2011 NPRM), at 5; Alexandra Lang (comment 87, 2011 NPRM), at 1.

[15] NCTA (comment 113, 2011 NPRM), at 17–18.

[16] *Id.*

[17] *See* 16 CFR 312.2: ''*Collects* or *collection* means the gathering of any personal information from a child by any means, including but not limited to * * *''

[18] Several other commenters raised concern that the language ''prompting, or encouraging'' could make sites or services that post third-party ''Like'' or ''Tweet This'' buttons subject to COPPA. *See* Association for Competitive Technology (comment 5, 2011 NPRM), at 6; Direct Marketing Association (''DMA'') (comment 37, 2011 NPRM), at 6; *see also* American Association of Advertising Agencies (comment 2, 2011 NPRM), at 2–3; Interactive Advertising Bureau (''IAB'') (comment 73, 2011 NPRM), at 12. The collection of personal information by plug-ins on child-directed sites is addressed fully in the discussion regarding changes to the definition of *operator. See* Part II.A.4.a., *infra.*

[19] Under the Rule, operators who offered services such as social networking, chat, and bulletin boards and who did not pre-strip (*i.e.,* completely delete) such information were deemed to have ''disclosed'' personal information under COPPA's definition of *disclosure. See* 16 CFR 312.2.

[20] *See* P. 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.*

the Commission had provided sufficient guidance on the deletion of personal information.[21] In response, several commenters urged a new standard, arguing that the 100% deletion standard, while well-intentioned, was an impediment to operators' implementation of sophisticated automated filtering technologies that may actually aid in the detection and removal of personal information.[22]

In the 2011 NPRM, the Commission stated that the 100% deletion standard set an unrealistic hurdle to operators' implementation of automated filtering systems that could promote engaging and appropriate online content for children, while ensuring strong privacy protections by design. To address this, the Commission proposed replacing the 100% deletion standard with a ''reasonable measures'' standard. Under this approach, an operator would not be deemed to have collected personal information 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.''[23]

Although the Institute for Public Representation raised concerns about the effectiveness of automated filtering techniques,[24] most comments were resoundingly in favor of the ''reasonable measures'' standard. For example, one commenter stated that the revised language would enable the use of automated procedures that could provide ''increased consistency and more effective monitoring than human monitors,''[25] while another noted that it would open the door to ''cost-efficient and reliable means of monitoring children's communications.''[26] Several commenters noted that the proposed reasonable measures standard would likely encourage the creation of more rich, interactive online content for children.[27] Another commenter noted that the revised provision, by offering greater flexibility for technological solutions, should help minimize the burden of COPPA on children's free expression.[28]

The Commission is persuaded that the 100% deletion standard should be replaced with a reasonable measures standard. The reasonable measures standard strikes the right balance in ensuring that operators have effective, comprehensive measures in place to prevent public online disclosure of children's personal information and ensure its deletion from their records, while also retaining the flexibility operators need to innovate and improve their mechanisms for detecting and deleting such information. Therefore, the final Rule amends paragraph (2) of the definition of *collects or collection* to adopt the reasonable measures standard proposed in the 2011 NPRM.

c. Collects or Collection, Paragraph (3)

In the 2011 NPRM, the Commission proposed to modify paragraph (3) of the Rule's definition of *collects or collection* to clarify that it includes all means of passively collecting personal information from children online, irrespective of the technology used. The Commission sought to accomplish this by removing from the original definition the language ''or use of any identifying code linked to an individual, such as a cookie.''[29]

The Commission received several comments supporting,[30] and several comments opposing,[31] this proposed change. Those opposing the change generally believed that this change somehow expanded the definition of *personal information.* As support for their argument, these commenters also referenced the Commission's proposal to include persistent identifiers within the definition of *personal information.*

The Commission believes that paragraph (3), as proposed in the 2011 NPRM, is sufficiently understandable. The paragraph does nothing to alter the fact that the Rule covers only the collection of *personal information.* Moreover, the final Rule's exception for the limited use of persistent identifiers to support internal operations—312.5(c)(7)—clearly articulates the specific criteria under which an operator will be exempt from the Rule's notice and consent requirements in connection with the passive collection of a persistent identifier.[32] Accordingly, the Commission adopts the definition of *collects or collection* as proposed in the 2011 NPRM.

2. Definition of Disclose or Disclosure

In the 2011 NPRM, the Commission proposed making several minor modifications to Section 312.2 of the Rule's definition of *disclosure,* including broadening the title of the definition 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 *disclosure* shall apply.[33] In addition, the Commission proposed moving the definitions of *release of personal information* and *support for the internal operations of the Web site or online service* contained within the definition of *disclosure* to make them stand-alone definitions within Section 312.2 of the Rule.[34]

One commenter asked the Commission to modify paragraph (2) of the proposed definition by adding an opening clause linking it to the definition of *collects or collection.*[35] While this commenter did not state its reasons for the proposed change, the Commission believes that the language of paragraph (2) is sufficiently clear so as not to warrant making the change suggested. Therefore, the Commission modifies the definition of *disclosure or disclosure* as proposed in the 2011 NPRM.

3. Definition of Online Contact Information

Section 312.2 of the Rule defines *online contact information* as ''an email address or any other substantially similar identifier that permits direct contact with a person online.'' The 2011 NPRM proposed clarifications to the definition to flag that the term broadly covers all identifiers that permit direct

[21] *See* 75 FR at 17090, Question 9.

[22] *See* Entertainment Software Association (''ESA'') (comment 20, 2010 FRN), at 13–14; R. Newton (comment 46, 2010 FRN), at 4; Privo, Inc. (comment 50, 2010 FRN), at 5; B. Szoka (comment 59, 2010 FRN), at 19; *see also* Wired Safety (comment 68, 2010 FRN), at 15.

[23] *See* 76 FR at 59808.

[24] *See* Institute for Public Representation (comment 71, 2011 NPRM), at 19.

[25] *See* NCTA (comment 113, 2011 NPRM), at 8.

[26] DMA (comment 37, 2011 NPRM), at 7.

[27] *See* DMA *id.;* Institute for Public Representation (comment 71, 2011 NPRM), at 3; kidSAFE Seal Program (comment 81, 2011 NPRM), at 5; NCTA (comment 113, 2011 NPRM), at 8; Toy Industry Association (comment 163, 2011 NPRM), at 8.

[28] *See* TechFreedom (comment 159, 2011 NPRM), at 6.

[29] 76 FR at 59808.

[30] Privacy Rights Clearinghouse indicated its belief that this change would give operators added incentive to notify parents of their information collection practices, particularly with regard to online tracking and behavioral advertising. *See* Privacy Rights Clearinghouse (comment 131, 2011 NPRM), at 2; *see also* Consumers Union (comment 29, 2011 NPRM), at 2; kidSAFE Seal Program (comment 81, 2011 NPRM), at 6.

[31] *See* DMA (comment 37, 2011 NPRM), at 9–10; IAB (comment 73, 2011 NPRM), at 12; NCTA (comment 113, 2011 NPRM), at 17–18; National Retail Federation (comment 114, 2011 NPRM), at 2–3; TechAmerica (comment 157, 2011 NPRM), at 5–6.

[32] *See* Part II.C.10.g., *infra.*

[33] *See* 2011 NPRM, 76 FR at 59809.

[34] The Commission intended this change to clarify what was meant by the terms *release of personal information* and *support for the internal operations of the Web site or online service,* where those terms are referenced elsewhere in the Rule and are not directly connected with the terms *disclose or disclosure.*

[35] *See* kidSAFE Seal Program (comment 81, 2011 NPRM), at 8 (''[P]aragraph (b) under the definition of ''disclose or disclosure'' should have the following opening clause: Subject to paragraph (b) under the definition of ''collects or collection,'' making personal information collected by an operator from a child publicly available * * *.'').

contact with a person online and to ensure consistency between the definition of *online contact information* and the use of that term within the definition of *personal information.*[36] The proposed revised definition identified commonly used online identifiers, including email addresses, instant messaging (''IM'') user identifiers, voice over Internet protocol (''VOIP'') identifiers, and video chat user identifiers, while also clarifying that the list of identifiers was non-exhaustive and would encompass other substantially similar identifiers that permit direct contact with a person online.[37] The Commission received few comments addressing this proposed change.

One commenter opposed the modification, asserting that IM, VOIP, and video chat user identifiers do not function in the same way as email addresses. The commenter's rationale for this argument was that not all IM identifiers reveal the IM system in use, which information is needed to directly contact a user.[38] The Commission does not find this argument persuasive. While an IM address may not reveal the IM program provider in every instance, it very often does. Moreover, several IM programs allow users of different messenger programs to communicate across different messaging platforms. Like email, instant messaging is a communications tool that allows people to communicate one-to-one or in groups B sometimes in a faster, more real-time fashion than through email. The Commission finds, therefore, that IM identifiers provide a potent means to contact a child directly.

Another commenter asked the Commission to expand the definition of *online contact information* to include mobile phone numbers. The commenter noted that, given the Rule's coverage of mobile apps and web-based text messaging programs, operators would benefit greatly from collecting a parent's mobile phone number (instead of an email address) in order to initiate contact for notice and consent.[39] The Commission recognizes that including mobile phone numbers within the definition of *online contact information* could provide operators with a useful tool for initiating the parental notice process through either SMS text or a phone call. It also recognizes that there may be advantages to parents for an operator to initiate contact via SMS text B among them, that parents generally have their mobile phones with them and that SMS text is simple and convenient.[40] However, the statute did not contemplate mobile phone numbers as a form of online contact information, and the Commission therefore has determined not to include mobile phone numbers within the definition.[41] Thus, the final Rule adopts the definition of *online contact information* as proposed in the 2012 SNPRM.

4. Definitions of Operator and Web Site or Online Service Directed to Children

In the 2012 SNPRM, the Commission proposed modifying the definitions of both *operator* and *Web site or online service directed to children* to allocate and clarify the responsibilities under COPPA when independent entities or third parties, *e.g.,* advertising networks or downloadable plug-ins, collect information from users through child-directed sites and services. Under the proposed revisions, the child-directed content provider would be strictly liable for personal information collected by third parties through its site. The Commission reasoned that, although the child-directed site or service may not own, control, or have access to the personal information collected, such information is collected on its behalf due to the benefits it receives by adding more attractive content, functionality, or advertising revenue. The Commission also noted that the primary-content provider is in the best position to know that its site or service is directed to children, and is appropriately positioned to give notice and obtain consent.[42] By contrast, if the Commission failed to impose obligations on the content providers, there would be no incentive for child-directed content providers to police their sites or services, and personal information would be collected from young children, thereby undermining congressional intent. The Commission also proposed imputing the child-directed nature of the content site to the entity collecting the personal information only if that entity knew or had reason to know that it was collecting personal information through a child-directed site.[43]

Most of the comments opposed the Commission's proposed modifications. Industry comments challenged the Commission's statutory authority for both changes and the breadth of the language, and warned of the potential for adverse consequences. In essence, many industry comments argued that the Commission may not apply COPPA where independent third parties collect personal information through child-directed sites,[44] and that even if the Commission had some authority, exercising it would be impractical because of the structure of the ''online ecosystem.''[45] Many privacy and children's advocates agreed with the 2012 SNPRM proposal to hold child-directed content providers strictly liable, but some expressed concern about holding plug-ins and advertising networks to a lesser standard.[46]

For the reasons discussed below, the Commission, with some modifications to the proposed Rule language, will retain the strict liability standard for child-directed content providers that allow other online services to collect personal information through their sites. The Commission will deem a plug-in or other service to be a covered co-operator only where it has actual knowledge that it is collecting information through a child-directed site.

a. Strict Liability for Child-Directed Content Sites: Definition of Operator

Implementing strict liability as described above requires modifying the current definition of *operator.* The Rule, which mirrors the statutory language, defines *operator* in pertinent part, as

[36] The Rule's definition of *personal information* included the sub-category ''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 email address.'' The 2011 NPRM proposed replacing that sub-category of personal information with *online contact information.*

[37] 76 FR at 59810.

[38] *See* DMA (comment 37, 2011 NPRM), at 11.

[39] kidSAFE Seal Program (comment 81, 2011 NPRM), at 7. Acknowledging the Commission's position that cell phone numbers are outside of the statutory definition of *online contact information,* kidSAFE advocates for a statutory change, if needed, to enable mobile app operators, in particular, to reach parents using contact information ''relevant to their ecosystem.''

[40] At the same time, the Commission believes it may be impractical to expect children to correctly distinguish between mobile and land-line phones when asked for their parents' mobile numbers.

[41] Moreover, given that the final Rule's definition of *online contact information* encompasses a broad, non-exhaustive list of online identifiers, operators will not be unduly burdened by the Commission's determination that cell phone numbers are not online contact information.

[42] 2012 SNPRM, 77 FR at 46644. The Commission acknowledged that this decision reversed a previous policy choice to place the burden of notice and consent entirely upon the information collection entity.

[43] In so doing, the Commission noted that it believed it could hold the information collection entity strictly liable for such collection because, when operating on child-directed properties, that portion of an otherwise general audience service could be deemed *directed to children.* 2012 SNPRM, 77 FR at 46644–46645.

[44] *See, e.g.,* Facebook (comment 33, 2012 SNPRM), at 3–4.

[45] *See* Microsoft (comment 66, 2012 SNPRM), at 6; IAB (comment 49, 2012 SNPRM), at 5; DMA (comment 28, 2012 SNPRM), at 5.

[46] *See, e.g.,* Institute for Public Representation (comment 52, 2012 SNPRM), at 20; Common Sense Media (comment 20, 2012 SNPRM), at 6.

''any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, where such Web site or online service is operated for commercial purposes, including any person offering products or services for sale through that Web site or online service, involving commerce * * *'' [47]

In the 2012 SNPRM, the Commission proposed adding a proviso to that definition stating that personal information is *collected or maintained on behalf of* an operator where it is collected in the interest of, as a representative of, or for the benefit of, the operator.

Industry, particularly online content publishers, including app developers, criticized this proposed change.[48] Industry comments argued that the phrase ''on whose behalf'' in the statute applies only to agents and service providers,[49] and that the Commission lacks the authority to interpret the phrase more broadly to include any incidental benefit that results when two parties enter a commercial transaction.[50] Many commenters pointed to an operator's post-collection responsibilities under COPPA, *e.g.,* mandated data security and affording parents deletion rights, as evidence that Congress intended to cover only those entities that control or have access to the personal information.[51]

Commenters also raised a number of policy objections. Many argued that child-directed properties, particularly small app developers, would face unreasonable compliance costs and that the proposed revisions might choke off their monetization opportunities,[52] thus decreasing the incentive for developers to create engaging and educational content for children.[53] They also argued that a strict liability standard is impractical given the current online ecosystem, which does not rely on close working relationships and communication between content providers and third parties that help monetize that content.[54] Some commenters urged the Commission to consider a safe harbor for content providers that exercise some form of due diligence regarding the information collection practices of plug-ins present on their site.[55]

Privacy organizations generally supported imposing strict liability on content providers. They agreed with the Commission's statement in the 2012 SNPRM that the first-party content provider is in a position to control which plug-ins and software downloads it integrates into its site and that it benefits by allowing information collection by such third parties.[56] They also noted how unreasonable it would be for parents to try to decipher which entity might actually be collecting data through the child-directed property.[57]

Finally, many commenters expressed concern that the language describing ''on whose behalf'' reaches so broadly as to cover not only child-directed content sites, but also marketplace platforms such as Apple's iTunes App Store and Google's Android market (now Google Play) if they offered child-directed apps on their platforms.[58] These commenters urged the Commission to revise the language of the Rule to exclude such platforms.

After considering the comments, the Commission retains a strict liability standard for child-directed sites and services that allow other online services to collect personal information through their sites.[59] The Commission disagrees with the views of commenters that this is contrary to Congressional intent or the Commission's statutory authority. The Commission does not believe Congress intended the loophole advocated by many in industry: Personal information being collected from children through child-directed properties with no one responsible for such collection.

Nor is the Commission persuaded by comments arguing that the phrase ''on whose behalf'' must be read extremely narrowly, encompassing only an agency relationship. Case law supports a broader interpretation of that phrase.[60] Even some commenters opposed to the Commission's interpretation have

[47] 15 U.S.C. 6501(2). The Rule's definition of *operator* reflects the statutory language. *See* 16 CFR 312.2.

[48] *See, e.g.,* Application Developers Alliance (comment 5, 2012 SNPRM), at 3–4; Association of Competitive Technology (comment 7, 2012 SNPRM), at 4–5; IAB (comment 49, 2012 SNPRM), at 5–6; Online Publishers Association (comment 72, 2012 SNPRM), at 10–11; Magazine Publishers of America (comment 61, 2012 SNPRM), at 3–5; The Walt Disney Co. (comment 96, 2012 SNPRM), at 4–5; S. Weiner (comment 97, 2012 SNPRM), at 1–2; WiredSafety (comment 98, 2012 SNPRM), at 3.

[49] *See* DMA (comment 28, 2012 SNPRM), at 12; Internet Commerce Coalition (comment 53, 2012 SNPRM), at 5; TechAmerica (comment 87, 2012 SNPRM), at 2–3.

[50] *See, e.g.,* Gibson, Dunn & Crutcher (comment 39, 2012 SNPRM), at 7–9; Facebook (comment 33, 2012 SNPRM), at 6 (entities acting primarily for their own benefit not considered to be acting on behalf of another party).

[51] *See, e.g.,* Business Software Alliance (comment 12, 2012 SNPRM), at 2–4; Internet Commerce Coalition (comment 53, 2012 SNPRM), at 5; *see also, e.g.,* IAB (comment 49, 2012 SNPRM), at 5; DMA (comment 28, 2012 SNPRM), at 6; Online Publishers Association (comment 72, 2012 SNPRM), at 10–11; The Walt Disney Co. (comment 96, 2012 SNPRM), at 3–5.

[52] *See* Center for Democracy & Technology (''CDT'') (comment 15, 2012 SNPRM), at 4–5; DMA (comment 28, 2012 SNPRM), at 5; Google (comment 41, 2012, SNPRM), at 3–4; Lynette Mattke (comment 63, 2012 SNPRM).

[53] *See* Google (comment 41, 2012 SNPRM), at 3; Application Developers Alliance (comment 5, 2012 SNPRM), at 5; Association for Competitive Technology (comment 6, 2012 SNPRM), at 5; The Walt Disney Co. (comment 96, 2012 SNPRM), at 4; ConnectSafely (comment 21, 2012 SNPRM), at 2.

[54] *See* Application Developers Alliance (comment 5, 2012 SNPRM), at 3; Online Publishers Association (comment 72, 2012 SNPRM), at 11; The Walt Disney Co. (comment 96, 2012 SNPRM), at 4; DMA (comment 28, 2012 SNPRM), at 4.

[55] *See, e.g.,* Online Publishers Association (comment 72, 2012 SNPRM), at 11 (publisher should be entitled to rely on third party's representations about its information practices); The Walt Disney Co. (comment 96, 2012 SNPRM), at 5 (operator of a site directed to children should be permitted to rely on the representations made by third parties regarding their personal information collection practices, as long as the operator has undertaken reasonable efforts to limit any unauthorized data collection); Internet Commerce Coalition (comment 53, 2012 SNPRM), at 6 (the Commission should state that operators whose sites or services are targeted to children should bind third party operators whom they know are collecting personal information through their sites or services to comply with COPPA with regard to that information collection).

[56] *See* Institute for Public Representation (comment 52, 2012 SNPRM), at 18–19; Common Sense Media (comment 20, 2012 SNPRM), at 4–6; EPIC (comment 31, 2012 SNPRM), at 5–6; Catholic Bishops (comment 92, 2012 SNPRM), at 3; CDT (comment 15, 2012 SNPRM), at 3.

[57] *See* Institute for Public Representation (comment 52, 2012 SNPRM), at 19; Common Sense Media (comment 20, 2012 SNPRM), at 5.

[58] *See* CDT (comment 15, 2012 SNPRM), at 5; Apple (comment 4, 2012 SNPRM), at 3–4; Assert ID (comment 6, 2012 SNPRM), at 5.

[59] Although this issue is framed in terms of child-directed content providers integrating plug-ins or other online services into their sites because that is by far the most likely scenario, the same strict liability standard would apply to a general audience content provider that allows a plug-in to collect personal information from a specific user when the provider has actual knowledge the user is a child.

[60] *National Organization for Marriage v. Daluz,* 654 F.3d 115, 121 (1st Cir. 2011) (statute requiring expenditure reports by independent PAC to the treasurer of the candidate ''on whose behalf'' the expenditure was made meant to the candidate who stands to benefit from the independent expenditure's advocacy); *accord American Postal Workers Union* v. *United States Postal Serv.,* 595 F. Supp 1352 (D.D.C. 1984) (Postal Union's activities held to be ''on behalf of'' a political campaign where evidence showed union was highly politicized, with goal of electing a particular candidate); *Sedwick Claims Mgmt. Servs.* v. *Barrett Business Servs., Inc.,* 2007 WL 1053303 (D. Or. 2007) (noting that 9th Circuit has interpreted the phrase ''on behalf of'' to include both ''to the benefit of'' *and* in a representative capacity); *United States* v. *Dish Network, LLC,* 2010 U.S. Dist. LEXIS 8957, 10 (C.D. Ill. Feb. 3, 2010) (reiterating the court's previous opinion that the plain meaning of the phrases ''on whose behalf'' or ''on behalf of'' is an act by a representative of, or an act for the benefit of, another).

acknowledged that the Commission's proposal is based on ''an accurate recognition that online content monetization is accomplished through a complex web of inter-related activities by many parties,'' and have noted that to act on behalf of another is to do what that person would ordinarily do herself if she could.[61] That appears to be precisely the reason many first-party content providers integrate these services. As one commenter pointed out, content providers ''have chosen to devote their resources to develop great content, and to let partners help them monetize that content. In part, these app developers and publishers have made this choice because collecting and handling children's data internally would require them to take on liability risk and spend compliance resources that they do not have.'' [62] Moreover, content-providing sites and services often outsource the monetization of those sites ''to partners'' because they do not have the desire to handle it themselves.[63]

In many cases, child-directed properties integrate plug-ins to enhance the functionality or content of their properties or gain greater publicity through social media in an effort to drive more traffic to their sites and services. Child-directed properties also may obtain direct compensation or increased revenue from advertising networks or other plug-ins. These benefits to child-directed properties are not merely incidental; as the comments point out, the benefits may be crucial to their continued viability.[64]

The Commission recognizes the potential burden that strict liability places on child-directed content providers, particularly small app developers. The Commission also appreciates the potential for discouraging dynamic child-directed content. Nevertheless, when it enacted COPPA, Congress imposed absolute requirements on child-directed sites and services regarding restrictions on the collection of personal information; those requirements cannot be avoided through outsourcing offerings to other operators in the online ecosystem. The Commission believes that the potential burden on child-directed sites discussed by the commenters in response to the 2012 SNPRM will be eased by the more limited definition of persistent identifiers, the more expansive definition of *support for internal operations* adopted in the Final Rule, and the newly-created exception to the Rule's notice and parental consent requirements that applies when an operator collects only a persistent identifier and only to support the operator's internal operations.[65]

The Commission considered including the ''due-diligence'' safe harbor for child-directed content providers that many of the comments proposed.[66] Nevertheless, as many other comments pointed out, it cannot be the responsibility of parents to try to pierce the complex infrastructure of entities that may be collecting their children's personal information through any one site.[67] For child-directed properties, one entity, at least, must be strictly responsible for providing parents notice and obtaining consent when personal information is collected through that site. The Commission believes that the primary-content site or service is in the best position to know which plug-ins it integrates into its site, and is also in the best position to give notice and obtain consent from parents.[68] Although the Commission, in applying its prosecutorial discretion, will consider the level of due diligence a primary-content site exercises, the Commission will not provide a safe harbor from liability.

When it issued the 2012 SNPRM, the Commission never intended the language describing ''on whose behalf'' to encompass platforms, such as Google Play or the App Store, when such stores merely offer the public access to someone else's child-directed content. In these instances, the Commission meant the language to cover only those entities that designed and controlled the content, *i.e.,* the app developer or site owner. Accordingly, the Commission has revised the language proposed in the 2012 SNPRM to clarify that personal information will be deemed to be collected on behalf of an operator where it benefits by allowing another person to collect personal information *directly from* users of such operator's site or service, thereby limiting the provision's coverage to operators that design or control the child-directed content.[69] Accordingly, the Final Rule shall state that personal information is *collected or maintained on behalf of* an operator when it is collected or maintained by an agent or service provider of the operator; or the operator benefits by allowing another person to collect personal information directly from users of such operator's Web site or online service.

b. Operators Collecting Personal Information Through Child-Directed Sites and Online Services: Moving to an Actual Knowledge Standard

In the 2012 SNPRM, the Commission proposed holding responsible as a co-operator any site or online service that ''knows or has reason to know'' it is collecting personal information through a host Web site or online service directed to children. Many commenters criticized this standard. Industry comments contended that such a standard is contrary to the statutory mandate that general audience services be liable only if they have actual knowledge they are collecting information from a child.[70] They further

[61] Application Developers Alliance (comment 5, 2012 SNPRM), at 2; *see also* Gibson, Dunn & Crutcher (comment 39, 2012 SNPRM), at 7.

[62] Application Developers Alliance (comment 5, 2012 SNPRM), at 4.

[63] *Id.; see also* Association for Competitive Technology (comment 7, 2012 SNPRM), at 5; *see generally* DMA (comment 28, 2012 SNPRM), at 5; Facebook (comment 33, 2012 SNPRM), at 3; Online Publishers Association (comment 72, 2012 SNPRM), at 11.

[64] *Id.*

[65] *See* Part II.A.5.b., *infra* (discussion of persistent identifiers and support of internal operations).

[66] The type of due diligence advocated ranged from essentially relying on a plug-in or advertising network's privacy policy to requiring an affirmative contract. *See, e.g.,* The Walt Disney Co. (comment 96, 2012 SNPRM), at 5 (operator should be able to rely on third party's representations about its information collection practices, if operator makes reasonable efforts to limit unauthorized data collection); Gibson, Dunn & Crutcher (comment 39, 2012 SNPRM), at 23–24 (provide a safe harbor for operators that certify they do not receive, own, or control any personal information collected by third parties; alternatively, grant a safe harbor for operators that also certify they do not receive a specific benefit from the collection, or that obtain third party's certification of COPPA compliance); Internet Commerce Coalition (comment 53, 2012 SNPRM), at 6–7 (provide a safe harbor for operators whose policies prohibit third party collection on their sites).

[67] *See* Common Sense Media (comment 20, 2012 SNPRM), at 4–5; EPIC (comment 31, 2012 SNPRM), at 6; Institute for Public Representation (comment 52, 2012 SNPRM), at 18–19.

[68] Some commenters, although not conceding the need to impose strict liability on any party, noted that if the burden needed to fall on either the primary content provider or the plug-in, it was better to place it on the party that controlled the child-directed nature of the content. *See, e.g.,* CTIA (comment 24, 2012 SNPRM), at 8–9; CDT (comment 15, 2012 SNPRM), at 4–5. Not surprisingly, industry members primarily in the business of providing content did not share this view. *See, e.g.,* Association for Competitive Technology (comment 7, 2012 SNPRM), at 4–5; Business Software Alliance (comment 12, 2012 SNPRM), at 2–4; Entertainment Software Association (comment 32, 2102 SNPRM), at 9; Online Publishers Association (comment 72, 2012 SNPRM), at 10–11; The Walt Disney Co. (comment 96, 2012 SNPRM), at 6.

[69] This clarification to the term ''on behalf of'' is intended only to address platforms in instances where they function as an conduit to someone else's content. Platforms may well wear multiple hats and are still responsible for complying with COPPA if they themselves collect personal information directly from children.

[70] *See* Business Software Alliance (comment 12, 2012 SNPRM), at 4–5; Digital Advertising Alliance (comment 27, 2012 SNPRM), at 2; Google (comment 41, 2012 SNPRM), at 4; Internet Commerce Coalition (comment 53, 2012 SNPRM), at 7; Magazine Publishers of America (comment 61, 2012

Continued

argued that the standard is vague because it is impossible to determine what type of notification would provide a ''reason to know.'' Thus, the commenters argued that the standard triggers a duty to inquire.[71] In addition, commenters stated that even after inquiring, it might be impossible to determine which sites are truly directed to children (particularly in light of the Commission's revised definition of *Web site directed to children* to include those sites that are likely to attract a disproportionate percentage of children under 13).[72] Conversely, many privacy advocates believed it is necessary to impose some duty of inquiry, or even strict liability, on the entity collecting the personal information.[73]

After considering the comments, the Commission has decided that while it is appropriate to hold an entity liable under COPPA for collecting personal information on Web sites or online services directed to children, it is reasonable to hold such entity liable only where it has *actual knowledge* that it is collecting personal information directly from users of a child-directed site or service. In striking this balance by moving to an actual knowledge standard, the Commission recognizes that this is still contrary to the position advocated by many industry comments: That a plug-in or advertising network that collects personal information from users of both general audience and child-directed sites must be treated monolithically as a general audience service, liable only if it has actual knowledge that it is collecting personal information from a specific child.[74] However, the COPPA statute also defines *Web site or online service directed to children* to include ''that portion of a commercial Web site or online service that is targeted to children.'' Where an operator of an otherwise general audience site or online service has actual knowledge it is collecting personal information directly from users of a child-directed site, and continues to collect that information, then, for purposes of the statute, it has effectively adopted that child-directed content as its own and that portion of its service may appropriately be deemed to be directed to children.[75]

Commenters urged that, whatever standard the Commission ultimately adopts, it provide guidance as to when a plug-in or advertising network would be deemed to have knowledge that it is collecting information through a child-directed site or service.[76] Knowledge, by its very nature, is a highly fact-specific inquiry. The Commission believes that the actual knowledge standard it is adopting will likely be met in most cases when: (1) A child-directed content provider (who will be strictly liable for any collection) directly communicates the child-directed nature of its content to the other online service; or (2) a representative of the online service recognizes the child-directed nature of the content. The Commission does not rule out that an accumulation of other facts would be sufficient to establish actual knowledge, but those facts would need to be analyzed carefully on a case-by-case basis.

5. Definition of Personal Information

a. Screen or User Names

The Rule defines *personal information* as including ''a screen name that reveals an individual's email address.'' [77] In the 2011 NPRM, the Commission proposed to modify this definition to include ''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 Web site or online service.'' [78] The Commission intended this change to address scenarios in which a screen or user name could be used by a child as a single credential to access multiple online properties, thereby permitting him or her to be directly contacted online, regardless of whether the screen or user name contained an email address.[79]

Some commenters expressed concern that the Commission's screen-name proposal would unnecessarily inhibit functions that are important to the operation of child-directed Web sites and online services.[80] In response to this concern, the 2012 SNPRM proposed covering screen names as *personal information* only in those instances in which a screen or user name rises to the level of *online contact information.* In such cases, the Commission reasoned, a screen or user name functions much like an email address, an instant messaging identifier, or ''any other substantially similar identifier that permits direct contact with a person online.'' [81]

The Commission received a number of comments in support of this change from industry associations and advocacy groups.[82] Commenters recognized the change as providing operators with the flexibility to use screen or user names both for internal administrative purposes and across affiliated sites, services, or platforms without requiring prior parental notification or verifiable parental consent.[83]

A number of commenters, however, despite clear language otherwise in the 2012 SNPRM, continued to express concern that the Commission's proposed revision would limit operators' use of anonymized screen names in place of children's real names in filtered chat, moderated interactive forums, or as log-in credentials providing users with seamless access to content across multiple platforms and devices.[84] Some of these commenters

SNPRM), at 8; Toy Industry Association (comment 89, 2012 SNPRM), at 10–11; *see also* ACLU (comment 3, 2012 SNPRM), at 2–3; TechAmerica (comment 87, 2012 SNPRM), at 3.

[71] *See* CDT (comment 15, 2012 SNPRM), at 2; CTIA (comment 24, 2012 SNPRM), at 10; Entertainment Software Association (comment 32, 2012 SNPRM), at 9; Marketing Research Association (comment 62, 2012 SNPRM), at 2; Tangman (comment 85, 2012 SNPRM).

[72] *See* DMA (comment 28, 2012 SNPRM), at 9; Magazine Publishers of America (comment 61, 2012 SNPRM), at 8; Menessec (comment 65, 2012 SNPRM); Privo (comment 76, 2012 SNPRM), at 8.

[73] *See* Common Sense Media (comment 20, 2012 SNPRM), at 6; Institute for Public Representation (comment 52, 2012 SNPRM), at 20–22.

[74] *See* Digital Advertising Alliance (comment 27, 2012 SNPRM), at 2; DMA (comment 28, 2012 SNPRM), at 8–9; Entertainment Software Association (comment 32, 2012 SNPRM), at 13–14.

[75] Similarly, when a behavioral advertising network offers age-based advertising segments that target children under 13, that portion of its service becomes an *online service directed to children. Contra* DMA (comment 28, 2012 SNPRM), at 12. The Commission also believes that narrowing the definition of persistent identifiers and further revisions to the definition of *Web site or online service directed to children* ease (although not entirely eliminate) many of the concerns expressed in industry comments. *See, e.g.,* CDT (comment 15, 2012 SNPRM), at 3; Digital Advertising Alliance (comment 27, 2012 SNPRM), at 2; Entertainment Software Association (comment 32, 2012 SNPRM), at 14 (combination of reason to know standard and expanded definition of persistent identifiers creates an unworkable result).

[76] *See* Microsoft (comment 66, 2012 SNPRM), at 2; TRUSTe (comment 90, 2012 SNPRM), at 4; *see also* Association for Competitive Technology (comment 7, 2012 SNPRM), at 3–4; Google (comment 41, 2012 SNPRM), at 4; DMA (comment 28, 2012 SNPRM), at 7; Viacom (comment 95, 2012 SNPRM), at 8–9.

[77] *See* 16 CFR 312.2 (paragraph (n), definition of *personal information*).

[78] 2011 NPRM, 76 FR at 59810.

[79] *Id.*

[80] *See* DMA (comment 37, 2011 NPRM), at 15–16; ESA (comment 47, 2011 NPRM), at 9; NCTA (comment 113, 2011 NPRM), at 12; Scholastic (comment 144, 2011 NPRM), at 12; A. Thierer (comment 162, 2011 NPRM), at 6; TRUSTe (comment 164, 2011 NPRM), at 3; The Walt Disney Co. (comment 170, 2011 NPRM), at 21.

[81] *See* 2011 NPRM, 76 FR at 59810 (proposed definition of *online contact information*).

[82] *See* Common Sense Media (comment 20, 2012 SNPRM), at 7; Information Technology Industry Council (comment 51, 2012 SNPRM), at 2; Marketing Research Association (comment 62, 2012 SNPRM), at 3; Promotion Marketing Association (comment 77, 2012 SNPRM), at 8; TechAmerica (comment 87, 2012 SNPRM), at 5–6.

[83] *See, e.g.,* Promotion Marketing Association, *id.*

[84] *See* DMA (comment 28, 2012 SNPRM), at 16; ESA (comment 32, 2012 SNPRM), at 5; kidSAFE Seal Program (comment 56, 2012 SNPRM), at 5; NCTA (comment 69, 2012 SNPRM), at 4–5; Online

urged the Commission to refine the definition further, for example, by explicitly recognizing that the use of screen names for activities such as moderated chat will not be deemed as permitting ''direct contact'' with a child online and therefore will not require an operator using anonymous screen names to notify parents or obtain their consent.[85] Others suggested a return to the Commission's original definition of screen or user names, *i.e.,* only those that reveal an individual's online contact information (as newly defined).[86] Yet others hoped to see the Commission carve out from the definition of screen or user name uses to support an operator's internal operations (such as using screen or user names to enable moderated or filtered chat and multiplayer game modes).[87]

The Commission sees no need to qualify further the proposed description of *screen or user name.* The description identifies precisely the form of direct, private, user-to-user contact the Commission intends the Rule to cover—*i.e.,* ''online contact [that] can now be achieved via several methods besides electronic mail.'' [88] The Commission believes the description permits operators to use anonymous screen and user names in place of individually identifiable information, including use for content personalization, filtered chat, for public display on a Web site or online service, or for operator-to-user communication via the screen or user name. Moreover, the definition does not reach single log-in identifiers that permit children to transition between devices or access related properties across multiple platforms. For these reasons, the Commission modifies the definition of *personal information,* as proposed in the 2012 SNPRM, to include ''a screen or user name where it functions in the same manner as *online contact information,* as defined in this Section.''

b. *Persistent Identifiers* and *Support for Internal Operations*

Persistent identifiers have long been covered by the COPPA Rule, but only where they are associated with individually identifiable information.[89] In the 2011 NPRM, and again in the 2012 SNPRM, the Commission proposed broader Rule coverage of persistent identifiers.

First, in the 2011 NPRM, the Commission proposed covering persistent identifiers in two scenarios—(1) where they are used for functions other than or in addition to support for the internal operations of the Web site or online service, and (2) where they link the activities of a child across different Web sites or online services.[90] After receiving numerous comments on the proposed inclusion of persistent identifiers within the definition of *personal information,*[91] the Commission refined its proposal in the 2012 SNPRM.

In the Commission's refined proposal in the 2012 SNPRM, the definition of *personal information* would include a persistent identifier ''that can be used to recognize a user over time, or across different Web sites or online services, where such persistent identifier is used for functions other than or in addition to support for the internal operations of the Web site or online service.'' [92] The Commission also proposed to set forth with greater specificity the types of permissible activities that would constitute *support for internal operations.*[93] The proposed revision to this latter definition was intended to accomplish three goals: (1) To incorporate into the Rule text many of the types of activities—user authentication, maintaining user preferences, serving contextual advertisements,[94] and protecting against fraud or theft—that the Commission initially discussed as permissible in the 2011 NPRM; (2) to specifically permit the collection of persistent identifiers for functions related to site maintenance and analysis, and to perform network communications that many commenters viewed as crucial to their ongoing operations;[95] and (3) to make clear that none of the information collected may be used or disclosed to contact a specific individual, including through the use of behavioral advertising.[96]

Most of the commenters who responded to the 2012 SNPRM opposed the Commission's refinement. Many continued to argue, as they had done in response to the 2011 NPRM, that because persistent identifiers only permit contact with a device, not a specific individual, the Commission was exceeding its statutory authority by defining them as *personal information.*[97] Others argued strenuously for the benefits to children, parents, operators, and commerce of collecting anonymous information on, and delivering advertisements to, unknown or unnamed users.[98] Some commenters maintained that, to comply with COPPA's notice and consent requirements in the context of persistent identifiers, sites would be forced to collect more personal information on their users, contrary to COPPA's goals of data minimization.[99]

Because the proposed definition of persistent identifiers ran hand-in-hand with the proposed carve-out for

Publishers Association (comment 72, 2012 SNPRM), at 12; Toy Industry Association (comment 89, 2012 SNPRM), at 13; TRUSTe (comment 90, 2012 SNPRM), at 5–6.

[85] *See* Online Publishers Association (comment 72, 2012 SNPRM), at 12; TRUSTe TRUSTe (comment 90, 2012 SNPRM), at 5–6.

[86] *See* kidSAFE Seal Program (comment 56, 2012 SNPRM), at 5.

[87] *See* ESA (comment 32, 2012 SNPRM), at 5.

[88] *See* Common Sense Media (comment 20, 2012 SNPRM), at 7.

[89] *See* 16 CFR 312.2 of the existing Rule (paragraph (f), definition of *personal information*).

[90] *See* 2011 NPRM, 76 FR at 59812 (proposed definition of *personal information,* paragraphs (g) and (h)).

[91] Those comments are discussed in the 2012 SNPRM, 77 FR at 46647.

[92] *Id.*

[93] The proposed definition of *support for internal operations* was published at 77 FR 46648.

[94] Contextual advertising is ''the delivery of advertisements based upon a consumer's current visit to a Web page or a single search query, without the collection and retention of data about the consumer's online activities over time.'' *See* Preliminary FTC Staff Report, ''Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,'' (Dec. 2010), at 55 n.134, *available at http://ftc.gov/os/2010/12/101201privacyreport.pdf.* Such advertising is more transparent and presents fewer privacy concerns as compared to the aggregation and use of data across sites and over time for marketing purposes. *See id.*

[95] For example, the term ''personalize the content on the Web site or online service'' was intended to permit operators to maintain user-driven preferences, such as game scores, or character choices in virtual worlds.

[96] *Id.*

[97] 15 U.S.C. 6501(8)(F) defines personal information to include ''any other identifier that the Commission determines permits the physical or online contacting of a specific individual.'' *See, e.g.,* Gibson Dunn & Crutcher (comment 39, 2012 SNPRM), at 20 (''This expansion of the definition of 'personal information' is inconsistent with the text of COPPA, which limits 'personal information' to categories of information that *by themselves* can be used to identify and contact a specific individual. Every category of information that COPPA enumerates—name, physical address, email address, telephone number, and Social Security number—as well as the catch-all for 'any other identifier that the Commission determines permits the physical or online *contacting* of a specific individual,' 15 U.S.C. § 6501(8)(A)–(F)—is information that makes it possible to identify and contact a specific individual''); *see also* Business Software Alliance (comment 12, 2012 SNPRM), at 5–6; CTIA (comment 24, 2012 SNPRM), at 14–17; Chappell (comment 18, 2012 SNPRM), at 1; DMA (comment 28, 2012 SNPRM), at 10; Facebook (comment 33, 2012 SNPRM), at 9; Information Technology Industry Council (comment 51, 2012 SNPRM), at 2; Internet Commerce Coalition (comment 53, 2012 SNPRM), at 11–13; Microsoft (comment 66, 2012 SNPRM), at 3; NetChoice (comment 70, 2012 SNPRM), at 7; TechFreedom (comment 88, 2012 SNPRM), at 5–6.

[98] *See* Application Developers Alliance (comment 5, 2012 SNPRM), at 6; Business Software Alliance (comment 12, 2012 SNPRM), at 6); Information Technology and Innovation Foundation (comment 50, 2012 SNPRM), at 6–7; NetChoice (comment 70, 2012 SNPRM), at 6.

[99] Facebook (comment 33, 2012 SNPRM), at 9–10; Google (comment 41, 2012 SNPRM), at 5; J. Holmes (comment 47, 2012 SNPRM).

permissible activities, most commenters also opined on the proposed scope of the definition of *support for internal operations.*[100] Unsurprisingly, these commenters urged the Commission to broaden the definition either to make the list of permissible activities non-exhaustive,[101] or to clarify that activities such as ensuring legal and regulatory compliance, intellectual property protection, payment and delivery functions, spam protection, statistical reporting, optimization, frequency capping, de-bugging, market research, and advertising and marketing more generally would not require parental notification and consent on COPPA-covered sites or services.[102] Other commenters expressed confusion about which entities operating on or through a property could take advantage of the *support for internal operations* exemption.[103] Children's advocacy groups, by contrast, expressed fear that the proposed definition was already ''so broad that it could exempt the collection of many persistent identifiers used to facilitate targeted marketing.''[104]

Several commenters supported the Commission's premise that the collection of certain persistent identifiers permits the physical or online contacting of a specific individual, but asked the Commission to take a different tack to regulating such identifiers. Rather than cover all persistent identifiers and then carve out permissible uses, these commenters suggested a simpler approach: the Commission should apply the Rule only to those persistent identifiers used for the purposes of contacting a specific child, including through online behavioral advertising.[105]

The Commission continues to believe that persistent identifiers permit the online contacting of a specific individual. As the Commission stated in the 2011 NPRM, it is not persuaded by arguments that persistent identifiers only permit the contacting of a device.[106] This interpretation ignores the reality that, at any given moment, a specific individual is using that device. Indeed, the whole premise underlying behavioral advertising is to serve an advertisement based on the perceived preferences of the individual user.[107]

Nor is the Commission swayed by arguments noting that multiple individuals could be using the same device. Multiple people often share the same phone number, the same home address, and the same email address, yet Congress still classified these, standing alone, as ''individually identifiable information about an individual.'' [108] For these reasons, and the reasons stated in the 2011 NPRM, the Commission will retain persistent identifiers within the definition of personal information.

However, the Commission recognizes that persistent identifiers are also used for a host of functions that have little or nothing to do with contacting a specific individual, and that these uses are fundamental to the smooth functioning of the Internet, the quality of the site or service, and the individual user's experience. It was for these reasons that the Commission proposed to expand the definition of *support for internal operations* in the 2012 SNPRM.

The Commission has determined to retain the approach suggested in the 2011 NPRM and refined in the 2012 SNPRM, with certain revisions. First, the final Rule modifies the proposed definition of *persistent identifier* to cover ''a persistent identifier that can be used to recognize a user over time *and* across different Web sites or online services.'' This modification takes into account concerns several commenters raised that using a persistent identifier within a site or service over time serves an important function in conducting site performance assessments and supporting intra-site preferences.[109] However, in this context, not every Web site or service with a tangential relationship will be exempt—the term ''different'' means either sites or services that are unrelated to each other, or sites or services where the affiliate relationship is not clear to the user.[110]

Second, the Commission has determined that the carve-out for use of a persistent identifier to provide support for the internal operations of a Web site or online service is better articulated as a separate exception to the Rule's requirements. For this reason, it has amended Section 312.5(c) (''*Exceptions to prior parental consent*'') to add a new exception providing that where an operator collects only a persistent identifier for the sole purpose of providing support for its internal operations, the operator will have no notice or consent obligations under the Rule. This is a change in organization, rather than a substantive change, from the Commission's earlier proposals.

In addition, in response to the arguments made in a number of comments, the Commission has further modified the 2012 SNPRM proposed definition of *support for internal operations* to add frequency capping of advertising and legal or regulatory compliance to the permissible uses

---

[100] Association for Competitive Technology (comment 7, 2012 SNPRM), at 5; Business Software Alliance (comment 12, 2012 SNPRM), at 6–7; CTIA (comment 24, 2012 SNPRM), at 17–18; DMA (comment 28, 2012 SNPRM), at 10–12; Internet Commerce Coalition (comment 53, 2012 SNPRM), at 12; Microsoft (comment 66, 2012 SNPRM), at 3–5; NetChoice (comment 70, 2012 SNPRM), at 8–9.

[101] *See* DMA (comment 28, 2012 SNPRM), at 11 (warning that an exhaustive list is likely to have unintended consequences if companies are not afforded flexibility as technologies evolve); Digital Advertising Alliance (comment 27, 2012 SNPRM), at 3; Internet Commerce Coalition (comment 53, 2012 SNPRM), at 3–4, 12 (''[T]he definition of 'support for the internal operations' of a Web site is too narrow. * * * This list of 'exempt' collections is incomplete and risks quickly becoming outmoded.''); Magazine Publishers of America (comment 61, 2012 SNPRM), at 11; Online Publishers Association (comment 72, 2012 SNPRM), at 8; Promotion Marketing Association (comment 77, 2012 SNPRM), at 7; Computer and Communications Industry Association (comment 27, 2011 NPRM), at 4 (the exceptions are narrow and ''immobile short of another rulemaking'').

[102] *See, e.g.,* Association for Competitive Technology (comment 7, 2012 SNPRM), at 5; IAB (comment 49, 2012 SNPRM), at 4; TechFreedom (comment 88, 2012 SNPRM), at 11; Toy Industry Association (comment 89, 2012 SNPRM), at 15; Viacom Inc. (comment 95, 2012 SNPRM), at 13.

[103] CDT (comment 15, 2012 SNPRM), at 6–7; Google (comment 41, 2012 SNPRM), at 5; Toy Industry Association (comment 89, 2012 SNPRM), at 14.

[104] Institute for Public Representation (comment 52, 2012 SNPRM), at 13.

[105] *See* CDT (comment 15, 2012 SNPRM), at 6 (''We do, however, agree with the Commission that behavioral targeting of children using unique identifiers should trigger COPPA compliance obligations''); Internet Commerce Coalition (comment 53, 2012 SNPRM), at 12; *see also* AT&T (comment 8, 2011 NPRM), at 7; Future of Privacy Forum (comment 55, 2011 NPRM), at 2; WiredTrust (comment 177, 2011 NPRM), at 9; Visa Inc. (comment 168, 2011 NPRM), at 2.

[106] *See* 2011 NPRM, 76 FR at 59811.

[107] *See* J. Bowman, ''Real-time Bidding—How It Works and How To Use It,'' Warc Exclusive (Feb. 2011), *available at http://www.improvedigital.com/en/wp-content/uploads/2011/09/Warc-RTB-Feb11.pdf* (''With real-time bidding, advertisers can decide to put a specific ad in front of a specific individual web user on a given site, bid for that impression and—if they win the bid—serve the ad, all in the time it takes for a page to load on the target consumer's computer.''); L. Fisher, ''eMarketer's Guide to the Digital Advertising Ecosystem: Mapping the Display Advertising Purchase Paths and Ad Serving Process'' (Oct. 2012), *available at http://www.emarketer.com/Corporate/reports* (media buyers can deliver personalized, impression-by-impression, ads based on what is known about individual viewer attributes, behaviors, and site context).

[108] 15 U.S.C. 6501(8).

[109] *See* Toy Industry Association (comment 89, 2012 SNPRM), at 14; *see also* ESA (comment 32, 2012 SNPRM), at 8; NetChoice (comment 70, 2012 SNPRM), at 7–8.

[110] This interpretation of affiliate relationships is consistent with prior Commission articulations. *See* FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012), at 41–42, *available at http://ftc.gov/os/2012/03/120326privacyreport.pdf* (''The Commission maintains the view that affiliates are third parties, and a consumer choice mechanism is necessary unless the affiliate relationship is clear to consumers''); *see also* kidSAFE Seal Program (comment 56, 2012 SNPRM), at 5 (asking the Commission to clarify what is meant by the phrase '' 'across *different* Web sites or online services' in the context of persistent identifiers'').

enumerated therein.[111] The Commission declines to add certain other language proposed by commenters, such as intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging, because it believes that these functions are sufficiently covered by the definitional language permitting activities that ''maintain or analyze'' the functions of the Web site or service, or protect the ''security or integrity'' of the site or service. Under this revised definition, most of the activities that commenters cite to as important to permitting the smooth and optimal operation of Web sites and online services will be exempt from COPPA coverage.

The Commission also is cognizant that future technical innovation may result in additional activities that Web sites or online services find necessary to support their internal operations. Therefore, the Commission has created a voluntary process—new Section 312.12(b)—whereby parties may request Commission approval of additional activities to be included within the definition of *support for internal operations.* Any such request will be placed on the public record for notice and comment, and the Commission will act on it within 120 days.

The final amended language makes clear that operators may only engage in activities ''necessary'' to support the covered functions. The Commission agrees with commenter EPIC that ''[t]he presence of the word 'necessary' [in the statute] * * * indicates that the use of persistent identifiers is to be limited to the above activities, and that these activities are to be narrowly construed.'' [112] Moreover, operators may not use persistent identifiers that fall within the Rule's definition of *personal information* for any purposes other than those listed within the definition of *support for internal operations.* Accordingly, the Rule will require operators to obtain parental consent for the collection of persistent identifiers where used to track children over time and across sites or services. Without parental consent, operators may not gather persistent identifiers for the purpose of behaviorally targeting advertising to a specific child. They also may not use persistent identifiers to amass a profile on an individual child user based on the collection of such identifiers over time and across different Web sites in order to make decisions or draw insights about that child, whether that information is used at the time of collection or later.[113]

Several commenters sought clarification of whether a party's status as a first party or a third party would affect its ability to rely upon the *support for internal operations* definition.[114] To the extent that a child-directed content site or service engages service providers to perform functions encompassed by the definition of *support for internal operations,* those functions will be covered as support for the content-provider's internal operations. If a third party collecting persistent identifiers is deemed an *operator* under the Rule (*e.g.,* because it has actual knowledge it is collecting personal information from users of a child-directed site or service, or it has actual knowledge it is collecting personal information from a child through a general audience site or service), that operator may rely on the Rule's *support for internal operations* definition when it uses persistent identifier information for functions that fall within it.

c. Photographs, Videos, and Audio Files

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, in the 2011 NPRM, the Commission reevaluated the privacy and safety implications of such practices as they pertain to children. The Commission determined that the inherently personal nature of photographs, and the fact that they may contain information such as embedded geolocation data, or can be paired with facial recognition technology, makes them identifiers that ''permit the physical or online contacting of a specific individual.'' [115] The Commission found the same risks attendant with the online uploading of video and audio files.[116] Accordingly, the Commission proposed creating a new category within the definition of *personal information* covering a photograph, video, or audio file where such file contains a child's image or voice.

Some commenters supported this proposal. For example, the Institute for Public Representation, on behalf of a group of children's privacy advocates, stated that ''[b]ecause photographs, videos, and audio files can convey large amounts of information about children that can make them more vulnerable to behavioral advertising, and possibly put their personal safety at risk as well, these types of information should be included in the definition of personal information.''[117]

Several commenters criticized the Commission's proposal, claiming that the effect would limit children's participation in online activities involving ''user-generated content.'' [118] Several commenters issued blanket statements that photos, videos, and audio files, in and of themselves, do not permit operators to locate or contact a child.[119] Other commenters stated that the Commission's proposal is premature, arguing that facial recognition technologies are only in their nascent stages.[120] Finally, several commenters argued that the Commission should narrow the scope of its proposal, exempting from coverage photos, videos, or audio files that have been prescreened to remove any metadata or other individually identifiable information.[121] Others asked the Commission to carve out from coverage photos or videos where used to

[111] *See, e.g.,* Digital Advertising Alliance (comment 27, 2012 SNPRM), at 3; DMA (comment 28, 2012 SNPRM), at 11; IAB (comment 73, 2011 NPRM), at 10–11; Magazine Publishers of America (comment 61, 2012 SNPRM), at 11; Microsoft (comment 66, 2012 SNPRM), at 5; Online Publishers Association (comment 123, 2011 NPRM), at 4–5; Viacom Inc. (comment 95, 2012 SNPRM), at 14.

[112] *See* EPIC (comment 31, 2012 SNPRM), at 9. The Commission disagrees with the contention by certain commenters that the word ''necessary'' is confusing and unduly restrictive. *See* Online Publishers Association (comment 72, 2012 SNPRM), at 9. In this context, the term means that an operator may collect a covered persistent identifier if it uses it for the purposes listed in the definition of *support for internal operations.* The operator need not demonstrate that collection of the identifier was the only means to perform the activity.

[113] 144 Cong. Rec. S8482 (Statement of Sen. Bryan (1998)).

[114] *See, e.g.,* Association for Competitive Technology (comment 7, 2012 SNPRM), at 5; IAB (comment 73, 2011 NPRM), at 11.

[115] *See* 2011 NPRM, 76 FR at 59813.

[116] *Id.*

[117] Institute for Public Representation (comment 71, 2011 NPRM), at 33; Privacy Rights Clearinghouse (comment 131, 2011 NPRM), at 2.

[118] *See* DMA (comment 37, 2011 NPRM), at 17; Promotion Marketing Association (comment 133, 2011 NPRM), at 12; NCTA (comment 113, 2011 NPRM), at 16. Certain commenters interpreted the Commission's proposal as inapplicable to user-generated content, but applicable to an operator's own use of children's images or voices. *See* CTIA (comment 32, 2011 NPRM), at 12; National Retail Federation (comment 114, 2011 NPRM), at 4; F. Page (comment 124, 2011 NPRM).

[119] *See* American Association of Advertising Agencies (comment 2, 2011 NPRM), at 4; Internet Commerce Coalition (comment 74, 2011 NPRM), at 5; Promotion Marketing Association (comment 133, 2011 NPRM), at 12; *see also* DMA (comment 37, 2011 NPRM), at 17.

[120] *See* Intel Corp. (comment 72, 2011 NPRM), at 6–7; Motion Picture Association of America (''MPAA'') (comment 109, 2011 NPRM), at 13.

[121] *See* Privo (comment 76, 2012 SNPRM), at 7; DMA (comment 37, 2011 NPRM), at 17–18; Promotion Marketing Association (comment 133, 2011 NPRM), at 12; WiredSafety (comment 177, 2011 NPRM), at 10.

support internal operations of a site or service.[122] Commenter WiredSafety urged the Commission to adopt a standard that would permit operators to blur images of children before uploading them, thereby reducing the risks of exposure.[123]

The Commission does not dispute that uploading photos, videos, and audio files can be entertaining for children. Yet, it is precisely the very personal nature of children's photographic images, videos, and voice recordings that leads the Commission to determine that such files meet the standard for ''personal information'' set forth by Congress in the COPPA statute. That is, in and of themselves, such files ''*permit* the physical or online contacting of a specific individual.'' [124] As the Privacy Rights Clearinghouse stated, ''[a]s facial recognition advances, photos and videos have the potential to be analyzed and used to target and potentially identify individuals.'' [125] Given these risks, the Commission continues to believe it is entirely appropriate to require operators who offer young children the opportunity to upload photos, videos, or audio files containing children's images or voices to obtain parental consent beforehand.[126] Therefore, the Commission adopts the modification of the definition of *personal information* regarding photos, videos, and audio files as proposed in the 2011 NPRM, without qualification.

d. Geolocation Information

In the 2011 NPRM, the Commission stated that, in its view, existing paragraph (b) of the definition of *personal information* already covered any geolocation information that provides precise enough information to identify the name of a street and city or town.[127] However, because geolocation information can be presented in a variety of formats (*e.g.,* coordinates or a map), and in some instances can be more precise than street name and name of city or town, the Commission proposed making geolocation information a stand-alone category within the definition of *personal information.*[128]

Similar to the comments raised in response to the 2010 FRN, a number of commenters opposed this change. These commenters argued that anonymous, technical geolocation information, without the addition of any other identifier, was insufficient to contact an individual child.[129] The Internet Commerce Coalition stated that in identifying geolocation information ''sufficient to identify a street name and name of city or town'' as personal information, the Commission has missed the key to what makes an address ''personal,'' namely the street number.[130] Accordingly, such commenters asked the Commission to clarify that geolocation information will only be deemed personal information if, when combined with some other information or identifier, it would permit contacting an individual.[131]

These commenters overlook that the COPPA statute does not require the submission of a street number to make address information ''personal.'' Nor is it limited to home address, primary residence, or even a static address. Rather, Congress chose to use the words ''or other physical address, including street name and name of city or town.'' [132] This word choice not only permits the inclusion of precise mobile (*i.e.,* moving) location information, it may very well mandate it.[133] As commenter Consumers Union stated, ''[s]ince a child's physical address is already considered personal information under COPPA, geolocation data, which provides precise information about a child's whereabouts at a specific point in time, must also necessarily be covered.'' [134]

In addition, the Commission disagrees with those commenters who state that geolocation information, standing alone, does not permit the physical or online contacting of an individual within the meaning of COPPA.[135] Just as with persistent identifiers, the Commission rejects the notion that precise geolocation information allows only contact with a specific device, not the individual using the device. By that same flawed reasoning, a home or mobile telephone number would also only permit contact with a device.

Several commenters asked the Commission to refine the Rule's coverage of geolocation so that it targets particular uses. Commenter CTIA, citing photo-sharing services as an example, asked that geolocation information embedded in metadata (as often is the case with digital photographs) be excluded from the Rule's coverage.[136] Arguing that there should be a legal difference between using geolocation information for convenience or to protect a child's safety and to market to a child, commenter kidSAFE Seal Program suggested that geolocation data only be considered ''personal information'' when it is being used for marketing purposes.[137] Finally, commenter TRUSTe asked that the Commission amend the definition to cover ''precise geolocation data that can be used to identify a child's actual physical location at a given point in time.''[138]

The Commission sees no basis for making the suggested revisions. With respect to excluding geolocation

[122] ESA (comment 47, 2011 NPRM), at 14 n.21; kidSAFE Seal Program (comment 81, 2011 NPRM), at 11.

[123] *See* WiredSafety (comment 177, 2011 NPRM), at 10 (''the risk of using a preteen's clear image in still photos or in video formats is obvious''); *see also* Intel (comment 72, 2011 NPRM), at 7 (''we propose limiting the Commission's new definition to 'a photograph, video or audio file where such file contains a child's image or voice *which may reasonably allow identification of the child*' ''). The Commission believes that operators who choose to blur photographic images of children prior to posting such images would not be in violation of the Rule.

[124] 15 U.S.C. 6501(8)(F) (italics added).

[125] Privacy Rights Clearinghouse (comment 131, 2011 NPRM), at 2; *see also* TRUSTe (comment 164, 2011 NPRM), at 7 (''biometrics such as those provided in a photo, video or audio recording are personal information and greater protections need to be provided'').

[126] The Commission notes that this amendment would not apply to uploading photos or videos on general audience sites such as Facebook or YouTube, absent actual knowledge that the person uploading such files is a child.

[127] 76 FR at 59813.

[128] *Id.* Adding new paragraph (10) to the definition of *personal information* in 16 CFR 312.2.

[129] *See* AT&T (comment 8, 2011 NPRM), at 5; *see also* American Association of Advertising Agencies (comment 2, 2011 NPRM), at 4; CTIA (comment 32, 2011 NPRM), at 9; DMA (comment 37, 2011 NPRM), at 17; Promotion Marketing Association (comment 133, 2011 NPRM), at 13; Software & Information Industry Association (''SIIA'') (comment 150, 2011 NPRM), at 8; Verizon (comment 167, 2011 NPRM), at 6.

[130] *See* Internet Commerce Coalition (comment 74, 2011 NPRM), at 5; *see also* AT&T (comment 8, 2011 NPRM), at 5–6.

[131] *See, e.g.,* CTIA (comment 32, 2011 NPRM), at 9; Future of Privacy Forum (comment 55, 2011 NPRM), at 5; Verizon (comment 167, 2011 NPRM), at 6 (''Consistent with Congressional intent, geolocation information should be treated as personal information only when the data is tied to a specific individual.'').

[132] 15 U.S.C. 6501(8)(B).

[133] For this reason, the Commission finds those comments focusing on the potential to capture a large geographic area to be inapposite. *See* IAB (comment 73, 2011 NPRM), at 6 (''without an address or other additional data to identify a household or individual, a street name and city could encompass a large geographic area and as many as 1,000 households. For example, Sepulveda Boulevard, in the Los Angeles area, is over 40 miles long'').

[134] *See* Consumers Union (comment 29, 2011 NPRM), at 3; *see also* EPIC (comment 41, 2011 NPRM), at 8–9 (''As with IP addresses and user names, geolocation information can be used to track a particular device, which is usually linked to a particular individual.'').

[135] *See* American Association of Advertising Agencies (comment 2, 2011 NPRM), at 4; AT&T (comment 8, 2011 NPRM), at 6; DMA (comment 37, 2011 NPRM), at 17; Promotion Marketing Association (comment 133, 2011 NPRM), at 13; Verizon (comment 167, 2011 NPRM), at 6.

[136] CTIA (comment 32, 2011 NPRM), at 9.

[137] kidSAFE Seal Program (comment 81, 2011 NPRM), at 11.

[138] TRUSTe (comment 164, 2011 NPRM), at 3.

information in metadata, the Commission notes that in the 2011 NPRM, it specifically cited such geolocation metadata as one of the bases for including photographs of children within the definition of *personal information*.[139] With respect to the comment from kidSAFE Seal Program, the statute does not distinguish between information collected for marketing as opposed to convenience; therefore, the Commission finds no basis for making such a distinction for geolocation information. Finally, the Commission sees little to no practical distinction between ''geolocation data that can be used to identify a child's actual physical location at a given point in time'' and geolocation information ''sufficient to identify street name and name of a city or town,'' and it prefers to adhere to the statutory language. Accordingly, the Commission modifies the definition of *personal information* as proposed in the 2011 NPRM, and covered operators will be required to notify parents and obtain their consent prior to collecting geolocation information from children.

6. Definition of Release of Personal Information

In the 2011 NPRM, the Commission proposed to define the term *release of personal information* separately from the definition of *disclosure,* since the term applied to provisions of the Rule that did not solely relate to disclosures.[140] The Commission also proposed technical changes to clarify that the term ''release of personal information'' addresses business-to-business uses of personal information, not public disclosures, of personal information.[141] The Commission received little comment on this issue and therefore adopts the proposed changes.

7. Definition of Web Site or Online Service Directed to Children

In the 2012 SNPRM, the Commission proposed revising the definition of Web site or online service directed to children to allow a subset of sites falling within that category an option not to treat all users as children. The proposed revision was sparked by a comment from The Walt Disney Company that urged the Commission to recognize that sites and services directed to children fall along a continuum and that those sites targeted to both children and others should be permitted to differentiate among users. Noting that Disney's suggestion in large measure reflected the prosecutorial discretion already applied by the Commission in enforcing COPPA, the Commission proposed revisions to implement this concept. The Commission received numerous comments on this proposal. Although many commenters expressed support for the concept, the proposed implementing language was criticized.

Paragraphs (a) and (b) of the SNPRM's proposed revisions sought to define the subset of sites directed to children that would still be required to treat all users as children: those that knowingly target children under 13 as their primary audience, and those that, based on the overall content of the site, are likely to attract children under 13 as their primary audience. Paragraph (c) sought to describe those child-directed sites that would be permitted to age-screen to differentiate among users—namely those sites that, based on overall content, are likely to draw a disproportionate number of child users.

Although most commenters concurred that operators intentionally targeting children as their primary audience should be covered as Web sites directed to children,[142] some worried about the precise contours of the term ''primary audience'' and sought guidance as to percentage thresholds.[143] Some commenters also opposed any interpretation of COPPA that required child-directed Web sites to presume all users are children.[144]

Many commenters argued that the Commission exceeded its authority by defining *Web site or online service directed to children* based on criteria other than the sites' intent to target children. These commenters argued that Congress, by defining Web sites directed to children as those ''targeted'' to children, was imposing a subjective intent requirement.[145] The Commission disagrees. The Commission believes that if Congress had wanted to require subjective intent on the part of an operator before its site or service could be deemed *directed to children,* it would have done so explicitly.[146] Intent cannot be the only scenario envisioned by Congress whereby a site would be deemed directed to children.[147] Certainly, a Web site or online service that has the attributes, look, and feel of a property targeted to children under 13 will be deemed to be a site or service directed to children, even if the operator were to claim that was not its intent.

Paragraph (c) sought to describe those child-directed sites that would be permitted to age-screen to differentiate among users, namely those sites that, based on overall content, are likely to draw a disproportionate number of child users. While a handful of comments supported this definition,[148] for the most part, it was criticized by a spectrum of interests. On one side were advocates such Common Sense Media, EPIC, and the Institute for Public Representation. These advocates argued that recognizing a category of sites and services directed to mixed-audiences, targeted both to young children and others, would undercut the other revisions the Commission has proposed, thereby lessening privacy protections for children.[149] Such advocates also argued that the proposed category might create incentives, or loopholes, for operators that currently provide child-directed Web sites or services to claim their online properties are covered by paragraph (c) of the definition and become exempt from COPPA by age-gating.[150]

On the other side were a number of commenters who feared that the proposal would significantly expand the range of Web sites and online services that fall within the ambit of COPPA's coverage, including both teen-oriented and general-audience sites and services that incidentally appeal to children as well as adults. Much of this fear appears

[139] *See* 76 FR at 59813 n.87.

[140] *See* 2011 NPRM, 76 FR at 59804, 59809. The Commission originally proposed to define *release of personal information* as ''the sharing, selling, renting, or any other means of providing personal information to any third party.'' The Commission's revised definition removes the phrase ''or any other means of providing personal information'' to avoid confusion and overlap with the second prong of the definition of *disclosure* governing an operator making personal information collected from a child publicly available, *e.g.,* through a social network, a chat room, or a message board. *See* 16 CFR 312.2 (definition of *disclosure*).

[141] *Id.*

[142] *See* ACLU (comment 3, 2012 SNPRM), at 3; Online Publishers Association (comment 72, 2012 SNPRM), at 4.

[143] *See* DMA (comment 28, 2012 SNPRM), at 13–14; Institute for Public Representation (comment 52, 2012 SNPRM), at 25–27; Privo (comment 76, 2012 SNPRM), at 3; TechFreedom (comment 88, 2012 SNPRM), at 3; Toy Industry Association (comment 89, 2012 SNPRM), at 12; WiredTrust and WiredSafety (comment 98, 2012 SNPRM), at 3–4.

[144] *See* Facebook (comment 33, 2012 SNPRM), at 10; Viacom Inc. (comment 95, 2012 SNPRM), at 5.

[145] *See, e.g.,* Online Publishers Association (comment 72, 2012 SNPRM), at 4 (''The plain meaning of 'targeted' in this context requires a deliberate selection of an audience of children.'').

[146] *See* 15 U.S.C. 6501(10)(A) (''The term 'Web site or online service directed to children' means—(i) a commercial Web site or online service that is targeted to children; or (ii) that portion of a commercial Web site or online service that is targeted to children.'').

[147] *See* ACLU (comment 3, 2012 SNPRM), at 4 (''paragraphs (a) and (b) of the proposed definition are largely noncontroversial'').

[148] *See, e.g.,* U.S. Conference of Catholic Bishops (comment 92, 2012 SNPRM), at 4.

[149] Institute for Public Representation (comment 52, 2012 SNPRM), at (i).

[150] Common Sense Media (comment 20, 2012 SNPRM), at 9; EPIC (comment 31, 2012 SNPRM), at 4–5; Institute for Public Representation, *supra* note 149, at 27–28.

to have been driven by the specific language the Commission proposed; that is, sites or services that, based on their overall content, were ''likely to attract an audience that includes a disproportionately large percentage of children under age 13 as compared to the percentage of such children in the general population.'' Some argued that the use of the term ''disproportionate'' is vague,[151] potentially unconstitutional,[152] unduly expansive,[153] or otherwise constitutes an unlawful shift from the statute's actual knowledge standard for general audience sites to one of constructive knowledge.[154] Many worried that the Commission's proposal would lead to widespread age-screening, or more intensive age-verification, across the entire body of Web sites and online services located on the Internet.[155] Other commenters suggested that the Commission implement this approach through a safe harbor, not by revising a definition.[156]

The comments reflect a misunderstanding of the purpose and effect of the change proposed in the 2012 SNPRM. The Commission did not intend to expand the reach of the Rule to additional sites and services, but rather to create a new compliance option for a subset of Web sites and online services already considered *directed to children* under the Rule's totality of the circumstances standard.

To make clear that it will look to the totality of the circumstances to determine whether a site or service is directed to children (whether as its primary audience or otherwise), the Commission has revised and reordered the definition of *Web site or online service directed to children* as follows. Paragraph (1) of the definition contains the original Rule language setting forth several factors the Commission will consider in determining whether a site or service is directed to children. In addition, paragraph (1) amends this list of criteria to add musical content, the presence of child celebrities, and celebrities who appeal to children, as the Commission originally proposed in the 2011 NPRM.[157] Although some commenters expressed concern that these additional factors might capture general audience sites,[158] produce inconsistent results,[159] or be overly broad (since musicians and celebrities often appeal both to adults and children),[160] the Commission believes that these concerns are unfounded. The Commission reiterates that these factors are some among many that the Commission will consider in assessing whether a site or service is *directed to children,* and that no single factor will predominate over another in this assessment.

Paragraph (2) of the definition sets forth the actual knowledge standard for plug-ins or ad networks, as discussed in Part II.A.4.b herein, whereby a plug-in, ad network, or other property is covered as a Web site or online service directed to children under the Rule when it has actual knowledge that it is collecting personal information directly from users of a child-directed Web site or online service.

The Commission amends paragraph (3) of the definition to clarify when a child-directed site would be permitted to age-screen to differentiate among users. This paragraph codifies the Commission's intention to first apply its ''totality of the circumstances'' standard to determine whether any Web site or online service falling under paragraph (3) is *directed to children.* The Commission then will assess whether children under age 13 are the primary audience for the site or service. Paragraph (3) codifies that a site or service that is directed to children, but that does not target children as its primary audience, may use an age screen in order to apply all of COPPA's protections only to visitors who self-identify as under age 13. As the Commission stated in the 2012 SNPRM, at that point, the operator will be deemed to have actual knowledge that such users are under 13 and must obtain appropriate parental consent before collecting any personal information from them and must also comply with all other aspects of the Rule.[161]

The Commission retains its longstanding position that child-directed sites or services whose primary target audience is children must continue to presume all users are children and to provide COPPA protections accordingly.[162] Some commenters contend that the Commission should permit this presumption to be rebutted, even on sites primarily targeting children, by the use of a simple age screen that distinguishes child users from other users.[163] Although the Commission is now permitting this on sites or services that target children only as a secondary audience or to a lesser degree, the Commission believes adopting this standard for *all* child-directed sites would virtually nullify the statutory distinction between ''actual knowledge'' sites and those directed to children, creating a *de facto* actual knowledge standard for all operators.[164]

Finally, paragraph (4) of the definition restates the statutory proviso that a site or service will not be deemed to be child-directed where it simply links to a child-directed property.

*B. Section 312.4: Notice*

1. Direct Notice to a Parent

In the 2011 NPRM, the Commission proposed refining the Rule requirements for the direct notice to ensure a more effective ''just-in-time'' message to parents about an operator's information practices.[165] As such, the Commission proposed 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 the Rule requires. The proposed revised language of § 312.4 specified, in each instance where the Rule requires direct notice, the precise information that operators must provide to parents regarding the items of personal information the operator already has obtained from the child (generally, the

[151] *See, e.g.,* P. Aftab (comment 1, 2012 SNPRM), at 6–7; NCTA (comment 69, 2012 SNPRM), at 14; Marketing Research Association (comment 62, 2012 SNPRM), at 2; NetChoice (comment 70, 2012 SNPRM), at 4–5; SIIA (comment 84, 2012 SNPRM), at 10.

[152] *See, e.g.,* CDT (comment 15, 2012 SNPRM), at 7–10; Family Online Safety Institute (comment 34, 2012 SNPRM), at 3; Internet Commerce Coalition (comment 53, 2012 SNPRM), at 9; T. Mumford (comment 68, 2012 SNPRM); Online Publishers Association (comment 72, 2012 SNPRM), at 6; Viacom (comment 95, 2012 SNPRM), at 5.

[153] *See, e.g.,* DMA (comment 28, 2012 SNPRM), at 14; Magazine Publishers of America (comment 61, 2012 SNPRM), at 6–7.

[154] *See* CDT (comment 15, 2012 SNPRM), at 7.

[155] *See* ACLU (comment 3, 2012 SNPRM), at 5; DMA (comment 28, 2012 SNPRM), at 14–15; Magazine Publishers of America (comment 61, 2012 SNPRM), at 8; Toy Industry Association (comment 89, 2012 SNPRM), at 7, 11.

[156] Entertainment Software Association (comment 32, 2012 SNPRM), at 2; Online Publishers Association (comment 72, 2012 SNPRM), at 7–8; Viacom Inc. (comment 95, 2012 SNPRM), at 6.

[157] 2011 NPRM, 76 FR at 59814.

[158] *See* DMA (comment 37, 2011 NPRM), at 18–19; MPAA (comment 109, 2011 NPRM), at 19.

[159] *See* Verizon (comment 167, 2011 NPRM), at 10.

[160] *See* SIIA (comment 150, 2011 NPRM), at 9.

[161] *See* 2012 SNPRM, 77 FR at 46646.

[162] The Commission intends the word ''primary'' to have its common meaning, *i.e.,* something that stands first in rank, importance, or value. This must be determined by the totality of the circumstances and not through a precise audience threshold cut-off. *See* definition of ''primary.'' *Merriam-Webster.com* (2012), *available at http://www.merriam-webster.com* (last accessed Nov. 5, 2012).

[163] P. Aftab (comment 1, 2012 SNPRM), at 5; Facebook (comment 33, 2012 SNPRM), at 12–13; Future of Privacy Forum (comment 37, 2012 SNPRM), at 8.

[164] *See* DMA (comment 28, 2012 SNPRM), at 8 (an operator's choice of content serves as a proxy for knowledge that its users are primarily children under 13).

[165] *See* 2011 NPRM, 76 FR at 59816.

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 revisions also were intended to make clear that each form of direct notice must provide a hyperlink to the operator's online notice of information practices.[166]

In general, commenters supported the Commission's proposed changes as providing greater clarity and simplicity to otherwise difficult-to-understand statements.[167] These changes were viewed as especially important in an era of children's intense engagement with mobile applications accessed through a third-party app store and where an online notice might not be as readily accessible.[168] Only one commenter objected to the concept of placing greater emphasis on the direct, rather than the online, notice, stating that the changes would unduly necessitate lengthy direct notices and would prove overwhelming for parents and challenging to implement in the mobile environment.[169]

The Commission also proposed adding a paragraph setting out the contours of a new direct notice in situations where an operator voluntarily chooses to collect a parent's online contact information from a child in order to provide parental notice about a child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. The Commission's proposal for a voluntary direct notice in situations where an operator does not otherwise collect, use, or disclose personal information from a child garnered very little attention. Only one commenter sought clarification of the specific language the Commission proposed.[170]

Several commenters urged the Commission to use the occasion of the Rule review to develop a model COPPA direct notice form that operators voluntarily could adopt,[171] to mandate that such notifications be optimized for the particular devices on which they are displayed,[172] or to implement a Web site rating system.[173] The Commission believes that these suggestions are better suited as ''best practices'' [174] rather than as additions to the text of the Rule.

The Commission has determined to retain in the final Rule the modifications proposed in the 2011 NPRM. However, the Commission has reorganized the paragraphs to provide a better flow and guidance for operators, and has clarified that the voluntary direct notice provision described above is, indeed, voluntary for operators who choose to use it.[175]

2. Notice on the Web Site or Online Service

In the 2011 NPRM, the Commission proposed several changes to the Rule's online notice requirement. First, the Commission proposed requiring all operators collecting, using, or disclosing information on a Web site or online service to provide contact information, including, at a minimum, the operator's name, physical address, telephone number, and email address.[176] This proposal marked a change from the existing Rule's proviso that such operators could designate one operator to serve as the point of contact.

With the exception of the Institute for Public Representation,[177] commenters who spoke to the issue opposed mandating that the online notice list all operators. Some objected to the sheer volume of potentially confusing information this would present to parents,[178] and stated that the proposal provided no additional consumer benefit to parents, given that the existing Rule implies that the single operator designee should be prepared to ''respond to all inquiries from parents concerning the operators' privacy policies and use of children's information.'' [179] Some also spoke to the burden on the primary operator of having to maintain a current list of all applicable operators' contact information,[180] and expressed confusion as to which operators needed to be listed.[181]

The Commission believes that a requirement for the primary operator to provide specific, current, contact information for every operator that collects information on or through its Web site or service has the potential to confuse parents, for whom such online notices are intended to be accessible and useful. After considering the comments, the Commission has determined to retain the Rule's ''single operator designee'' proviso; that is, an operator will be required to list all operators collecting or maintaining personal information from children through the Web site or online service, but need only list the contact information for the one operator who will be responsible for responding to parents' inquiries.

In the 2011 NPRM, the Commission also proposed 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 Web site 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.[182] As a part of this revision, the Commission proposed removing the required statement 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.[183] This proposal was opposed by the Institute for Public Representation, which views the statement as a way to educate parents as to whether or not the operator actually complies with data minimization principles.[184] This organization also asked the Commission to require operators to disclose information to parents on how the data they collect is secured from potential breaches.[185] The Commission has considered this input but nevertheless adopts both of these changes in the final Rule.

The Commission sees great value for parents of streamlined online notices and continues to believe that the removal of extraneous information from such notices will further this goal.[186]

[166] *Id.*

[167] *See* EPIC (comment 41, 2011 NPRM), at 9; Institute for Public Representation (comment 71, 2011 NPRM), at 40–41; kidSAFE Seal Program (comment 81, 2011 NPRM), at 12; NCTA (comment 113, 2011 NPRM), at 22.

[168] AssertID (comment 6, 2012 SNPRM), at 2.

[169] IAB (comment 73, 2011 NPRM), at 13.

[170] N. Savitt (comment 142, 2011 NPRM), at 2.

[171] H. Valetk (comment 166, 2011 NPRM), at 3.

[172] TRUSTe (comment 164, 2011 NPRM), at 10.

[173] Lifelock (comment 93, 2011 NPRM), at 1.

[174] For example, to be considered by the various Commission-approved COPPA safe harbor programs.

[175] N. Savitt (comment 142, 2011 NPRM), at 2.

[176] *Id.*

[177] Institute for Public Representation (comment 71, 2011 NPRM), at 38–39.

[178] *See* Facebook (comment 50, 2011 NPRM), at 9; NCTA (comment 113, 2011 NPRM), at 22; Toy Industry Association (comment 89, 2012 SNPRM), at 6.

[179] IAB (comment 73, 2011 NPRM), at 12.

[180] DMA (comment 37, 2011 NPRM), at 20.

[181] kidSAFE Seal Program (comment 81, 2011 NPRM), at 12 (''Would this rule apply to one-time joint sponsors of a promotion who co-collect information on a Web site?'').

[182] 76 FR at 59815.

[183] *Id.*

[184] Institute for Public Representation (comment 71, 2011 NPRM), at 40.

[185] *Id.*

[186] *See* 2011 NPRM, 76 FR at 59815 (''In the Commission's experience, this blanket statement,

Continued

Accordingly, the Commission modifies the Rule as proposed in the 2011 NPRM to remove an operator's recitation in its online notice that it will not condition a child's participation on the provision of more information than is necessary. Again, however, the substantive requirement of § 312.7 remains in place.[187] In addition, and again in the interest of streamlining the online notices, the Commission declines to require operators to explain the measures they take to protect children's data. Nevertheless, the Rule's enhanced provisions on confidentiality and data security will help protect data collected from children online.

Finally, focusing on the part of the Commission's proposal that would require operators of general audience sites or services that have separate children's areas to post links to their notices of children's information practices on the home *or landing page or screen* of the children's area, the Toy Industry Association asked the Commission to forgo mandating links in any location where mobile apps can be purchased or downloaded because, in their view, changing commercial relationships may make it difficult to frequently update privacy policies in apps marketplaces.[188] The final amended Rule does not mandate the posting of such information at the point of purchase but rather on the app's home or landing screen. However, the Commission does see a substantial benefit in providing greater transparency about the data practices and interactive features of child-directed apps at the point of purchase and encourages it as a best practice.[189]

*C. Section 312.5: Parental Consent*

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.[190] ''Verifiable 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.'' [191] Accordingly, the Rule requires 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. § 312.5(b)(1).

The Rule sets forth a non-exhaustive list of methods that meet the standard of verifiable parental consent.[192] Specifically, paragraph (b)(2) states that methods to obtain verifiable parental consent that satisfy the requirements of the 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 email accompanied by a PIN or password obtained through one of the verification methods listed in the paragraph.[193]

Participants at the Commission's June 2, 2010 COPPA roundtable [194] and commenters to the 2010 FRN generally agreed that, while no one method provides complete certainty that the operator has reached and obtained consent from a parent, the methods listed in the Rule continue to have utility for operators and should be retained.[195]

A number of commenters urged the Commission to expand the list of acceptable mechanisms to incorporate newer technologies, or to otherwise modernize or simplify the Rule's mechanisms for parental consent.[196] Suggested methods of obtaining parental consent included sending a text message to the parent's mobile phone number,[197] offering online payment services other than credit cards,[198] offering parental controls in gaming consoles,[199] offering a centralized parental consent mechanism or parental opt-in list,[200] and permitting electronic signatures.[201]

In the 2011 NPRM, the Commission announced its determination that the record was sufficient to justify certain proposed mechanisms, but insufficient to adopt others. The 2011 NPRM proposed 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.

1. Electronic Scans and Video Verification

In the 2011 NPRM, the Commission proposed including electronically scanned versions of signed parental consent forms and the use of video verification methods among the Rule's non-exhaustive list of acceptable consent mechanisms. The proposal received support from several commenters, including Yahoo!, the DMA, kidSAFE Seal Program, the

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.'').

[187] *Id.*

[188] Toy Industry Association (Comment 163, 2011 NPRM), at 4.

[189] FTC Staff Report, ''Mobile Apps for Kids: Disclosures Still Not Making the Grade'' (Dec. 2012), at 7 (''Mobile Apps for Kids II Report''), *available at http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf* (noting that ''information provided prior to download is most useful in parents' decision-making since, once an app is downloaded, the parent already may have paid for the app and the app already may be collecting and disclosing the child's information to third parties'').

[190] Paragraph (a) of § 312.5 states that 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. 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.

[191] 15 U.S.C. 6501(9).

[192] *See* 16 CFR 312.5(b).

[193] Paragraph (b)(2) also sets out the sliding scale ''email plus'' method for obtaining parental consent in the instance where an operator collects a child's personal information only for *internal use.* The Commission's determination to retain the email plus method is discussed in Part II.C.7, *infra.*

[194] *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.*

[195] *See* DMA (comment 17, 2010 FRN), at 10, 12; Microsoft (comment 39, 2010 FRN), at 7; Toy Industry Association, Inc. (comment 63, 2010 FRN), at 3; WiredSafety.org. (comment 68, 2010 FRN), at 18.

[196] *See, e.g.,* BOKU (comment 5, 2010 FRN); DMA (comment 17, 2010 FRN), at 11–12; EchoSign, Inc. (comment 18, 2010 FRN); ESA (comment 20, 2010 FRN), at 7–9; Facebook (comment 22, 2010 FRN), at 2; J. Hiller (comment 27, 2010 FRN), at 447–50; M. Hoal (comment 30, 2010 FRN); Microsoft (comment 39, 2010 FRN), at 4; MPAA (comment 42, 2010 FRN), at 12; RelyID (comment 53, 2010 FRN), at 3; TRUSTe (comment 64, 2010 FRN), at 3; H. Valetk (comment 66, 2010 FRN), at 6; WiredSafety.org (comment 68, 2010 FRN), at 7; S. Wittlief (comment 69, 2010 FRN).

[197] *See* BOKU (comment 5, 2010 FRN); ESA (comment 20, 2010 FRN), at 11–12; TRUSTe (comment 64, 2010 FRN), at 3; H. Valetk (comment 66, 2010 FRN), at 6–7.

[198] *See* WiredSafety.org (comment 68, 2010 FRN), at 24 (noting that operators are considering employing online financial accounts, such as iTunes, for parental consent).

[199] *See* ESA (comment 20, 2010 FRN), at 9–10; Microsoft (comment 39, 2010 FRN), at 7.

[200] *See* ESA (comment 20, 2010 FRN), at 12; Janine Hiller (comment at 27, 2010 FRN), at 447.

[201] *See* DMA (comment 17, 2010 FRN), at 12; EchoSign (comment 18, 2010 FRN); ESA (comment 20, 2010 FRN), at 10; Toy Industry Association (comment 63, 2010 FRN), at 11.

NCTA, and Facebook.[202] Other commenters expressed reservations about whether these new methods would offer practical, economical, or scalable solutions for operators.[203]

As stated in the 2011 NPRM, the Commission finds that electronic scans and video conferencing are functionally equivalent to the written and oral methods of parental consent originally recognized by the Commission in 1999. It does not find the concerns of some commenters, that operators are not likely to widely adopt these methods, a sufficient reason to exclude them from the Rule. The list of consent mechanisms is not exhaustive and operators remain free to choose the ones most appropriate to their individual business models. Therefore, Section 312.5(b) of the final Rule includes electronic scans of signed consent forms and video-conferencing as acceptable methods for verifiable parental consent.

2. Government-Issued Identification

The Commission also proposed in the 2011 NPRM to allow 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 from the operator's records promptly after such verification is complete. Some operators already use this method of obtaining parental consent, and it is one of several available verification methods offered by the COPPA safe harbor program Privo.[204] In the NPRM, the Commission stated its recognition that information such as Social Security number, driver's license number, or another record of government-issued identification is sensitive data.[205] In permitting operators to use government-issued identification as an approved method of parental verification, the Commission emphasized the importance of limiting the collection of such identification information to only those segments of information needed to verify the data.[206] For example, the Commission noted that the last four digits of a person's Social Security number are commonly used by verification services to confirm a person's identity.[207] The Commission also stated its belief that the requirement that operators immediately delete parents' government-issued identification information upon completion of the verification process provides further protection against operators' unnecessary retention, use, or potential compromise of such information. Commenters in favor of adding this mechanism pointed out that using available technology to check a driver's license number or partial Social Security number reasonably ensures that the person providing consent is the parent.[208]

Other commenters expressed concern that allowing operators to collect sensitive government identification information from parents raises serious privacy implications.[209] Many commenters opined that the serious risks to parents' privacy outweighed the benefits of the proposal.[210] Some further argued that normalizing the use of this sensitive data for such a purpose would diminish users' alertness against identity theft schemes and other potentially nefarious uses.[211]

As the federal agency at the forefront of improving privacy protections for consumers, the Commission is sensitive to the privacy concerns raised by the comments. The Commission is also aware that both operators and parents benefit from having a choice of several acceptable methods for verifiable parental consent. Moreover, the Commission is not compelling any operator to use this method. The Commission believes that, on balance, government-issued ID provides a reliable and simple means of verifying that the person providing consent is likely to be the parent, and that the requirement that operators delete such data immediately upon verification substantially minimizes the privacy risk associated with that collection. Therefore, the Commission adopts this method among the Rule's non-exhaustive list of acceptable consent methods.[212]

3. Credit Cards

The 2011 NPRM also proposed including the term ''monetary'' to modify ''transaction'' in connection with use of a credit card to verify parental consent. This added language was 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.[213] The Commission received one comment specifically addressing this proposed language; EPIC supported the change as correctly limiting the circumstances under which

[202] *See* Yahoo! (comment 80, 2011 NPRM), at 4; DMA (comment 37, 2011 NPRM), at 23; kidSAFE Seal Program (comment 81, 2011 NPRM), at 16; NCTA (comment 113, 2011 NPRM), at 9; Facebook (comment 50, 2011 NPRM), at 8–9.

[203] *See* K. Dennis (comment 34, 2011 NPRM), at 2; A. Thierer (comment 162, 2011 NPRM), at 9; R. Newton (comment 118, 2011 NPRM).

[204] *See* application of Privo, Inc. to become a Commission-approved COPPA safe harbor program (Mar. 2004), *available at http://www.ftc.gov/os/2004/04/privoapp.pdf*, at 25.

[205] 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* FTC Staff Report, ''Self-Regulatory Principles for Online Behavioral Advertising'' (Feb. 2009), at 20 n.47, 42, 44, *available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf*.

[206] 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 at 59905. There, the Commission concluded that the use of a driver's license was an acceptable method of parental verification.

[207] *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*.

[208] For instance, Facebook commented that this mechanism achieves the delicate balance of making it easy for the parent to provide consent, while making it difficult for the child to pose as the parent; when combined with responsible data disposal practices, this method also protects the parent's information against unauthorized use or disclosure. *See* Facebook (comment 50, 2011 NPRM), at 9; *see also* kidSAFE Seal Program (comment 81, 2011 NPRM), at 16.

[209] Intel and the Marketing Research Association cautioned the Commission to avoid sending mixed messages about using such sensitive information while at the same time advising operators to adhere to principles of data minimization. Intel (comment 72, 2011 NPRM), at 7; Marketing Research Association (comment 97, 2011 NPRM), at 3.

[210] *See* Institute for Public Representation (comment 71, 2011 NPRM), at 42; *see also* TechFreedom (comment 159, 2011 NPRM), at 8 (requiring users to go through an age verification process would lead to a loss of personal privacy); New York Intellectual Property Law Association (comment 117, 2011 NPRM), at 3 (parents' privacy rights should not needlessly be put at risk in order to protect their children's privacy).

[211] *See* CDT (comment 17, 2011 NPRM), at 9; A. Thierer (comment 162, 2011 NPRM), at 8.

[212] kidSAFE Seal Program asked the Commission to consider whether operators can retain parents' verification information as proof that the verification occurred. *See* kidSAFE Seal Program (comment 81, 2011 NPRM), at 16. With regard to credit card information or government-issued identifiers, the Commission would consider whether an operator had retained a sufficiently truncated portion of the data as to make it recognizable to the parent but unusable for any other purpose.

[213] *See* 71 FR at 13247, 13253, 13254 (Mar. 15, 2006) (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*.

credit cards can be used as verification. The final Rule incorporates this change, stating ''credit card in connection with a monetary transaction.'' [214]

4. Alternative Online Payment Systems

At the outset of the Rule review, the Commission sought comment on whether to consider modifying the Rule to include alternative online payment systems, in addition to credit cards, as an acceptable means of verifying parental consent in connection with a monetary transaction. The Commission stated in the 2011 NPRM that, at such time, the record was insufficient to support a proposal to permit the use of alternative online payment systems for this purpose. The NPRM also indicated that the Commission was 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). Thus, the Commission welcomed further discussion of the risks and benefits of using electronic payment methods as a consent mechanism.

Several commenters to the 2011 NPRM asked the Commission to reconsider its position that online payment systems are not yet reliable enough to provide verifiable parental consent, arguing that certain online payment options can meet the same stringent criteria as credit cards.[215] In particular, Scholastic stressed the importance to operators, particularly in the context of digital apps and other downloadable content, of providing customers the flexibility to use various convenient electronic payment methods. Scholastic urged the Commission to amend the Rule to provide that payment methods other than credit cards, such as debit cards and electronic payment systems, can satisfy the Rule's consent mechanism requirements if they provide separate notification of each discrete monetary transaction to the primary account holder.[216]

The Commission, upon review of all of the relevant comments, is persuaded that it should allow the use of other payment systems, in addition to credit cards, provided that any such payment system can meet the same stringent criteria as a credit card. As Scholastic articulated in its comment, the Rule should allow operators to use any electronic or online payment system as an acceptable means of obtaining verifiable parental consent in connection with a monetary transaction where (just as with a credit card) the payment system is used in conjunction with a direct notice meeting the requirements of § 312.4(c) and the operator provides notification of each discrete monetary transaction to the primary account holder. Accordingly, § 312.5(b)(2) of the final Rule includes the following language ''requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder.''

5. Electronic or Digital Signatures

In response to the 2010 FRN, several commenters recommended that the Commission accept electronic or digital signatures as a form of verifiable consent.[217] In the 2011 NPRM, the Commission concluded that the term ''electronic signature'' has many meanings, ranging 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,'' [218] to an electronic image of the stylized script associated with a person. The Commission determined that electronic signatures, without more indicia of reliability, were problematic in the context of COPPA's verifiable parental consent requirement.[219] The NPRM welcomed further comment on how to enhance the reliability of these convenient methods.

In commenting on the 2011 NPRM, several commenters asked the FTC to reconsider the utility of electronic signatures in the online world.[220] The Commission has determined not to include electronic or digital signatures within the non-exhaustive list of acceptable consent mechanisms provided for in § 312.5, given the great variability in the reliability of mechanisms that may fall under this description. For instance, the Commission believes that simple digital signatures, which only entail the use of a finger or stylus to complete a consent form, provide too easy a means for children to bypass a site or service's parental consent process, and thus do not meet the statutory standard of ''reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.'' [221] However, the Rule would not prohibit an operator's acceptance of a digitally signed consent form where the signature provides other indicia of reliability that the signor is an adult, such as an icon, certificate, or seal of authenticity that accompanies the signature. At the same time, the Commission does not seek to limit or proscribe other types of digital signatures that may also meet the statutory standard. For these reasons, digital or electronic signatures are not included within the Rule's non-

[214] *But see* Part II.C.4., *infra.* Several comments note that some alternative payment systems, such as the use of a username and password in the iTunes store, afford equal notice and protections to parents for both paid and unpaid transactions by providing the primary account holder with a separate, contemporaneous notification of each discrete transaction.

[215] *See, e.g.,* Association for Competitive Technology (comment 5, 2011 NPRM), at 7; DMA (comment 37, 2011 NPRM), at 23; eBay (comment 40, 2011 NPRM), at 3–4; kidSAFE (comment 81, 2011 NPRM), at 16; Scholastic (comment 144, 2011 NPRM), at 9–10.

[216] Other commenters similarly urged that the Rule permit the use of alternate payment systems, where such systems are tied to a valid credit card account, require the user to enter a password, and provide the primary account holder with clear notification of each transaction through email confirmation. *See* Association for Competitive Technology (comment 5, 2011 NPRM), at 7; kidSAFE (comment 81, 2011 NPRM), at 16; *see also* eBay (comment 40, 2011 NPRM), at 3–4 (indicating its interest in leveraging PayPal business model to implement a youth account program directly linking children's accounts to verified parent accounts).

[217] *See* DMA (comment 17, 2010 FRN), at 12; EchoSign (comment 18, 2010 FRN); ESA (comment 20, 2010 FRN), at 10; Toy Industry Association (comment 63, 2010 FRN), at 11. For instance, the ESA proposed that the Commission incorporate a ''sign and send'' method, given that numerous commonly available devices allow users to input data by touching or writing on the device's screen.

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

[219] *See* 2011 NPRM at 59818. (The Commission indicated several concerns about allowing electronic signatures, including that, given the proliferation of mobile devices among children and the ease with which children could sign and return an on-screen consent, such mechanisms may not ''ensure that the person providing consent is the child's parent.'' The Commission also noted that, although the law recognizes electronic signatures for the assertion that an individual signed a document, they do not necessarily confirm the underlying identity of the individual signing the document).

[220] *See, e.g.,* DMA (comment 37, 2011 NPRM), at 23 (Congress passed ESIGN Act over a decade ago and consumers prefer completing transactions online with digital signatures over using cumbersome offline processes); ESA (comment 47, 2011 NPRM), at 22–23 (electronic sign-and-send method meets the statutory standard of ''reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent,'' while accommodating parents' use of tablet, mobile device, and small-screen technologies lacking computer peripherals such as printers or scanners); TechFreedom (comment 159, 2011 NPRM), at 8 (urging Commission to promote development of solutions such as electronic signatures now, rather than wait for next Rule revision).

[221] While the Commission recognizes that some children also may circumvent the Rule's parental notice and consent mechanisms by signing and sending parental consent forms through mail, fax, or electronic scan, it believes these methods clearly are not as simple for the child as using a computer or handheld device to instantly pen and send a signature.

exhaustive list of parental consent mechanisms.

6. Platform Methods of Parental Consent

In response to the 2010 FRN, several commenters asked the Commission to consider whether, and in what circumstances, parental control features in game consoles, and presumably other devices, could be used to provide notice to parents and obtain verified consent under COPPA.[222] In the 2011 NPRM, the Commission acknowledged that parental control features can offer parents a great deal of control over a child's user experience and can serve as a *complement* to COPPA's parental consent requirements. However, the Commission concluded that, at that time, it did not appear that any such systems were adequately designed to comply with COPPA, and that the record was insufficient for it to determine whether a hypothetical parental consent mechanism would meet COPPA's verifiable parental consent standard. The Commission, in the 2011 NPRM, encouraged continued exploration of the concept of using parental controls in gaming consoles and other devices to notify parents and obtain their prior verifiable consent.[223]

In response to both the 2011 NPRM and the 2012 SNPRM, numerous stakeholders, including several platform providers, Web site and app developers, and child and privacy advocates, asked the Commission to consider modifications to the Rule to make clear that operators can choose to use a common mechanism—administered by a platform, gaming console, device manufacturer, COPPA safe harbor program,[224] or other entity—for the purpose of providing notice and obtaining parental consent for multiple operators simultaneously.[225]

Commenters offered a variety of proposals. For instance, several commenters envisioned that platform providers could provide a general notice and obtain consent to collect personal information for those purposes specified in the general notice, and that app developers wanting to collect or use information in ways differing from the general notice would need to independently provide a second separate notice to parents and obtain their consent.[226] Facebook proposed that operators may also use such common consent mechanisms to meet other COPPA obligations, such as providing parental access to children's data collected by operators.[227] The Walt Disney Company proposed two possible mechanisms: a '' 'Kids Privacy Portal'—through which parents can express privacy preferences in one place for multiple online activities,'' or a joint agreement between the platform operator and application providers ''that determines how data will be collected and used, and how parents exercise control.'' [228] The Entertainment Software Association (''ESA'') proposed a similar program for video game platforms whereby consoles or hand-held device makers could leverage their existing parental controls technologies.[229]

Commenters cited several potential benefits of common consent mechanisms, including: (1) Encouraging the development of interactive content for children by easing the burden individualized notice and consent places on operators, especially in the context of mobile apps [230]; (2) focusing parental attention on one streamlined notice rather than on multiple, confusing, notices [231]; and (3) promoting privacy by eliminating the need for each of these other operators to separately collect online contact information from the child in order to obtain parental consent.[232] The Center for Democracy and Technology acknowledges that, while not all parents may want to delegate to platforms the authority to get consent on behalf of individual operators, ''others may want to empower their kids to share and obtain information through certain applications without being forced to sign off on every interaction with a new web service.'' [233]

The Commission believes that common consent mechanisms, such as a platform, gaming console, or a COPPA safe harbor program, hold potential for the efficient administration of notice and consent for multiple operators. A well-designed common mechanism could benefit operators (especially smaller ones) and parents alike if it offers a proper means for providing notice and obtaining verifiable parental consent, as well as ongoing controls for parents to manage their children's accounts.[234] The Commission believes

[222] *See* ESA (comment 20, 2010 FRN), at 4; Microsoft (comment 39, 2010 FRN), at 7.

[223] 2011 NPRM, 76 FR 59818 (Sept. 27, 2011), *available at http://ftc.gov/os/2011/09/110915coppa.pdf.*

[224] The Commission notes that Privo, Inc., one of the approved COPPA safe harbors, offers the option to its members to have Privo administer notice and consent programs for member operators.

[225] *See, e.g.,* P. Aftab (comment 1, 2012 SNPRM), at 7; Association for Competitive Technology (comment 5, 2011 NPRM), at 7–8 and (comment 7, 2012 SNPRM), at 8; Computer and Communications Industry Association (''CCIA'') (comment 27, 2011 NPRM), at 7–8; CDT (comment 15, 2012 SNPRM), at 5–6; Connect Safely (comment 21, 2012 SNPRM), at 3; ESA (comment 47, 2011 NPRM), at 21–26; Facebook (comment 33, 2012 SNPRM), at 18–20; Future of Privacy Forum (comment 55, 2011 NPRM), at 5–6 and (comment 37, 2012 SNPRM), at 3–6; Microsoft (comment 107, 2011 NPRM), at 13–15 and (comment 66, 2012 SNPRM), at 6; Novachi, Inc. (comment 119, 2011 NPRM); SIIA (comment 150, 2011 NPRM), at 10–12; TechFreedom (comment159, 2011 NPRM), at 7 and (comment 88, 2012 SNPRM), at 13; The Walt Disney Co. (comment 170, 2011 NPRM), at 17–19.

[226] *See, e.g.,* Association for Competitive Technology (comment 5, 2011 NPRM), at 7–8 and (comment 7, 2012 SNPRM), at 8; CCIA (comment 27, 2011 NPRM), at 7–8; Facebook (comment 33, 2012 SNPRM), at 18–20; Future of Privacy Forum (comment 55, 2011 NPRM), at 5–6 and (comment 37, 2011 SNPRM), at 3–6; Microsoft (comment 107, 2011 NPRM), at 13–15 and (comment 66, 2012 SNPRM), at 13; SIIA (comment 150, 2011 NPRM), at 10–12. Future of Privacy Forum's 2012 comment included proposed Rule language. *See also* NetChoice (comment 70, 2012 SNPRM), at 12 (proposing Rule language to clarify that COPPA allows for the use of common consent mechanisms).

[227] Facebook (comment 33, 2012 SNPRM), at 18–19.

[228] The Walt Disney Co. (comment 170, 2011 NPRM), at 18.

[229] ESA contemplates that the platforms would provide a notice ''that makes it clear that the child's personal information will be disclosed to third-party game publishers and application providers who may collect, use, and disclose such information through the console or handheld in order to provide a joint or related service,'' and that parental consent ''might be effective across any of the console or handheld maker's related video game platforms and Web sites clearly referenced in the console or handheld maker's privacy policy.'' ESA (comment 47, 2011 NPRM), at 26. Other proposals for common consent mechanisms included outsourcing the process to identity management services, which operators could access through open technology standards. *See* Novachi (comment 119, 2011 NPRM). CDT acknowledged the potential utility of platform-based outsourcing notice and consent, provided that the Commission required additional safeguards for common consent mechanisms, including parental controls for the *ongoing* management of consent. CDT (comment 15, 2012 SNPRM), at 5–6.

[230] *See, e.g.,* CCIA (comment 27, 2011 NPRM), at 7–8 (stating that platform-based consent programs would ''promote COPPA's goals'' by encouraging developers ''who do not have the resources to independently acquire verifiable parental consent'' to create content and services for children; *see also* ConnectSafely.org (comment 21, 2012 SNPRM), at 3; P. Aftab (comment 1, 2012 SNPRM), at 7; Tech Freedom (comment 159, 2011 NPRM), at 7.

[231] For example, Microsoft stated that common consent mechanisms ''would benefit parents because requiring each third party separately to obtain parental consent could be confusing, overwhelming, and costly for parents.'' Microsoft (comment 66, 2012 SNPRM), at 6.

[232] Microsoft, *id.; see also* CCIA (comment 27, 2011 NPRM), at 8; Facebook (comment 33, 2012 SNPRM), at 19 (''A rule that enables operators to leverage a common platform for notice and consent would substantially advance the Commission's goal of ensuring that parents receive clear, understandable, and manageable information; it would also minimize the practical and economic costs to parents as a result of multiple consent requests.''); TechAmerica (comment 87, 2012 SNPRM), at 8.

[233] CDT (comment 15, 2012 SNPRM), at 6.

[234] Under the system proposed by the Future of Privacy Forum, parents would be apprised of a common set of information practices to which they could consent on an aggregate basis, then would

Continued

that such methods could greatly simplify operators' and parents' abilities to protect children's privacy.

Despite the potential benefits, the Commission declines, at this time, to adopt a specific provision for the following reasons. First, even without an express reference in the Rule to such a process, nothing forecloses operators from using a common consent mechanism so long as it meets the Rule's basic notice and consent requirements.[235] Second, the Commission did not specifically seek comment on this precise issue; nor has it proposed any language in either the NPRM or the SNPRM to address this point. Accordingly, the Commission is reluctant to adopt specific language without the benefit of notice and comment on such language to explore all potential legal and practical challenges of using a common consent mechanism.[236] Finally, the Commission believes that parties interested in using a common consent mechanism have the option to participate in the voluntary Commission approval process set forth in Section 312.5(3) of the final Rule.[237] That process would enable the Commission to evaluate, and other interested parties to publicly comment upon, such proposals in an effort to bring to market sound and practical solutions that will serve a broad base of operators.

7. The Sliding Scale (''Email Plus'') Method

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.[238] 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.[239] Such an additional step has 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.[240] The purpose of the additional step is to provide greater assurance that the person providing consent is, in fact, the parent. This consent method is often called ''email plus.'' [241]

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.[242] However, it believed that this lower cost option was acceptable as a temporary option, in place until the Commission determined that more reliable (and affordable) consent methods had adequately developed.[243] In 2006, the Commission extended use of the sliding scale indefinitely, stating that the agency would continue to monitor technological developments and modify the Rule should an acceptable electronic consent technology develop.[244]

Email plus has enjoyed wide appeal among operators, who credit its simplicity.[245] The Commission sought comment in response to the 2010 FRN and at the June 2010 public roundtable on whether to retain email plus in the final Rule. Numerous commenters to the 2010 FRN, including associations who represent operators, supported the continued retention of this method as a low-cost means to obtain parents' consent.[246] 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 a child provides 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.[247]

In the 2011 NPRM, the Commission proposed eliminating email plus as a means of obtaining parental consent. The Commission considered whether operators' continued reliance on email plus may have inhibited the development of more reliable methods of obtaining verifiable parental consent. The Commission also made clear that, 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.

Several commenters supported the Commission's proposal to eliminate email plus. These commenters opined that children can easily circumvent email plus and thus, that it is not

receive individualized notices for additional practices that go beyond those outlined in the common notice. The platform would also ensure that parents have access to easy mechanisms through which to retract their consent to the child's use of any particular site or service. Future of Privacy Forum (comment 37, 2012 SNPRM), at 4–6.

[235] As noted in note 219, *supra,* one such common consent mechanism is currently provided by an approved COPPA safe harbor, and there may be others already in operation as well.

[236] The Commission would want to explore further the difficulties of making sure the notice accurately reflects each individual operator's information practices; how to provide parents with a means to access the operator's privacy policy with regard to information collected from children; and giving parents controls sufficient to refuse to permit an operator's further use or future collection of their child's personal information, and to direct the operator to delete the child's personal information and or disable the child's account with that operator.

[237] *See* Part II.C.8., *infra.*

[238] *See* 2010 Rule Review, *supra* note 6, at 17091.

[239] The sliding scale approach was adopted in the Rule in response to comments that stated that internal uses of information, such as marketing to children, presented less risk than external disclosures of the information to third parties or through public postings. *See* 1999 Statement of Basis and Purpose, 64 FR at 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.

[240] The Commission notes that, assuming an operator has obtained a parent's mobile phone number from the parent in response to the first email, confirmation of a parent's consent may done via an SMS or MMS text to the parent.

[241] By contrast, for uses of personal information that involve disclosing the information to the public or third parties, the Rule requires operators to use more reliable methods of obtaining verifiable parental consent, including but not limited to those identified in § 312.5(b)(1).

[242] 64 FR at 59902 (''[E]mail alone does not satisfy the COPPA because it is easily subject to circumvention by children.'').

[243] *See id.* at 59901 (''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.'').

[244] *See* 71 FR at 13247, 13255, 13254 (Mar. 15, 2006).

[245] *See* WiredSafety.org (comment 68, 2010 FRN), 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.'').

[246] *See* R. Newton, 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;* DMA (comment 17, 2010 FRN), at 10; IAB (comment 34, 2010 FRN), at 2; R. Newton (comment 46, 2010 FRN), at 3; PMA (comment 51, 2010 FRN), at 4–5; Toy Industry Association, Inc. (comment 63, 2010 FRN), at 8.

[247] *See* Privo, Inc. (comment 50, 2010 FRN), 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, 2010 FRN), 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.''); *see also* D. Tayloe and P. Spaeth, Remarks from Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online, at 215–17 (email plus is very unreliable).

sufficiently effective to meet the statutory requirement of being reasonably calculated to ensure that it is the parent providing consent.[248] Some of these commenters also echoed the Commission's concern that operators' continued reliance on email plus is a disincentive to innovation.[249]

A majority of the comments, however, strongly urged the Commission to retain email plus.[250] Several commenters indicated that email plus remains a widely used and valuable tool for communicating with parents and obtaining consent. These commenters maintained that email plus is easy for companies and parents to use, easy to understand, effective, and affordable.[251] In addition, several commenters expressed concern that other approved methods for obtaining consent would impose significant burdens on operators and parents.[252] Commenters also questioned whether other methods for verifiable parental consent are any more reliable than email plus.[253] Finally, several commenters challenged the FTC's assumption that eliminating email plus would spur further innovation in parental consent mechanisms.[254]

The Commission is persuaded by the weight of the comments that email plus, although imperfect, remains a valued and cost-effective consent mechanism for certain operators. Accordingly, the final Rule retains email plus as an acceptable consent method for operators collecting personal information only for *internal* use. Nevertheless, the Commission continues to believe that email plus is less reliable than other methods of consent, and is concerned that, twelve years after COPPA became effective, so many operators rely upon what was supposed to be a temporary option. The Commission is also concerned about perpetuating for much longer a distinction between internal and external uses of personal information that the COPPA statute does not make. Thus, the Commission strongly encourages industry to innovate to create additional useful mechanisms as quickly as possible.

8. Voluntary Process for Commission Approval of Parental Consent Mechanisms

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.'' [255] The Rule thus 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, the recent Rule review process revealed that, whether out of concern for potential liability, ease of implementation, or lack of technological developments, operators have been reluctant to utilize consent methods other than those specifically set forth in the Rule.[256] As a result, little technical innovation in the area of parental consent has occurred.

To encourage the development of new consent mechanisms, and to provide transparency regarding consent mechanisms that may be proposed, the Commission in the 2011 NPRM proposed establishing 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 its filing.

The NPRM stated the Commission's belief that this new approval process, aided by public input, would allow the Commission to give careful consideration, on a case-by-case basis, to new forms of obtaining consent as they develop in the marketplace. The Commission also noted that the new process would increase transparency by publicizing approvals or rejections of particular consent mechanisms, and

[248] *See* K. Dennis, AssertID (comment 34, 2011 NPRM), at 2; AssertID (comment 6, 2012 SNPRM), at 1; TRUSTe (comment 164, 2011 NPRM), at 11; EPIC (comment 41, 2011 NPRM), at 9; Institute for Public Representation (comment 71, 2011 NPRM), at 41; S. Leff, WhooGoo (comment 60, 2012 SNPRM).

[249] *See* AssertID, *supra* note 248; Institute for Public Representation, *supra* note 248.

[250] *See, e.g.,* American Association of Advertising Agencies (comment 2, 2011 NPRM); Association of Educational Publishers (comment 7, 2011 NPRM); ATT (comment 8, 2011 NPRM); d. boyd (comment 13, 2011 NPRM); DMA (comment 37, 2011 NPRM); ESA (comment 47, 2011 NPRM); Internet Commerce Coalition (comment 74, 2011 NPRM); kidSAFE Seal Program (comment 81, 2011 NPRM); Magazine Publishers of America (comment 61, 2012 SNPRM); Marketing Research Association (comment 97, 2011 NPRM); R. Newton (comment 118, 2011 NPRM); N. Savitt (comment 142, 2011 NPRM); Scholastic (comment 144, 2011 NPRM).

[251] *See, e.g.,* Association of Educational Publishers (comment 7, 2011 NPRM), at 1 (email plus is effective way to balance parental involvement with children's freedom to pursue educational experiences online); Scholastic (comment 144, 2011 NPRM), at 3 (email plus strikes a balance between the ease of getting consent and low safety risk to children from internal use of their data); Toy Industry Association (comment 163, 2011 NPRM), at 4–5 (similar cost-effective and efficient technologies to replace this method have not yet been developed); NCTA (comment 113, 2011 NPRM), at 20 (termination of email plus will have negative consequences and leave operators with no viable alternative); Privo (comment 132, 2011 NPRM), at 2 (email plus is a reasonable approach that can be understood by all constituents); d. boyd (comment 13, 2011 NPRM), at 5–6 (email plus imposes fewer burdens on families, particular low-income and immigrant families, than other available mechanisms); DMA (comment 37, 2011 NPRM), at 21 (elimination of email plus would create economic challenges in a difficult economic time).

[252] *See* Association for Competitive Technology (comment 7, 2012 SNPRM), at 6 (FTC should not remove easy to understand email plus without finding ways to make parental consent simpler); Toy Industry Association (comment 89, 2012 SNPRM), at 15 (the alternatives to email plus are not likely to be useful, effective, or cost-effective); *see also* American Association of Advertising Agencies (comment 2, 2011 NPRM), at 2 (this could result in a major reduction in parental consents obtained, solely due to burdensomeness of process); Association of Educational Publishers (comment 7, 2011 NPRM), at 2 (methods such as print, fax, or scan impede timely access to online resources; requiring credit cards or identification imposes barriers that may alienate parents; and other mechanisms impose financial costs on operators that may result in less free content); ESA (comment 47, 2011 NPRM), at 17–18 (requiring other methods of consent will make it harder to offer children robust content; no public benefit in requiring operators to make the costly changeover to other mechanisms); Scholastic (comment 144, 2011 NPRM), at 5–6 (credit card use is not an option for Scholastic, which offers free services; existing options are cumbersome and slow for parents and operators, and newly proposed options are less privacy protective, affordable, or accessible than email plus); TechFreedom (comment 159, 2011 NPRM), at 7–8 (making parental consent more difficult to obtain would disproportionately burden smaller players in the market and retard new entry); Wired Trust (comment 177, 2011 NPRM), at 5 (eliminating email plus will likely result in reduction in innovative and valuable online features for children).

[253] *See* d. boyd (comment 13, 2011 NPRM), at 6 (no data to suggest that children are evading email plus more than other consent mechanisms); Scholastic (comment 144, 2011 NPRM), at 8 (no evidence that proposed methods are significantly more reliable); *see also* kidSAFE Seal Program (comment 81, 2011 NPRM), at 13–14 (the Commission has not shown any harm to children due to use of email plus); SIIA (comment 150, 2011 NPRM), at 12–13 (proposing that only a small percentage of children are likely to falsify parental consent).

[254] *See, e.g.,* ACT (comment 7, 2012 SNPRM), at 6; Internet Commerce Coalition (comment 74, 2011 NPRM), at 5; Marketing Research Association (comment 97, 2011 NPRM), at 3; A. Thierer (comment 162, 2011 NPRM), at 7; WiredTrust (comment 177, 2011 NPRM), at 5.

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

[256] 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, 2010 FRN), at 3 (''innovation in developing procedures to obtain parental consent has been limited as Web sites choose to use the methods suggested by the FTC out of fear that a more innovative method could lead to liability'').

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

The Commission received several comments expressing support for the concept of a voluntary Commission approval process for new consent mechanisms.[257] At the same time, several commenters that supported the concept also opined that the 180-day approval period was too lengthy and would likely to discourage use of the program.[258] Commenters also expressed concerns that applications for approval would be subject to public comment.[259] One commenter asked the Commission instead to consider publicly releasing a letter explaining the Commission's decision to approve or disapprove a mechanism and thereby signaling what is an acceptable consent mechanism, without causing undue delay or risking the disclosure of proprietary information.[260]

One commenter opposed to the voluntary approval process asserted that it would be *ultra vires* to the COPPA statute and would create a *de facto* requirement for FTC approval of any new consent mechanisms, thereby discouraging operators from developing or using new means not formally approved by the Commission.[261] The Commission does not believe that offering operators the opportunity to apply for a voluntary approval process will either *de facto* create an additional COPPA requirement or chill innovation. This is just one more option available to operators.

The Commission also is persuaded by the comments requesting that it shorten the 180-day approval period. Accordingly, the final Rule's provision for Commission approval of parental consent mechanisms provides that the Commission shall issue a written determination within 120 days of the filing of the request. The Commission anticipates that some commenters will find that this time period also is longer than desired; however, it sets a reasonable time frame in which to solicit public comment and carefully determine whether a consent mechanism is sufficiently well-designed to fulfill the Rule's requirements.

The Commission has determined not to alter the requirement that the proposed mechanisms undergo public review and comment. This is an important component of the approval process. Moreover, just as the Commission has done for COPPA safe harbor applicants, it would permit those entities that voluntarily seek approval of consent mechanisms to seek confidential treatment for those portions of their applications that they believe warrant trade secret protection. In the event an applicant is not comfortable with the Commission's determination as to which materials will be placed on the public record, it will be free to withdraw the proposal from the approval process.

Accordingly, the Commission has amended the Rule to institute this voluntary approval process. For ease of organization, the Commission has created a new section—312.12 (''Voluntary Commission Approval Processes'')—to encompass both this approval process and the process for approval of additional activities under the *support for internal operations* definition.

9. Safe Harbor Approval of Parental Consent Mechanisms

Several commenters urged the Commission to permit Commission-approved safe harbor programs to serve as laboratories for developing new consent mechanisms.[262] The Commission stated its agreement in the 2011 NPRM that establishing such a system may aid the pace of development in this area. The Commission also stated that, given the measures proposed to strengthen Commission oversight of safe harbor programs, allowing safe harbors to approve new consent mechanisms would not result in the loosening of COPPA's standards for parental consent. Thus, the 2011 NPRM included a proposed Rule provision 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). Although one commenter expressed concern that this would lead to a ''race to the bottom'' by safe harbor programs,[263] most of the comments were favorable.[264] Moreover, the Commission believes its added oversight will prevent any ''race to the bottom'' efforts. Accordingly, the Commission adopts this provision unchanged from its September 2011 proposal.

10. Exceptions to Prior Parental Consent

The COPPA Act and the Rule address five fact patterns under which an operator may collect limited pieces of personal information from children prior to, or sometimes without, obtaining parental consent.[265] 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 safety of the child or the integrity of the Web site.[266] The 2011 NPRM proposed minor changes to the Rule to add one new exception.

a. Section 312.5(c)(1)

The Rule's first exception, § 312.5(c)(1), 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. In view of the limited purpose of the exception—to reach *the parent* to initiate the consent process—the Commission proposed in the 2011 NPRM to limit the information

[257] *See* CCIA (comment 27, 2011 NPRM), at 6 (voluntary approval mechanism is an ''excellent step'' to encourage innovation, provide assurance to potential operators, and ensure parents' participation); Yahoo! (comment 180, 2011 NPRM), at 4 (streamlined approval process for new mechanisms is critical to encouraging innovation); *see also* Consumers Union (comment 29, 2011 NPRM), at 5; FOSI (comment 51, 2011 NPRM), at 7; kidSAFE Seal Program (comment 81, 2011 NPRM), at 16.

[258] *See, e.g.,* CCIA (comment 27, 2011 NPRM), at 6 (process must be completed more quickly in order to be useful to industry); Facebook (comment 50, 2011 NPRM), at 14 (Commission's extensive experience with COPPA should enable its more expeditious approval or disapproval of new mechanisms).

[259] *See, e.g.,* CCIA (comment 27, 2011 NPRM), at 6 (while public comment is important, the Commission should consider ''an alternate private track'' for consent mechanisms involving proprietary technology or a competitive advantage); Facebook (comment 50, 2011 NPRM), at 15 (public comment requirement could negatively affect economic incentives for innovation where rival operators might be able to copy the mechanism).

[260] Facebook (comment 50, 2011 NPRM), at 15.

[261] DMA (comment 37, 2011 NPRM), at 24.

[262] *See* MPAA (comment 42, 2010 FRN), at 12; Rebecca Newton (comment 46, 2010 FRN), at 2; Privo (comment 50, 2010 FRN), at 2; PMA (comment 51, 2010 FRN), at 5; B. Szoka (comment 59, 2010 FRN), Szoka Responses to Questions for the Record, at 56; TRUSTe (comment 64, 2010 FRN), at 3; *see also generally* WiredSafety.org (comment 68, 2010 FRN), at 31–32.

[263] CommonSense Media (comment 26, 2011 NPRM), at 16 (raising concern that safe harbor providers may ''race to the bottom'' to offer operators low-cost consent programs with low standards of verifiable consent, unless the Commission requires safe harbors to publicly disclose their approvals and report them to the FTC).

[264] *See, e.g.,* eBay (comment 40, 2011 NPRM), at 4; kidSAFE Seal Program (comment 81, 2011 NPRM), at 16; TRUSTe (comment 164, 2011 NPRM), at 11 (noting cost benefit to operators to get early review of mechanism at design or wireframe stage).

[265] *See* 15 U.S.C. 6502(b)(2); 16 CFR 312.5(c).

[266] The Act and Rule currently permit the collection of limited personal information for the 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 Web site or online service. *See* 15 U.S.C. 6502(b)(2); 16 CFR 312.5(c)(1)–(5).

collection under this exception to the parent's online contact information only. However, as one commenter pointed out,[267] the COPPA statute expressly provides that, under this exception, an operator can collect ''the name or online contact information of a parent or child.'' [268]

Accordingly, the Commission retains § 312.5(c)(1) allowing for the collection of the name or online contact information of the parent or child in order to initiate the notice and consent process.[269]

b. Section 312.5(c)(2)

The 2011 NPRM proposed adding one additional 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 Web site or online service that does not otherwise collect, use, or disclose children's personal information.[270] The proposed exception, numbered 312.5(c)(2), provided that 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 indicated its belief 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.

The few comments addressing this proposed additional exception generally supported it.[271] Certain commenters recommended minor clarifications, such as adding language to indicate that the notice is voluntary and that operators can link a parent's email address to the child's account.[272] Upon consideration of the commenters' suggestions, the Commission has made minor changes to the language of this exception to clarify that its use is voluntary and that operators can use the exception to provide notice and subsequent updates to parents. The Commission did not find that clarification is needed to enable operators to link the parent's email to the child's account. Therefore, § 312.5(c)(2) of the final Rule permits the collection of a parent's online contact information to provide voluntary notice to, and subsequently update the parent about, the child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information, where the parent's contact information is not used or disclosed for any other purpose.[273]

c. Section 312.5(c)(3) (One-Time Use Exception)

Section 312.5(c)(2) of the Rule provides that an operator is not required to provide notice to a parent or obtain consent where the operator has collected *online contact information from a child* for the sole purpose of responding on a one-time basis to a child's request, and then deletes the information. The 2011 NPRM proposed a minor change to the language of the one-time use exception, stating that the exception would apply where the operator collected *a child's online contact information* for such purpose. One commenter pointed out that the Rule language, ''online contact information from a child,'' is taken directly from the COPPA statute. The commenter also expressed concern that the Commission's proposed change to the language may prevent operators from offering several popular one-time use activities under this exception.[274] In proposing this minor change, the Commission did not intend to further constrict the permissible uses of online contact information under the one-time-use exception (such as notifications regarding a contest or sweepstakes, homework help, birthday messages, forward-to-a-friend emails, or other similar communications). The Commission is persuaded, therefore, to retain the existing language in § 312.5(c)(3) permitting the collection of *online contact information from a child.*

d. Section 312.5(c)(4) (Multiple Use Exception)

The Rule provides that an operator may notify a parent via email or postal address that it has collected a child's online contact information to contact a child multiple times (for instance, to provide the child with a newsletter or other periodic communication).[275] The 2011 NPRM proposed revising the multiple contacts exception to allow for the collection of a child's and a parent's online contact information; and to strike the collection of postal address on the basis that it is now outmoded for this use. Although one commenter argued that postal address continues to provide a reasonable means of contacting the parent,[276] the Commission believes that the revised provision provides operators with a sufficient and practical means of contacting a parent in connection with the multiple use exception. The Commission also notes that the collection of postal address for the purpose of providing notice to a parent is not specifically provided for in the COPPA statute [277] or elsewhere in the Rule's notice requirements. Therefore, the language of § 312.5(4), as proposed in the 2011 NPRM, is hereby adopted in the final Rule.

e. Section 312.5(c)(5) (Child Safety Exception)

The 2011 NPRM proposed minor changes to the language of the child safety exception to state the purpose of the exception up-front, and to make clear that the operator can collect both the child's and the parent's online contact information where it is necessary to protect the safety of the child and where the information is not used for any other purpose. The Commission received one comment recommending that the Rule also allow for the collection of the parent's name, which the commenter believes may aid in contacting the parent, if necessary.[278] The Commission recognizes that the circumstances under which the child-safety exception becomes important may vary significantly. As such, the Commission is persuaded to further modify this exception to allow for collection of the parent's name, given that the exception is available only

[267] N. Savitt (comment 142, 2011 NPRM), at 2; *see also* kidSAFE Seal Program (comment 81, 2011 NPRM), at 17 (this exception should also allow the collection of a child's online contact information to enable the operator to notify the child that the parent has consented).

[268] 15 U.S.C. 6502(b)(2)(B).

[269] *See* Part II.B.1., *supra* (discussing the parallel correction to § 312.4(c)(1) (direct notice to a parent required under § 312.5(c)(1)).

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

[271] *See, e.g.,* DMA (comment 37, 2011 NPRM), at 26; kidSAFE Seal Program (comment 81, 2011 NPRM), at 17–18; N. Savitt (comment 142, 2011 NPRM), at 2.

[272] *See* N. Savitt (comment 142, 2011 NPRM), at 2 (proposing that the exception clearly indicate that providing such notice is optional); kidSAFE (comment 81, 2011 NPRM), at 18 (seeking clarification that parent's online contact information is linkable to child's account for updating purposes).

[273] Section 312.4(c)(2) of the final Rule sets out the direct notice requirements under this exception. *See* Part II.B.1., *supra.*

[274] *See* Promotion Marketing Association (comment 133, 2011 NPRM), at 5–6.

[275] Under this exception, the Rule requires the operator only to provide the parent the opportunity to *opt-out* of granting consent, rather than requiring it to obtain opt-in consent.

[276] *See* DMA (comment 37, 2011 NPRM), at 25–26.

[277] *See* 15 U.S.C. 6502(b)(2)(C) (statute requires operator to ''use reasonable efforts to provide a parent notice'').

[278] kidSAFE Seal Program (comment 81, 2011 NPRM), at 18.

where necessary 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. Section 312.5(c)(5) of the final Rule therefore provides that an operator can collect a child's and a parent's name and online contact information, to protect the safety of a child, where such information is not used or disclosed for any purpose unrelated to the child's safety.

f. Section 312.5(c)(6) (Security of the Site or Service Exception)

The final Rule incorporates the language of the Rule, with only minor, non-substantive changes to sentence structure.

g. Section 312.5(c)(7) (Persistent Identifier Used To Support Internal Operations Exception)

As described in Section II.C.5.b. above, the final Rule creates an exception for the collection of a persistent identifier, and no other personal information, where used solely to provide *support for the internal operations of the Web site or online service.* Where these criteria are met, the operator will have no notice or consent obligations under this exception.

h. Section 312.5(c)(8) (Operator Covered Under Paragraph (2) of Definition of Web Site or Online Service Directed to Children Collects a Persistent Identifier From a Previously Registered User)

Paragraph (2) of the definition of *Web site or online service directed to children* sets forth the actual knowledge standard for plug-ins under the Rule. The Commission is providing for a new, narrow, exception to the Rule's notice and consent requirements for such an operator where it collects a persistent identifier, and no other personal information, from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. The Commission has determined that, in this limited circumstance where an operator has already age-screened a user on its own Web site or online service, and such user has self-identified as being over the age of 12, the burden of requiring that operator to assume that this same user is a child outweighs any benefit that might come from providing notice and obtaining consent before collecting the persistent identifier in this instance. This exception only applies if the user affirmatively interacts with the operator's online service (*e.g.,* by clicking on a plug-in), and does not apply if the online service otherwise passively collects *personal information* from the user while he or she is on another site or service.

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

In the 2011 NPRM, the Commission proposed amending § 312.8 to strengthen the provision requiring operators to maintain the confidentiality, security, and integrity of personal information collected from children. Specifically, the Commission proposed adding a requirement that operators take reasonable measures to ensure 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.[279]

The Commission received a number of comments in support of its proposal. EPIC asserted, ''[third-party data collectors] are the ''least cost avoiders'' and can more efficiently protect the data in their possession than could the data subjects who have transferred control over their personal information.'' [280] The CDT found the proposal to be a ''sensible requirement that third-party operators put in place reasonable security procedures.'' [281] And the Privacy Rights Clearinghouse stated, ''the proposed revision * * * would enhance consumer trust and reduce the likelihood that data will be mishandled when disclosed to an outside party.'' [282]

Several commenters opposed the Commission's proposal outright, finding it to be unduly onerous on small businesses [283] or *ultra vires* to the statute.[284] The Commission finds this opposition unpersuasive. The requirement that operators take reasonable care to release children's personal information only to entities that will keep it secure flows directly from the statutory requirement that covered operators ''establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.'' [285]

Several commenters asked the Commission to consider narrowing the proposal so that it applies only to third parties with whom the operator has a contractual relationship, rather than to all third parties, given the breadth of the Rule's definition of *third party.*[286] These concerns are obviated by the Commission's proposal in the 2011 NPRM to narrow the definition of *release* to include only business-to-business disclosures, and not the sort of open-to-the-public disclosures that worry the commenters.[287]

Other commenters expressed concern with the Commission's use of the words ''reasonable measures'' and ''ensure'' in the proposed revised language, stating that such phrases are too subjective to be workable and set an impossible-to-reach standard.[288] Requiring operators to use ''reasonable measures'' both to establish their own data protection programs and to evaluate the programs of others has long been the standard the Commission employs in the context of its data security actions, and provides companies with the flexibility necessary to effectuate strong data privacy programs.[289] Importantly, the

[279] *See* 2011 NPRM, 76 FR at 59821. The Rule was silent on the data security obligations of third parties. However, the online notice provision in the Rule required operators to state in their privacy policies whether they disclose personal information to third parties, and if so, whether those third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the operator. *See* § 312.4(b)(2)(iv) of the Rule.

[280] EPIC (comment 41, 2011 NPRM), at 10–11; *see also* H. Valetk (comment 166, 2011 NPRM), at 2.

[281] CDT (comment 17, 2011 NPRM), at 2.

[282] Privacy Rights Clearinghouse (comment 131, 2011 NPRM), at 2.

[283] Marketing Research Association (comment 97, 2011 NPRM), at 4.

[284] DMA (comment 37, 2011 NPRM), at 26.

[285] 15 U.S.C. 6502(b)(1)(D).

[286] *See* Facebook (comment 50, 2011 NPRM), at 15–16 (''The current definition of *third party* in Section 312.1 sweeps so broadly that it also encompasses other users who can view content or receive communications from the child—including, for example, the child's relatives or classmates. Under the proposed amendment, operators would be obligated to take reasonable measures to ensure that these relatives and classmates have 'reasonable procedures' in place to protect the child's personal information''); CDT (comment 17, 2011 NPRM), at 2 (''consistent with the Commission's goal of addressing business-to-business data sharing, the Commission should make it clear that these additional data security requirements apply only to other FTC-regulated entities with which the operator has a contractual relationship'').

[287] *See* 2011 NPRM, 76 FR at 59809.

[288] IAB (comment 73, 2011 NPRM), at 14 (''The IAB is concerned that these requirements, if finalized, would create a risk of liability to companies based on highly subjective standards and on third party activities ''); MPAA (comment 109, 2011 NPRM), at 16–17 (''the proposed requirement that operators take measures sufficient to *ensure* compliance by vendors and other third parties might be misapplied to make operators the effective guarantors of those measures. As a practical matter, no business is in a position to exercise the same degree of control over another, independent business as it can exercise over its own operations.'').

[289] *See, e.g.,* In the Matter of Compete, Inc., FTC File No. 102 3155 (proposed consent order) (Oct. 29, 2012), *available at http://www.ftc.gov/os/caselist/1023155/121022competeincagreeorder.pdf;* In the Matter of Franklin's Budget Car Sales, Inc., FTC Docket No. C–4371 (consent order) (Oct. 3, 2012), *available at http://ftc.gov/os/caselist/1023094/121026franklinautomalldo.pdf;* In the Matter of EPN, Inc., FTC Docket No. C–4370 (consent order) (Oct. 3, 2012), *available at http://ftc.gov/os/caselist/1123143/121026epndo.pdf;* In

reasonable measures standard is the one set by Congress for operators' confidentiality, security, and integrity measures in the COPPA statute.[290]

The Commission finds merit, however, in the concerns expressed about the difficulty operators may face in ''ensuring'' 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 children's personal information.[291] The Motion Picture Association of America (''MPAA'') urged the Commission to take the approach adopted in the Safeguards Rule implemented under the Gramm-Leach-Bliley Act. Entities covered by the Safeguards Rule are required to take ''reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue'' and to ''requir[e] service providers by contract to implement and maintain such safeguards.'' [292]

After reviewing these comments, the Commission has decided to modify the standard required when an operator releases children's personal information to service providers and third parties. Operators must inquire about entities' data security capabilities and, either by contract or otherwise, receive assurances from such entities about how they will treat the personal information they receive. They will not be required to ''ensure'' that those entities secure the information absolutely.

Accordingly, the revised confidentiality, security, and integrity provision (§ 312.8) states that the operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

### *E. Section 312.10: Data Retention and Deletion Requirements*

In the 2011 NPRM, the Commission proposed adding a data retention and deletion provision (new Section 312.10).[293] The general tenet of data security, that deleting unneeded information is an integral part of any reasonable data security strategy (discussed in the Commission's 1999 COPPA Rulemaking), informed the Commission's rationale for this new provision.[294] In addition, the new proposed provision flowed from the statutory authority granted in COPPA for regulations requiring operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[295]

The Commission received support for its data retention and deletion proposal from several consumer groups and an individual commenter.[296] The Institute for Public Representation stated that, without such a provision, operators have no incentive to eliminate children's personal information and may retain it indefinitely.[297] Other supporters mentioned that a requirement to retain and eliminate data works in tandem with the Rule's requirement that data be kept confidential and secure, and has the added benefit of reducing the risk and impact of data breaches.[298]

Other commenters, primarily industry members, opposed the addition of a data retention and deletion provision, stating that it was unnecessary, vague, and unduly prescriptive.[299] These commenters especially objected to the combination of the data retention and deletion provision with the proposed expansion of the definition of *personal information* to include persistent identifiers. They asserted that the proposed deletion requirement would require companies to delete non-personally identifiable information, such as data used for Web site and marketing analytics.[300]

The Commission chose the phrases ''for only as long as is reasonably necessary'' and ''reasonable measures'' to avoid the very rigidity about which commenters opposing this provision complain.[301] Such terms permit operators to determine their own data retention needs and data deletion capabilities, without the Commission dictating specific time-frames or data destruction practices.[302]

While this new provision may require operators to give additional thought to notions of data retention and deletion, it should not add significantly to operators' burden. The existing Rule already prohibits operators from conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate.[303] Operators also must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[304] This new data retention and deletion provision, Section 312.10, requires operators to anticipate the reasonable lifetime of the personal information they collect from children, and apply the same concepts of data security to its disposal as they are required to do with regard to its collection and maintenance.

Therefore, the Commission modifies Section 312.10 as originally proposed, without change from its 2011 proposal.

### *F. Section 312.11: Safe Harbors*

The COPPA statute established a ''safe harbor'' for participants in Commission-approved COPPA self-regulatory programs.[305] As noted in the 2011 NPRM, 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

---

the Matter of Upromise, Inc., FTC Docket No. C–4351 (consent order) (Apr. 3, 2012), *available at http://www.ftc.gov/os/caselist/1023116/120403upromisedo.pdf.*

[290] 15 U.S.C. 6502(b)(1)(D).

[291] Facebook (comment 50, 2011 NPRM), at 16; MPAA (comment 109, 2011 NPRM), at 16–17.

[292] 16 CFR 314.4(d).

[293] *See* 76 FR at 59822.

[294] *See* 1999 Notice of Proposed Rulemaking, 64 FR at 22750, 22758–59 (''The 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.'').

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

[296] EPIC (comment 41, 2011 NPRM), at 4–5; Institute for Public Representation (comment 71, 2011 NPRM), at 42–43; Sarah Kirchner (comment 82, 2011 NPRM); Privacy Rights Clearinghouse (comment 131, 2011 NPRM), at 2–3.

[297] Institute for Public Representation, *supra* note 296, at 42–43.

[298] *See* EPIC (comment 41, 2011 NPRM), at 12; Privacy Rights Clearinghouse (comment 131, 2011 NPRM), at 2–3.

[299] American Association of Advertising Agencies (comment 2, 2011 NPRM), at 3; DMA (comment 37, 2011 NPRM), at 27; NCTA (comment 113, 2011 NPRM), at 21; National Retail Federation (comment 114, 2011 NPRM), at 4; TRUSTe (comment 164, 2011 NPRM), at 11–12; Yahoo! (comment 180, 2011 NPRM), at 15–16.

[300] *See* DMA (comment 37, 2011 NPRM), at 26; Yahoo! (comment 180, 2011 NPRM), at 15.

[301] *See* National Retail Federation (comment 114, 2011 NPRM), at 4; TRUSTe (comment 164, 2011 NPRM), at 12.

[302] For this reason, the Commission declines to adopt the Institute for Public Representation's request that it require companies to delete children's personal information within three months. *See* Institute for Public Representation (comment 71, 2011 NPRM), at 43.

[303] 16 CFR 312.7.

[304] 16 CFR 312.8.

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

COPPA's substantive provisions.[306] 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.[307]

In the 2011 NPRM, the Commission proposed several significant substantive changes to the Rule's safe harbor provision to strengthen the Commission's oversight of participating safe harbor programs. The proposed changes include a requirement that applicants seeking Commission approval of self-regulatory guidelines submit comprehensive information about their capability to run an effective safe harbor program. The changes also establish more rigorous baseline oversight by Commission-approved safe harbor programs of their members. In addition, the changes require Commission-approved safe harbor programs to submit periodic reports to the Commission. The Commission also proposed certain structural and linguistic changes to increase the clarity of the Rule's safe harbor provision.[308]

The Commission received several comments regarding the proposed changes, including comments from all four of the COPPA safe harbor programs the Commission had approved by 2011,[309] as well as from several other industry associations.[310] With the exception of a few areas discussed below, commenters favorably viewed the Commission's proposed revisions.[311] First, among commenters who mentioned them, there was uniform support for the proposed revised criteria for approval of self-regulatory guidelines, which would mandate that (at a minimum) safe harbor programs conduct annual, comprehensive reviews of each of their members' information practices.[312] Accordingly, the Commission retains paragraph (b)(2) (''Criteria for approval of self-regulatory guidelines'') without change from its 2011 proposal.

In paragraph (c) (''Request for Commission approval of self-regulatory program guidelines''), the Commission proposed requiring applicants to explain in detail their business model and their technological capabilities and mechanisms for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program. Again, commenters who mentioned it uniformly supported this change.[313] Accordingly, the Commission revises paragraph (c) (''Request for Commission approval of self-regulatory program guidelines'') without change from its 2011 proposal.

The response to the 2011 proposal for periodic reporting by safe harbors to the Commission (paragraph (d)) was more ambivalent.[314] While commenters generally supported stronger Commission oversight of safe harbor activities post-approval, they were concerned that a requirement forcing safe harbors to ''name names'' of violative member operators would chill the programs' abilities to recruit and retain members, and generally would be counter to notions of self-regulation.[315]

The Commission continues to believe that there is great value in receiving regular reports from its approved safe harbor programs. It is persuaded, however, that these reports need not name the member operators who were subject to a safe harbor's annual comprehensive review. Rather, the Commission has revised paragraph (d) to permit safe harbors to submit a report to the Commission containing an *aggregated summary* of the results of the independent assessments conducted under paragraph (b)(2). In addition, to simplify matters, the Commission has changed the required reporting period to an *annual* requirement rather than one occurring every eighteen months after the first annual report.[316] Therefore, the Commission amends paragraph (d) of the safe harbor provision so that it reads as set forth at § 312.11(d) in the regulatory amendments of this rule.

## III. Final Regulatory Flexibility Act Analysis

The Regulatory Flexibility Act of 1980 (''RFA'')[317] 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.[318] The Commission is not required to make such analyses if a Rule would not have such an economic effect.[319] As described below, the Commission anticipates the final Rule amendments will result in more Web sites and online services being subject to the Rule and to the Rule's disclosure and other compliance requirements. As discussed in Part IV.C, below, the Commission believes that a high proportion of operators of Web sites and online services potentially affected by

[306] *See* 2011 NPRM, 76 FR at 59822 (citing the 1999 Statement of Basis and Purpose, 64 FR at 59906).

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

[308] *See* 2011 NPRM, 76 FR at 59822–24.

[309] CARU (comment 20, 2011 NPRM); Entertainment Software Rating Board (''ESRB'') (comment 48, 2011 NPRM); Privo (comment 132, 2011 NPRM); TRUSTe (comment 164, 2011 NPRM).

[310] DMA (comment 37, 2011 NPRM); IAB (comment 73, 2011 NPRM); kidSAFE Seal Program (comment 81, 2011 NPRM).

[311] *See, e.g.,* CARU (comment 20, 2011 NPRM), at 2 (''In general, CARU believes that most of the proposed modifications will not only strengthen the safe harbor program, but will facilitate and enhance the Commission's named goals of reliability, accountability, transparency and sustainability.'').

[312] CARU (comment 20, 2011 NPRM), at 3; ESRB (comment 48, 2011 NPRM), at 2; kidSAFE Seal Program (comment 81, 2011 NPRM), at 20; TRUSTe (comment 164, 2011 NPRM), at 12.

[313] *See, e.g.,* kidSAFE Seal Program (comment 81, 2011 NPRM), at 20 (''KSP supports this change and believes more detailed information during the application process will give the FTC greater comfort regarding the operations of safe harbor programs''); *see also* CARU (comment 20, 2011 NPRM), at 3; ESRB (comment 48, 2011 NPRM), at 3; TRUSTe (comment 164, 2011 NPRM), at 13. One commenter sought assurance that such materials will be treated confidentially. kidSAFE Seal Program (comment 81, 2011 NPRM), at 20. Safe harbor applicants may designate materials as ''confidential,'' and the Commission will apply the same standards of confidentiality to such materials as it does to other voluntary submissions. *See* 15 U.S.C. 46(f) and 57b–2, and the Commission's Rules of Practice 4.10–4.11, 16 CFR 4.10–4.11.

[314] The proposed change would have required safe harbor programs to submit periodic reports—within one year after the revised Rule goes into effect and every eighteen months thereafter—of the results of the independent audits under revised paragraph (b)(2) and of any disciplinary actions taken against member operators. *See* 2011 NPRM, 76 FR at 59823.

[315] *See* CARU (comment 20, 2011 NPRM), at 3 (''Much of the value of self-regulation is that issues can be handled quickly and effectively. The reporting of 'any' action taken against a Web site operator may have a chilling effect on Web site operators' willingness to raise compliance issues themselves''); DMA (comment 37, 2011 NPRM), at 26 (''Based on feedback from our members, the DMA has reason to believe that this revision would decrease interest and participation in the safe harbor programs in contravention of the Commission's goal of increasing safe harbor participation''); *see also* ESRB (comment 48, 2011 NPRM), at 4; IAB (comment 73, 2011 NPRM), at 14; kidSAFE Seal Program (comment 81, 2011 NPRM), at 20; Privo (comment 132, 2011 NPRM), at 8; TRUSTe (comment 164, 2011 NPRM), at 13.

[316] The kidSAFE Seal Program also sought to limit the Rule's reporting requirements to ''material'' descriptions of disciplinary action taken against member operators (paragraph (d)(1)), ''reasonable'' Commission requests for additional information (paragraph (d)(2)), and ''material'' consumer complaints (paragraph (d)(3)). *See* kidSAFE Seal Program (comment 81, 2011 NPRM), at 21. The Commission believes that such limitations are unnecessary and that the wording of the requirements in revised paragraph (d) will not be overly burdensome for compliance by safe harbor programs.

[317] 5 U.S.C. 601–612.

[318] *See* 5 U.S.C. 603–04.

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

these revisions are small entities as defined by the RFA.

As described in Part I.B above, in September 2011, the Commission issued a Notice of Proposed Rulemaking setting forth proposed changes to the Commission's COPPA Rule. The Commission issued a Supplemental Notice of Proposed Rulemaking in August 2012 in which the Commission proposed additional and alternative changes to the Rule. In both the 2011 NPRM and 2012 SNPRM, the Commission published IRFAs and requested public comment on the impact on small businesses of its proposed Rule amendments. The Commission received approximately 450 comments, combined, on the changes proposed in the 2011 NPRM and the 2012 SNPRM. Numerous comments expressed general concern that the proposed revisions would impose costs on businesses, including small businesses;[320] few comments discussed the specific types of costs that the proposed revisions might impose, or attempted to quantify the costs or support their comments with empirical data.

In the 2011 NPRM and 2012 SNPRM, the Commission proposed 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. The Commission proposed modifications to the definitions of *operator, personal information, support for internal operations,* and *Web site or online service directed to children.* Among other things, the proposed definition of *personal information* was revised to include persistent identifiers where they are used for purposes other than support for internal operations, and to include screen and user names where they function as online contact information. In addition, the Commission proposed adding a new Section to the Rule regarding data retention and deletion.

The Commission shares the concern many commenters expressed that operators be afforded enough time to implement changes necessary for them to comply with the final Rule amendments.[321] Accordingly, the final Rule will go into effect on July 1, 2013.

[320] *See, e.g.,* D. Russell-Pinson (comment 81, 2012 SNPRM), at 1; Ahmed Siddiqui (comment 83, 2012 SNPRM), at 1; Mindy Douglas (comment 29, 2012 SNPRM), at 1; Karen Robertson (comment 80, 2012 SNPRM), at 1; R. Newton (comment 118, 2011 NPRM), at 1.

[321] *See* DMA (comment 37, 2011 NPRM), at 17; National Cable & Telecommunications Association (comment 113, 2011 NPRM), at 15–16.

*A. Need for and Objectives of the Final Rule Amendments*

The objectives of the final Rule 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 final Rule amendments is the Children's Online Privacy Protection Act, 15 U.S.C. 6501 *et seq.*

*B. Significant Issues Raised by Public Comments, Summary of the Agency's Assessment of These Issues, and Changes, if Any, Made in Response to Such Comments*

In the IRFAs, the Commission sought comment regarding the impact of the proposed COPPA Rule amendments and any alternatives the Commission should consider, with a specific focus on the effect of the Rule on small entities. As discussed above, the Commission received hundreds of comments in response to the rule amendments proposed in the NPRM and SNPRM. The most significant issues raised by the public comments, including comments addressing the impacts on small businesses, are set forth below. While the Commission received numerous comments about the compliance burdens and costs of the rules, the Commission did not receive much quantifiable information about the nature of the compliance burdens. The Commission has taken the costs and burdens of compliance into consideration in adopting these amendments.

(1) Definitions

Definition of Collects or Collection

As described above in Part II.A.1.b., the Commission proposed amendments to the Rule provision that allows sites and services to make interactive content available to children, without providing parental notice and obtaining consent, if *all* personal information is deleted prior to posting. The Commission proposed replacing this 100% deletion standard with a ''reasonable measures'' standard to further enable sites and services to make interactive content available to children, without providing parental notice and obtaining consent, thereby reducing burdens on operators. Most comments favored the ''reasonable measures'' standard, and the Commission has adopted it.

Definitions of Operator and Web Site or Online Service Directed to Children

As discussed above in Part II.A.4., the Commission's proposed rule changes clarify the responsibilities under COPPA when independent entities or third parties, *e.g.,* advertising networks or downloadable plug-ins, collect information from users through child-directed sites and services. Under the proposed revisions, the child-directed content provider would be strictly liable for personal information collected from its users by third parties. The Commission also proposed imputing the child-directed nature of the content site to the entity collecting the personal information if that entity knew or had reason to know that it was collecting personal information through a child-directed site. Most of the comments opposed the Commission's proposed modifications. Some of these commenters asserted that the proposed revisions would impracticably subject new entities to the Rule and its compliance costs.[322]

With some modifications to the proposed Rule language, the Commission has retained the proposed strict liability standard for child-directed content providers that allow third parties to collect personal information from users of the child-directed sites, as discussed in Part II.A.5.b. The Commission recognizes the potential burden that strict liability places on child-directed content providers, particularly small app developers, but believes that the potential burden will be eased by the changes to the definitions of persistent identifier and *support for internal operations* adopted in the Final Rule, as well as the exception to notice and parental consent—§ 312.5(c)(7)—where an operator collects only a persistent identifier only to support its internal operations. Further, in light of the comments received, the Commission revised the language proposed in the 2012 SNPRM to clarify that the language describing ''on whose behalf'' does not encompass platforms, such as Google Play or the App Store, that offer access to someone else's child-directed content. Also in light of the comments received, the Commission deemed third-party plug-ins to be co-operators only where they have actual knowledge that

[322] *See, e.g.,* Application Developers Alliance (comment 5, 2012 SNPRM), at 3–5; Association for Competitive Technology (comment 7, 2012 SNPRM), at 3–5; Center for Democracy & Technology (''CDT'') (comment 15, 2012 SNPRM), at 4–5; DMA (comment 28, 2012 SNPRM), at 5, 17; J. Garrett (comment 38, 2012 SNPRM), at 1; L. Mattke (comment 63, 2012 SNPRM); S. Weiner (comment 97, 2012 SNPRM), at 1–2.

they are collecting personal information from users of a child-directed site. This change will likely substantially reduce the number of operators of third-party plug-ins, many of whom are small businesses, who must comply with the Rule in comparison to the proposal in the 2012 SNPRM. In response to comments requesting it, the Commission is also providing guidance in Part II.A.4.b. above as to when it believes this ''actual knowledge'' standard will likely be met.

Definition of Online Contact Information

The Commission proposed clarifications to the definition of *online contact information* to flag that the term broadly covers all identifiers that permit direct contact with a person online and to ensure consistency between the definition of *online contact information* and the use of that term within the definition of *personal information.* The proposed revised definition identified commonly used online identifiers, including email addresses, instant messaging (''IM'') user identifiers, voice over Internet protocol (''VOIP'') identifiers, and video chat user identifiers, while also clarifying that the list of identifiers was non-exhaustive. This amendment, which serves to clarify the definition, should not increase operators' burden.

Definition of Personal Information

a. Screen or User Names

As described above, the Commission in the 2011 NPRM proposed modifications to the inclusion of screen names in the definition of personal information. Numerous commenters expressed concern that the Commission's screen-name proposal would unnecessarily inhibit functions that are important to the operation of child-directed Web sites and online services. In response to this concern, the 2012 SNPRM proposed covering screen names as *personal information* only in those instances in which a screen or user name rises to the level of *online contact information.* As discussed in Part II.A.5.a., the Commission has adopted the proposal in the SNPRM. The revision permits operators to use anonymous screen and user names in place of individually identifiable information, including use for content personalization, filtered chat, for public display on a Web site or online service, or for operator-to-user communication via the screen or user name. Moreover, the definition does not reach single log-in identifiers that permit children to transition between devices or access related properties across multiple platforms. Thus, the provision for screen or usernames does not create any additional compliance burden for operators.

b. Persistent Identifiers and Support for Internal Operations

In the 2011 NPRM, and again in the 2012 SNPRM, the Commission proposed broadening the definition of personal information to include persistent identifiers, except where used to support the internal operations of the site or service. Numerous commenters opposed the inclusion of persistent identifiers, while others sought to broaden the definition of support for internal operations to allow for more covered uses of persistent identifiers. Some commenters maintained that, to comply with COPPA's notice and consent requirements in the context of persistent identifiers, sites would be burdened to collect more personal information on their users, which is also contrary to COPPA's goals of data minimization.[323] As set forth in Part II.A.5.b, the Commission believes that persistent identifiers permit the online contacting of a specific individual and thus are personal information. However, the Commission recognizes that including persistent identifiers within the definition of personal information may impose a burden on some operators to provide notice to parents and obtain consent under circumstances where they previously had no COPPA obligation. The Commission also recognizes that persistent identifiers are used for a host of functions that are unrelated to contacting a specific individual and fundamental to the smooth functioning of the Internet, the quality of the site or service, and the individual user's experience. Thus, the final Rule further restricts the proposed definition of *persistent identifiers* to ''a persistent identifier that can be used to recognize a user over time *and* across different Web sites or online services, where such persistent identifier is used for functions other than or in addition to support for the internal operations of the Web site or online service.'' (Emphasis added.) The Final Rule also modifies the definition of *support for internal operations* to broaden the list of activities covered within this category. As a result of these modifications, fewer uses of persistent identifiers will be covered in the Final Rule than in the proposals, thereby resulting in fewer operators being subject to the final Rule amendments.

c. Photographs, Videos, and Audio Files

In the 2011 NPRM, the Commission proposed creating a new category within the definition of *personal information* covering a photograph, video, or audio file where such file contains a child's image or voice. Some commenters supported this proposal; others were critical. The latter claimed that the proposal's effect would limit children's participation in online activities involving ''user-generated content,'' that photos, videos, and/or audio files, in and of themselves, do not permit operators to locate or contact a child, or that the Commission's proposal is premature.[324] The Commission determined, as discussed in Part II.A.5.c, that such files meet the standard for ''personal information'' set forth in the COPPA statute. While recognizing that defining *personal information* to include photos, videos, and/or audio files may affect a limited number of operators, this is warranted given the inherently personal nature of this content.

d. Geolocation Information

In the 2011 NPRM, the Commission stated that, in its view, existing paragraph (b) of the definition of *personal information* already covered any geolocation information that provides precise enough information to identify the name of a street and city or town. To make this clear, the Commission has made geolocation information a stand-alone category within the definition of *personal information.* Thus, this amendment should impose little or no additional burden on operators.

Definition of Web Site or Online Service Directed to Children

In the 2012 SNPRM, the Commission proposed revising the definition of Web site or online service directed to children to allow a subset of sites falling within that category an option not to treat all users as children. However, several commenters expressed concern and confusion that the proposed amendment would expand COPPA's reach to sites or services not previously covered under the definition of Web site directed to children, and thus would be likely to impose COPPA's burdens on

[323] Facebook (comment 33, 2012 SNPRM), at 9–10; Google (comment 41, 2012 SNPRM), at 5; J. Holmes (comment 47, 2012 SNPRM).

[324] *See* National Cable & Telecommunications Association (comment 113, 2011 NPRM), at 16; Wired Trust (comment 177, 2011 NPRM), at 10; Toy Industry Association (comment 163, 2011 NPRM), at 14; Privo (comment 132, 2011 NPRM), at 7; *see also* Center for Democracy and Technology (comment 17, 2011 NPRM), at 7–8.

operators not previously covered by the Rule. The Commission has clarified in Part II.A.7 that it did not intend to expand the reach of the Rule to additional sites and services through the proposed revision, but rather to create a new compliance option for a subset of Web sites and online services already considered *directed to children* under the Rule's totality of the circumstances standard. The Commission also clarified when a child-directed site would be permitted to age-screen to differentiate among users, thereby providing further guidance to businesses. This amendment will ease compliance burdens on operators of sites or services that qualify to age-screen their visitors. In addition, the Commission has made further clarifying edits to the definition of *Web site or online service directed to children* to incorporate the ''actual knowledge'' standard for plug-ins or ad networks, as discussed above.

(2) Section 312.4: Notice

Direct Notice to a Parent

The Commission proposed refining the Rule requirements for the direct notice to ensure a more effective ''just-in-time'' message to parents about an operator's information practices. Commenters generally supported the Commission's proposed changes as providing greater clarity and simplicity to otherwise difficult-to-understand statements. The Commission adopted the proposed modification but, in light of suggestions in the comments, reorganized the paragraphs to provide a better flow and guidance for operators.

Notice on the Web Site or Online Service

The Commission proposed to change the Rule's online notice provision to require all operators collecting, using, or disclosing information on a Web site or online service to provide contact information, including, at a minimum, the operator's name, physical address, telephone number, and email address. This proposal marked a change from the existing Rule's ''single operator designee'' proviso that such operators could designate one operator to serve as the point of contact. Almost all commenters who spoke to the issue opposed mandating that the online notice list all operators. Among the varied reasons cited in opposition to this change was the potential burden on operators. After considering the comments, the Commission has determined to retain the Rule's ''single operator designee'' proviso.

(3) Section 312.5: Parental Consent

Based on input the Commission received at its June 2, 2010 COPPA roundtable and comments to the 2010 FRN, in the 2011 NPRM the Commission proposed several significant changes to the mechanisms of verifiable parental consent set forth in paragraph (b) of § 312.5. These included recognizing electronic scans of signed consent forms, video conferencing, government-issued ID, and a credit card in connection with a monetary transaction as additional mechanisms for operators to obtain parental consent. In response to comments, the Commission also adopted amendments to allow the use of other payment systems, in addition to credit cards, in connection with a monetary transaction as verifiable parental consent, provided that any such payment system notifies the primary account holder of each discrete transaction. These changes provide operators with further flexibility in complying with the Rule.

The Commission also proposed eliminating the sliding scale (''email plus'') approach to parental consent for operators collecting personal information only for *internal* use. As discussed in Part II.C.7, most commenters urged the Commission to retain email plus, in part because they asserted it is more affordable and less burdensome for operators to use than other approved methods for obtaining consent. Persuaded by the weight of the comments, the Commission retained email plus as an acceptable consent method for internal use of personal information, thereby providing operators with the choice of a mechanism many deem useful and affordable.

Finally, the Commission also added two new voluntary processes for evaluation and pre-clearance of parental consent mechanisms: use of an FTC preapproval process and use of a safe harbor program for such purpose. The availability of these voluntary pre-clearance mechanisms may provide benefits to participating operators in reducing the burden associated with the start-up of a new COPPA compliance mechanism.

(4) Section 312.8: Confidentiality, Security, and Integrity of Personal Information Collected From Children

In 2011, the Commission proposed amending § 312.8 of the Rule to require that operators take reasonable measures to ensure 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. Although many commenters supported this proposal, some raised concerns about the language ''reasonable measures'' and ''ensure.'' Other commenters opposed the requirement as unduly onerous on small businesses. The Commission found merit in the concerns expressed about the difficulty operators may face in ''ensuring'' that any service provider or third party has in place reasonable confidentiality and security procedures. Thus, the Commission has lessened the burden on operators that would have been imposed by the earlier proposal by requiring operators to take reasonable steps to release personal information only to service providers and third parties capable of maintaining it securely.

(5) Section 312.10: Data Retention and Deletion Requirements

The Commission also has added a data retention and deletion provision (new Section 312.10) to the Rule to require operators to anticipate the reasonable lifetime of the personal information they collect from children, and apply the same concepts of data security to its disposal as they are required to do with regard to its collection and maintenance. While several commenters supported this provision, several others objected to it as unnecessary, vague, or unduly prescriptive.[325] These commenters especially objected to the burden imposed by the combination of the data retention and deletion provision with the proposed expansion of the definition of *personal information* to include persistent identifiers. The Commission believes these concerns are not warranted in light of the language of the final Rule amendments, and that this requirement should not add significantly to operators' burdens.

(6) Section 312.11: Safe Harbors

The Commission proposed changing the Rule's safe harbor provision to strengthen the Commission's oversight of participating safe harbor programs. Among other things, the Commission proposed requiring those programs to submit periodic reports to the Commission. Commenters generally viewed the proposed revisions favorably, but expressed concern that the proposed language requiring safe harbors to name violative member operators, would chill participation in the programs. Heeding these concerns,

[325] *See, e.g.,* DMA (comment 37, 2011 NPRM), at 27; Toy Industry Association (comment 163, 2011 NPRM), at 16–17.

the Commission will not require regular reports from approved safe harbor programs to name the member operators who were subject to a safe harbor's annual comprehensive review. The final Rule amendments instead will require safe harbor programs to submit an aggregated summary of the results of the annual, comprehensive reviews of each of their members' information practices. These amendments ensure the effectiveness of the safe harbor programs upon which numerous operators rely for assistance in their compliance with COPPA.

*C. Description and Estimate of the Number of Small Entities Subject to the Final Rule or Explanation Why No Estimate Is Available*

The revised definitions in the Final Rule will affect operators of Web sites and online services directed to children, as well as those operators that have actual knowledge that they are collecting personal information from children. The Final Rule amendments will impose costs on entities that are ''operators'' under the Rule. The Commission staff is unaware of any comprehensive empirical evidence concerning the number of operators subject to the Rule. However, based on the public comments received and the modifications adopted here, the Commission staff estimates that approximately 2,910 existing operators may be subject to the Rule's requirements and that there will be approximately 280 new operators per year for a prospective three-year period.

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.[326] Consistent with the estimate set forth in the 2012 SNPRM, Commission staff estimates that approximately 85–90% 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, discussions with industry members, privacy professionals, and advocates, and oversight of COPPA safe harbor programs. This estimate is also consistent with the sole comment that attempted to quantify how many operators are small entities.[327]

*D. Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Final Rule Amendments, Including an Estimate of the Classes of Small Entities Which Will Be Subject to the Rule and the Type of Professional Skills That Will Be Necessary To Comply*

The final Rule amendments will likely increase certain disclosure and other compliance requirements for covered operators. In particular, the 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 addition of language in § 312.8 (confidentiality, security, and integrity of personal information collected from children) will require operators to ''take reasonable steps'' to release children's personal information only to third parties capable of maintaining its confidentiality, security, and integrity, and who provide assurances that they will do so. The final Rule amendments contain additional reporting requirements for entities voluntarily seeking approval to be a COPPA safe harbor self-regulatory program, and additional compliance requirements for all Commission-approved safe harbor programs. Each of these improvements to the Rule may entail some added cost burden to operators, including those that qualify as small entities, but the Commission has considered these burdens and responded to commenters as described in Part III.C., above.

The revisions to the Rule's definitions will also likely increase the number of operators subject to the final Rule amendments' disclosure and other compliance requirements. In particular, the revised definition of *operator* will cover additional child-directed Web sites and online services that choose to integrate plug-ins or advertising networks that collect personal information from visitors. Similarly, the addition of paragraph (2) to the definition of *Web site or online service directed to children,* which clarifies that the Rule covers a Web site or online service that has actual knowledge that it is collecting personal information directly from users of a Web site or online service directed to children, will potentially cover additional Web sites and online services. These amendments may entail some added cost burden to operators, including those that qualify as small entities; however, as described above, other final Rule amendments will ease the burdens on operators and facilitate compliance.

The estimated burden imposed by these modifications to the Rule's definitions 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.,* Web site programming) and others that may be variable (*e.g.,* choosing to operate a family friendly Web site or online service), and the entity's income or profit from operation of the Web site or online service (*e.g.,* membership fees) or from related sources (*e.g.,* revenue from marketing to children through the site or service). As explained in the Paperwork Reduction Act section, in order to comply with the Rule's requirements, 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 2,910 Web site or online services that would qualify as *operators* under the final Rule amendments, that there will be approximately 280 new operators per year for a three-year period, and that approximately 85–90% of all such operators would qualify as small entities under the SBA's Small Business Size standards.

*E. Steps the Agency Has Taken To Minimize Any Significant Economic Impact on Small Entities, Consistent With the Stated Objectives of the Applicable Statute*

In drafting the amendments to the Rule's definitions, the Commission has attempted to avoid unduly burdensome requirements for all entities, including small businesses. The Commission believes that the final Rule amendments will advance the goal of children's online privacy in accordance with COPPA. For each of the modifications, the Commission has taken into account the concerns evidenced by the record. On balance, the Commission believes that the benefits to children and their parents outweigh the costs of implementation to industry.

The Commission has considered, but has decided not to propose, an

[326] *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/files/Size_Standards_Table.pdf.*

[327] Association for Competitive Technology (comment 7, 2012 SNPRM), at 2 (ACT's research ''found that 87% of educational apps are created by companies qualifying as 'small' by SBA guidelines''). ACT gave only limited information about how it calculated this figure.

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.[328] Accordingly, an exemption for small businesses would undermine the very purpose of the statute and Rule.

Nonetheless, the Commission has taken care in developing the final Rule amendments to set performance standards that regulated entities must achieve, but provide them with the flexibility to select the most appropriate, cost-effective, technologies to achieve COPPA's objective results. For example, the Commission has retained the standard that verifiable parental consent may be obtained via any means reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. The 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 has adopted the ''reasonable measures'' standard enabling operators to use competent filtering technologies to prevent children from publicly disclosing personal information, which the Commission believes will make it easier for operators to avoid the collection of children's personal information. The new definition of *support for internal operations* is intended to provide operators with the flexibility to collect and use personal information for purposes consistent with ordinary operation, enhancement, or security measures. Moreover, the changes to *Web site or online service directed to children* should provide greater flexibility to ''family friendly'' sites and services in developing mechanisms to provide the COPPA protections to child visitors.

[328] *See, e.g.,United States* v. *RockYou, Inc.,* No. 3:12–cv–01487–SI (N.D. Cal., entered Mar. 27, 2012); *United States* v. *Godwin,* No. 1:11–cv–03846–JOF (N.D. Ga., entered Feb. 1, 2012); *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., entered Sept. 11, 2006); *United States* v. *Bonzi Software, Inc.,* No. CV–04–1048 (C.D. Cal., filed Feb. 17, 2004); *United States* v. *Looksmart, Ltd.,* No. 01–605–A (E.D. Va., filed Apr. 18, 2001); *United States* v. *Bigmailbox.Com, Inc.,* No. 01–606–B (E.D. Va., filed Apr. 18, 2001).

## IV. 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 (APRA''), as amended, 44 U.S.C. 3501 *et seq.* OMB has approved the Rule's existing information collection requirements through July 31, 2014. In accordance with the PRA, the Commission is seeking OMB approval of the final Rule amendments under OMB Control No. 3084–0117. The disclosure, recordkeeping, and reporting requirements under the final Rule amendments discussed above constitute''collections of information'' for purposes of the PRA.

Upon publication of the 2011 NPRM and the 2012 SNPRM, the FTC submitted the proposed Rule amendments and a Supporting Statement to OMB. In response, OMB filed comments (dated October 27, 2011 and August 10, 2012) indicating that it was withholding approval pending the Commission's examination of the public comments in response to the 2011 NPRM and 2012 SNPRM. The remainder of this section sets forth a revised PRA analysis, factoring in relevant public comments and the Commission's resulting or self-initiated changes to the proposed Rule.

### *A. Practical Utility*

According to the PRA,''practical utility'' is'' the ability of an agency to use information, particularly the capability to process such information in a timely and useful fashion.'' [329] The Commission has maximized the practical utility of the new disclosure (notice) and reporting requirements contained in the final Rule amendments, consistent with the requirements of COPPA.

(1) Disclosure Requirements

The final Rule amendments to Section 312.4(c) more clearly articulate the specific information that operators' direct notices to parents must include about their information collection and use practices. The succinct, ''just-in-time'' notices will present key information to parents to better enable them to determine whether to permit their children to provide personal information online, seek access from a Web site or online service operator to review their children's personal information, and object to any further collection, maintenance, or use of such information. The final Rule amendments to the definitions of *operator* and *Web site or online service directed to children* in Section 312.2 will better ensure that parents are provided notice when a child-directed site or service chooses to integrate into its property other services that collect visitors' personal information. For example, the final Rule amendment to the definition of *operator* clarifies that child-directed Web sites that do not collect personal information from users, but that employ downloadable software plug-ins or permit other entities, such as advertising networks, to collect personal information directly from their users, are covered operators with responsibility for providing parental notice and obtaining consent. Additionally, the changes to the definition of *Web site or online service directed to children,* among other things, will clarify that the Rule covers a plug-in or ad network where it has actual knowledge that it is collecting personal information directly from users of a child-directed Web site or online service.

To avoid obscuring the most meaningful, material information for consumers, however, the Commission removed a previously proposed requirement, set forth in the 2011 NPRM, that *all* operators collecting, using, or disclosing information on a Web site or online service must provide contact information.[330] The Commission retained the existing Rule's proviso that such operators could designate one operator to serve as the point of contact. For the same reason, the Commission has streamlined the Rule's online notice requirement to require a simple statement of: (1) What information the operator collects from children, including whether the Web site 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.[331] As a part of this revision, the Commission also removed the required statement that the operator may not condition a child's participation in an activity on the child's disclosure of more personal

[329] 44 U.S.C. 3502(11). In determining whether information will have ''practical utility,'' OMB will consider ''whether the agency demonstrates actual timely use for the information either to carry out its functions or make it available to third-parties or the public, either directly or by means of a third-party or public posting, notification, labeling, or similar disclosure requirement, for the use of persons who have an interest in entities or transactions over which the agency has jurisdiction.'' 5 CFR 1320.3(l).

[330] 2011 NPRM, 76 FR at 59815.

[331] *See id.*

information than is reasonably necessary to participate in such activity.[332]

(2) Reporting Requirements

As stated above, the Commission believes that there is great value in receiving annual reports from its approved safe harbor programs. Obtaining this information (in addition to the Commission's right to access program records) will better ensure that all safe harbor programs keep sufficient records and that the Commission is routinely apprised of key information about the safe harbors' programs and membership oversight. Further, requiring annual reports to include a description of any safe harbor approvals of new parental consent mechanisms will inform the Commission of the emergence of new feasible parental consent mechanisms for operators. Additionally, the final Rule amendments impose more stringent requirements for safe harbor applicants' submissions to the Commission to better ensure that applicants are capable of administering effective safe harbor programs.

Thus, given the justifications stated above for the amended disclosure and reporting requirements, the final Rule amendments will have significant practical utility.

*B. Explanation of Estimated Incremental Burden Under the Final Rule Amendments*

1. Disclosure: 69,000 hours (for new and existing operators, combined).
2. Reporting: 720 hours (one-time burden, annualized, and recurring).
3. Labor Costs: $21,508,900.
4. Non-Labor/Capital Costs: $0.

Estimating PRA burden of the final Rule amendments' requirements depends on various factors, including the number of firms operating Web sites or online services directed to children or having actual knowledge that they are collecting or maintaining personal information from children, and the number of such firms that collect persistent identifiers for something other than support for the internal operations of their Web sites or online services.

In its 2011 NPRM PRA analysis, FTC staff estimated that there were then approximately 2,000 operators subject to the Rule. Staff additionally stated its belief that the number of operators subject to the Rule would not change significantly as a result of the proposed revision to the definition of *personal information* proposed in the 2011 NPRM.[333] Staff believed that altering that definition would potentially increase the number of operators, but that the increase would be offset by other proposed modifications. These offsets included provisions allowing the use of persistent identifiers to support the internal operations of a Web site 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 2011 NPRM PRA analysis also assumed that some operators of Web sites or online services will adjust their information collection practices so that they will not be collecting personal information from children.[334] In the 2011 NPRM PRA analysis, staff estimated that approximately 100 new operators per year [335] (over a prospective three-year OMB clearance [336]) of Web sites or online services would likely be covered by the Rule through the proposed modifications. No comments filed in response to the 2011 NPRM took direct issue with these estimates.[337] Commission staff also estimated that no more than one safe harbor applicant will submit a request within the next three years,[338] and this estimate has not been contested.

In its 2012 SNPRM PRA analysis, staff stated that the proposed modifications to the Rule would change the definitions of *operator* and *Web site or online service directed to children,* potentially increasing the number of operators subject to the Rule. Staff added, however, that the proposed amendments to the definitions of *support for internal operations* and *Web site or online service direct to children* should offset some of the effects of these other definitional expansions.[339] The 2012 SNPRM PRA analysis also assumed that some operators of Web sites or online services would adjust their information collection practices so that they would not be collecting personal information from children.[340] Based on those assumptions, FTC staff estimated that, in addition to the 2,000 existing operators already covered by the Rule (per the 2011 NPRM PRA analysis), there would be approximately 500 existing operators of Web sites or online services likely to be newly covered due to the proposed modifications.[341] Staff also estimated that 125 additional new operators per year (over a prospective three-year clearance) would be covered by the Rule through the proposed modifications. That was incremental to the previously cleared FTC estimate of 100 new operators per year for the then existing Rule.[342] The FTC's 2011 NPRM and 2012 SNPRM analyses thus cumulatively accounted for an estimated 2,500 existing operators and 225 new operators each year that would be subject to the proposed Rule amendments.[343]

Given the public comments received, the Commission now estimates, as detailed further below, that the final Rule amendments will cover 2,910 existing operators of Web sites or online services and 280 new operators per year.[344] These groups of covered operators would generally consist of certain traditional Web site operators, mobile app developers, plug-in developers, and advertising networks.

Existing Operators

The Commission received several comments directed to its estimates of the number of existing operators, all of which assert that the Commission significantly underestimated these

[332] *See id.*

[333] *Id.* at 59826.

[334] *Id.*

[335] *Id.*

[336] Under the PRA, agencies may seek from OMB a maximum three year clearance for a collection of information. 44 U.S.C. 3507(g).

[337] Likewise, no comments were received in response to the February 9, 2011 and May 31, 2011 **Federal Register** notices (76 FR 7211 and 76 FR 31334, respectively, *available at http://www.gpo.gov/fdsys/pkg/FR–2011–02–09/pdf/2011–2904.pdf* and *http://www.gpo.gov/fdsys/pkg/FR–2011–05–31/pdf/2011–13357.pdf*) seeking comment on the information requirements associated with the existing COPPA Rule and the FTC burden estimates for them. These notices included the Commission staff estimate that roughly 100 new web entrants each year will fall within the Rule's coverage.

[338] 2011 NPRM, 76 FR at 59826; *accord* 76 FR 7211 at 7213 and 76 FR at 31335.

[339] 2012 SNPRM, 77 FR at 46650.

[340] *Id.*

[341] *Id.*

[342] *Id.*

[343] Commenter Association for Competitive Technology therefore is mistaken in asserting that the ''FTC has estimated 500 existing education app makers will be affected by the proposed rule, and an additional 125 newly affected entities each successive year.'' Association for Competitive Technology (comment 7, 2012 SNPRM), at 2. The Commission's previous PRA analyses did not specifically estimate numbers of ''education app makers,'' and the commenter did not account for the Commission's 2011 NPRM estimate of 2,000 existing entities.

[344] Under the existing OMB clearance for the pre-amended Rule, however, the FTC had already accounted for an estimated 100 new operators each requiring approximately 60 hours to comply with the Rule. *See* 76 FR at 7211, 7212 (Feb. 9, 2011); 76 FR at 31334, 31335 (May 31, 2011). Thus, to avoid double-counting what has already been submitted to OMB and cleared, the ensuing calculations for new operators' disclosure burden account strictly for the difference between the revised population estimate (280) and the currently cleared estimate (100), *i.e.,* 180 additional new operators.

numbers.[345] The Association for Competitive Technology (''ACT'') cited data showing that as of September 2012, there were approximately 74,000 ''education'' apps in the iTunes App Store, and 30,000 in the Android market.[346] Based on its review of ''top'' apps, ACT calculated a ratio of 1.54 apps per developer of ''education'' apps in the iTunes App Store,[347] and that approximately 60% of apps in this category were directed to children under 13.[348] Based on this information, ACT calculated that approximately 28,800 app developers would be ''potentially affected'' by the proposed modifications to the Rule set forth in the 2011 NPRM and 2012 SNPRM.[349] One commenter, the moderator of an online group called ''Parents With Apps,'' stated that the group has more than 1,400 small developers of family-friendly apps as members.[350] Another commenter stated that the Silicon Valley Apps for Kids Meetup group had ''well over 500 members'' as of September 2012, and that ''the kids app market is incredibly vibrant with thousands of developers, over 500 of which'' are group members.[351]

Per the industry information source cited by ACT, the Commission believes that as of November 2012, there were approximately 75,000 education apps in the iTunes App Store and approximately 33,000 education apps in the Android market.[352] ACT's comment appears to suggest that it would be reasonable for the Commission to base its PRA estimate of the number of existing operators subject to the final Rule amendments on the number of ''Education'' app developers. The Commission agrees that developer activity in the ''Education'' category, to the extent it can be discerned through publicly available information, is a useful starting point for estimating the number of mobile app developers whose activities may bring them within coverage of the final Rule amendments. As discussed below, the Commission also looks to information about ''Education'' apps in the Google Play store, and apps in the game and entertainment categories in both the iTunes App Store and Google Play, as a basis for its estimates for this PRA analysis.[353]

Similar to what appears to have been ACT's methodology, Commission staff reviewed a list, generated using the desktop version of iTunes, of the Top 200 Paid and Top 200 Free ''Education'' apps in the iTunes App Store as of early November 2012. Based on the titles and a prima facie review of the apps' descriptions, staff believes that approximately 56% of them may be directed to children under 13.[354] Averaging this figure and ACT's 60% calculation, FTC staff estimates that 58% of ''Education'' Apps in the iTunes App Store may be directed to children under 13, meaning that 43,500 of those 75,000 ''Education'' apps may be directed to children under 13. To determine a ratio for the Education apps for the Android platform, Commission staff reviewed listings of the Top 216 Paid and Top 216 Free ''Education'' apps in the Google Play store as of mid-November 2012. Staff believes that approximately 42% of them may be directed to children under 13; 42% of 33,000 apps yields 13,860 apps that may be directed to children under 13. Adding these projected totals together yields 57,360 such apps for both platforms, combined.

It is unreasonable to assume, however, that all apps directed to children under 13 collect personal information from children, and that no developers only collect persistent identifiers in support for their internal operations. Data from the Mobile Apps for Kids II Report indicate that about 59% of the apps surveyed transmit device identification or other persistent identifiers, to their developers.[355] However, it is not clear how many of those app developers would be using those persistent identifiers in a way that would fall within the final Rule's amended definition of *personal information.* Indeed, the Commission believes, based on the comments received, that many developers would use such persistent identifiers to support internal operations as defined in the final Rule amendments and not for other purposes, such as behavioral advertising directed to children.[356] Furthermore, the Commission believes that some mobile app developers, like some other operators of Web sites or online services, will adjust their information collection practices so that they will not be collecting personal information from children. The data in the staff report do suggest, however, that approximately 3.5% of apps directed to children under 13 could be collecting location information or a device's phone number, thus making their developers more likely to be covered by the final Rule amendments.[357] The Commission believes it is reasonable to assume that an additional 1.5% of those apps could be collecting other personal information, including transmitting persistent identifiers to developers (or their partners) to use in ways that implicate COPPA. This results in an estimate of 5% of apps that may be directed to children under 13, *i.e.,* approximately 2,870 apps, that operate in ways that implicate the final Rule amendments.

To estimate the number of developers responsible for these apps,[358] Commission staff used the ''Browse'' function in iTunes, to generate a list of 6,000 apps in the ''Education'' category. Sorting that list by ''Genre'' generates a list of approximately 3,300 apps for which ''Education'' was listed as the ''Genre.'' Approximately 1,800 developers were listed in connection

[345] Association for Competitive Technology (comment 7, 2012 SNPRM), at 2–3; S. Weiner (comment 97, 2012 SNPRM), at 1–2; J. Garrett (comment 38, 2012 SNPRM), at 1; *see also* DMA (comment 28, 2012 SNPRM), at 17.

[346] Association for Competitive Technology (comment 7, 2012 SNPRM), at 2.

[347] *Id.* (''Unlike the game sector, where one developer may have several applications in the top 100, Educational Apps tended to be much closer to a one-to-one ratio between app and creator at 1.54 apps per developer.'').

[348] *Id.* ACT's comment does not describe the methodology it used to categorize apps as being directed to children under 13.

[349] *Id.* at 2–3.

[350] S. Weiner (comment 97, 2012 SNPRM), at 1–2.

[351] J. Garrett (comment 38, 2012 SNPRM), at 1.

[352] ''App Store Metrics,'' 148Apps.biz (accessed Nov. 14, 2012), *available at http://148apps.biz/app-store-metrics;* ''Android Statistic Top Categories,'' AppBrain (accessed Nov. 15, 2012), *available at http://www.appbrain.com/stats/android-market-app-categories.*

[353] Although there are other mobile app platforms and distribution channels, the Commission believes that the education, games, and entertainment categories in the iTunes App Store and the Google Play store adequately approximate the relevant universe of unique mobile app developers whose apps may be directed to children under 13.

[354] In estimating this percentage (and similar percentages throughout this section) for purposes of the PRA analysis, the Commission's staff attempted to err on the side of inclusion to count any apps that were likely to be used by children, whether independently or with parents' assistance. To ensure a generous accounting of operators potentially subject to the Rule, this estimate included, for example, even toddler apps unlikely to be used by children themselves without direct parental assistance.

[355] *See* Mobile Apps for Kids II Report, at 9–10, *supra* note 189.

[356] *See* L. Akemann (comment 2, 2012 SNPRM), at 1; DMA (comment 37, 2011 NPRM), at 7, 14; Scholastic (comment 144, 2011 NPRM), at 13–14; TRUSTe (comment 164, 2011 NPRM), at 5.

[357] *See* Mobile Apps for Kids II Report, at 5–6, 10, *supra* note 189 (14 of 400 apps tested transmitted the mobile device's geolocation or phone number). These apps also transmitted device identification.

[358] The Commission believes it is reasonable to assume, as ACT appears to, that developers responsible for multiple apps directed to children under 13 will typically have a single set of privacy practices, a single privacy policy to describe them, and will develop a single method of disclosing the information required by the final Rule amendments. Any marginal increase in developer burdens addressed in this PRA analysis arising from developers publishing additional apps is therefore not likely to be significant.

with these apps. Dividing 3,300 apps by 1,800 developers yields an iTunes education-apps-per-developer ratio of approximately 1.83,[359] and the Commission assumes this ratio would apply for Android apps, as well. Assuming a 1.83 education-apps-to-developer ratio, it appears that approximately 1,570 developers (2,870) 1.83) are responsible for apps directed to children under 13 that operate in ways likely to implicate the final Rule amendments.

At least one more adjustment to this total of approximately 1,570 potentially affected developers is warranted, however. Commission staff's research for its two Mobile Apps for Kids reports indicate that approximately 2.2% of developers of apps that may be directed to children under 13 develop apps for both iOS and Android.[360] To avoid double-counting developers that develop for both platforms, the Commission subtracts 18 developers from the total (*i.e.,* 1,570 × 2.2% = 34.54; 35) 2 = 17.5), leaving approximately 1,552 potentially affected developers of iOS and Android education apps that may be directed to children under 13.

The Commission believes it is also reasonable to add to this total existing developers of game and entertainment apps directed to children under 13. Commission staff reviewed a list, generated using the desktop version of iTunes, of the Top 200 Paid and Top 200 Free ''Game'' apps in the iTunes App Store as of mid November 2012. Staff believes that approximately 7% of them may be directed to children under 13. Publicly available industry data show that approximately 131,000 game apps were available in the iTunes App Store as of mid-November 2012;[361] thus, approximately 9,170 of those apps may be directed to children under 13. Assuming 5% of those apps operate in ways that bring their developers within the ambit of the final Rule amendments, at a general app-to-developer ratio of 3.8 apps per developer,[362] this yields approximately 120 developers (9,170 × .05 = 458.5; 458.5) 3.8 = 120.66). Commission staff observed that approximately 35% of developers of games that may be directed to children under the age of 13 also develop similar education apps. Thus, of the aforementioned 120 developers, 65% would not already have been counted in the previous tally of educational app developers. This calculation yields an estimate of approximately 78 additional developers of iTunes games apps primarily directed to children under 13 that likely are covered by the final Rule amendments.

Performing a similar calculation for iTunes ''Entertainment'' app developers yields few additional existing developers that are likely to be covered. Commission staff reviewed a list, generated using the desktop version of iTunes, of the Top 200 Paid and Top 200 Free ''Entertainment'' apps in the iTunes App Store as of mid-November 2012. Staff believes that approximately 2.5% of them may be directed to children under 13. Publicly available industry data show that approximately 67,600 ''Entertainment'' apps were available in the iTunes App Store as of mid-November 2012;[363] thus, approximately 1,690 of those apps may be directed to children under 13. Assuming 5% of those apps operate in ways that bring their developers within the ambit of the final Rule amendments, at a general app-to-developer ratio of 3.8 apps per developer, this yields approximately 22 developers (1,690 × .05 = 84.5; 84.5) 3.8 = 22.24). Commission staff observed that approximately 84% of developers of ''Entertainment'' apps that may be directed to children under the age of 13 also develop similar education and game apps. Thus, of the aforementioned 22 developers, 16% would not already have been counted in the previous tally of educational and games app developers. This calculation yields an estimate of approximately 4 additional developers of iTunes entertainment apps primarily directed to children under 13 that likely are covered by the final Rule amendments.

To account for Android ''Games'' apps, Commission staff reviewed listings of the Top 216 Paid and Top 216 Free ''Games'' apps in the Google Play store as of mid-November 2012. Staff believes that approximately 3% of them may be directed to children under 13. Three percent of 75,000 apps[364] yields about 2,250 Android ''Games'' apps that may be directed to children under 13. Assuming 5% of those apps operate in ways that bring their developers within the ambit of the final Rule amendments, at a general app-to-developer ratio of 3.8 apps per developer, this yields approximately 30 developers (2,250 × .05 = 112.5; 112.5) 3.8 = 29.6). Assuming that, as Commission staff observed in the iTunes App Store, approximately 35% of developers of games that may be directed to children under the age of 13 also develop similar education apps, 65% of the aforementioned 30 developers would not already have been counted in the previous tally of educational app developers. This calculation yields an estimate of approximately 19 additional developers of Android games apps primarily directed to children under 13 that likely are covered by the final Rule amendments.

Similarly, for Android ''Entertainment'' apps, Commission staff reviewed listings of the Top 216 Paid and Top 216 Free ''Entertainment'' apps in the Google Play store as of mid-November 2012. Staff believes that approximately 2% of them may be directed to children under 13. Two percent of 67,000 apps[365] yields about 1,340 Android ''Entertainment'' apps that may be directed to children under 13. Assuming 5% of those apps operate in ways that bring their developers within the ambit of the final Rule amendments, at a general app-to-developer ratio of 3.8 apps per developer, this yields approximately 18 developers (1,340 × .05 = 67; 67) 3.8 = 17.63). Assuming that, as Commission staff observed with regard to the iTunes App Store, approximately 84% of developers of entertainment apps that may be directed to children under the age of 13 also develop similar education and game apps, 16% of the aforementioned 18 developers would not already have been counted in the prior tally of educational and game app developers. This calculation yields an estimate of approximately 3 additional developers of Android entertainment apps primarily directed to children

[359] This appears to be a larger universe of data than ACT consulted in generating its education-apps-to-developer ratio of 1.54. *See* Association for Competitive Technology (comment 7, 2012 SNPRM), at 2. Data from the industry source ACT cites indicate a more general apps-to-developer ratio of approximately 3.8 apps per developer of iTunes App Store apps. *See* ''App Store Metrics,'' 148Apps.biz (accessed Nov. 14, 2012), *available at http://148apps.biz/app-store-metrics* (727,938 Total Active Apps; 191,366 Active Publishers in the U.S. App Store).

[360] *See* Mobile Apps for Kids II Report, at 26, *supra* note 189 (approximately 1.6% of developers of apps studied developed apps for both Android and iOS); FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing,* at 8–9 (Feb. 2012), *available at http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf* (approximately 2.7% of developers of apps studied developed apps for both Android and iOS). Averaging these two percentages indicates developer overlap of approximately 2.2%.

[361] ''App Store Metrics,'' 148 Apps.biz (accessed Nov. 14, 2012), *available at http://148apps.biz/app-store-metrics.*

[362] *See* note 357, *supra.*

[363] ''App Store Metrics,'' 148Apps.biz (accessed Nov. 14, 2012), *available at http://148apps.biz/app-store-metrics.*

[364] ''Android Statistic Top Categories,'' AppBrain (accessed Nov. 15, 2012), *available at http://www.appbrain.com/stats/android-market-app-categories* (total calculated by adding the number of apps in each ''Games'' subcategory).

[365] *Id.*

under 13 that likely are covered by the final Rule amendments.

Thus, the FTC estimates that approximately 1,660 mobile app developers (1,552 for iTunes and Android education apps + 78 for iTunes games apps + 4 for iTunes entertainment apps + 19 for Android games apps + 3 for Android entertainment apps = 1,656) are existing operators of Web sites or online services that will be covered by the final Rule amendments. The FTC's 2011 NPRM PRA estimate of 2,000 existing operators already covered by the Rule and its 2012 SNPRM PRA estimate of 500 newly covered existing operators,[366] however, already partially accounted for these mobile app developers because these estimates covered all types of operators subject to COPPA, including mobile app developers. As discussed above, comments on the FTC staff's estimate of the number of existing operators focused almost entirely on an asserted understatement of the number of mobile app developers that would be covered by the final Rule amendments. The estimate otherwise was not contested. Thus, the total numbers of mobile app developers set forth herein must be substituted for the total (unspecified) number of mobile app developers subsumed within the 2011 NPRM and 2012 SNPRM PRA estimates.

The Commission believes it is reasonable to substitute the above-noted estimate of 1,660 mobile app developers for half, *i.e.,* 1,250, of the 2,500 existing operators previously estimated to be ''covered'' and ''newly covered'' by the 2011 NPRM and 2012 SNPRM PRA estimates. Based on its experience, the Commission believes that half—if not more—of the existing operators currently covered by the Rule already develop or publish mobile apps. The remaining 1,250 operators would account for traditional Web site and other online service providers that are not mobile app developers, as well as plug-in developers and advertising networks that could be covered by the ''actual knowledge'' standard.[367] Thus, combining these totals (1,660 + 1,250) yields a total of 2,910 operators of existing Web sites or online services that would likely be covered by the final Rule amendments.

New Operators

The Commission received one comment asserting that the Commission significantly underestimated the number of new operators per year that will be covered by the proposed Rule amendments. One commenter, the moderator of an online group called ''Parents With Apps,'' stated that this group of more than 1,400 small developers of family-friendly apps grows by at least 100 new developers every six months.[368] This would constitute an annual growth rate of nearly 15% (200 new developers per year divided by 1,400 developers in the group = 0.1429). Although the Commission believes this rate of increase is due, at least in part, to increased awareness among developers of the group's existence rather than growth in the number of new developers, the Commission concludes it is reasonable to incorporate this information into its revised estimate. Assuming a base number of 1,660 existing mobile app developers estimated to be covered by the final Rule amendments, a 15% growth rate would yield, year-over-year after three years, an additional 864 new developers, or approximately 290 per year averaged over a prospective three-year clearance ($1{,}660 \times 1.15 = 1{,}909$; $1{,}909 \times 1.15 = 2{,}195$; $2{,}195 \times 1.15 = 2{,}524$; $2{,}524 - 1{,}660 = 864$; $864 \div 3 = 288$).[369]

Bureau of Labor Statistics (''BLS'') projections suggest a much more modest rate of growth. BLS has projected that employment of software application developers will increase 28% between 2010 and 2020.[370] Assuming 10% of that total 28% growth would occur each year of the ten-year period, and a base number of 1,660 existing mobile app developers, one can derive an increase of approximately 46 ($1{,}645 \times 0.028 = 46.48$) new mobile app developers per year on average that will be covered by the final Rule amendments. Combining the average based on the annual growth rate of Parents With Apps and that based on the BLS software application developer growth projection yields an increase of approximately 168 (290 + 46 = 336; 336 ÷ 2 = 168) new mobile app developers per year on average that will be covered by the proposed Rule amendments.

As with its previous estimates of existing developers, mobile app developers were already included in the Commission's 2011 NPRM PRA estimate of 100 new operators and the Commission's 2012 SNPRM PRA estimate of 125 additional new operators per year. As noted above, the Commission's 2011 NPRM and 2012 SNPRM PRA estimates of new operators were contested only as they relate to their estimation of new mobile app developers. Thus, the total number of new mobile app developers set forth herein should replace the total (unspecified) number of new mobile app developers subsumed within the 2011 NPRM and 2012 SNPRM PRA estimates.

The Commission believes it is reasonable to substitute the above-noted estimate of 168 mobile app developers for half, *i.e.,* 113, of the 225 new operators previously estimated to be covered by the 2011 NPRM and 2012 SNPRM PRA estimates. The remainder of the prior estimates would account for new Web site and other online service providers other than new mobile app developers, as well as new plug-in developers and advertising networks that could be covered by the ''actual knowledge'' standard. Thus, combining these totals (168 + 113 = 281) yields a total of approximately 280 new operators per year (over a prospective three-year clearance) of Web sites or online services that would likely be covered by the final Rule amendments. Given that the FTC's existing clearance already accounts for an estimate of 100 new operators,[371] the incremental calculation for additional OMB clearance is 180 new operators × 60 hours each = 10,800 hours.

*C. Recordkeeping*

Under the PRA, the term ''recordkeeping requirement'' means a requirement imposed by or for an agency on persons to maintain specified records, including a requirement to (A) Retain such records; (B) notify third parties, the Federal Government, or the public of the existence of such records; (C) disclose such records to third parties, the Federal Government, or the public; or (D) report to third parties, the Federal Government, or the public

[366] *See* 2011 NPRM, 76 FR at 59812, 59813; 2012 SNPRM, 77 FR at 46649.

[367] Disclosure burdens do not increase when taking into account plug-in developers and advertising networks with actual knowledge because the burden will fall on either the primary-content site or the plug-in, but need not fall on both. They can choose to allocate the burden between them. The Commission has chosen to account for the burden via the primary-content site or service because it would generally be the party in the best position to give notice and obtain consent from parents.

[368] S. Weiner (comment 97, 2012 SNPRM), at 1–2.

[369] *See also* Association for Competitive Technology (comment 5, 2011 SNPRM), at 2 (''total unique apps across all platforms continue to grow beyond the one million mark'' since Apple's 2008 launch of its App Store; ''[t]he mobile app marketplace has grown to a five billion dollar industry from scratch in less than four years.'').

[370] Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Outlook Handbook, 2012–13 Edition,* Software Developers, *http://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm* (visited November 16, 2012).

[371] *See* note 342, *supra.*

regarding such records.'' The final amendments do not affect the Rule's existing recordkeeping requirements. Moreover, FTC staff believes that most of the records listed in the Rule's pre-existing safe harbor recordkeeping provisions consist of documentation that such parties have kept in the ordinary course of business irrespective of the Rule.[372] Any incremental burden, such as that for maintaining the results of independent assessments under section 312.11(d), would be, in staff's view, marginal.

*D. Disclosure Hours*

(1) New Operators' Disclosure Burden

Under the existing OMB clearance for the Rule, the FTC has estimated that new operators will each spend approximately 60 hours to craft a privacy policy, design mechanisms to provide the required online privacy notice and, where applicable, direct notice to parents in order to obtain verifiable consent. Several commenters noted that this 60-hour estimate failed to take into account accurate costs of compliance with the Rule, but they did not provide the Commission with empirical data or specific evidence on the number of hours such activities require.[373] The Toy Industry Association (''TIA'') [374] asserts that the Commission underestimated the number of hours shown in the 2011 NPRM and 2012 SNPRM PRA calculations,[375] and that ''[d]epending on the FTC's final revisions to the COPPA Rule, the time it takes to implement technological changes could more than triple the Commission's 60-hour estimate.'' [376] These assertions appear to be based primarily on TIA's concern that the FTC's estimate did not include costs ''of 'ensuring' security procedures of third parties, securing deletion, managing parental consents, or updating policies to disclose changes in 'operators.' In addition, the FTC seems to reference only top level domains and, as such, its estimates for implementation of new verifiable parental consent requirements are very low.'' [377] TIA states that ''the additional processes and procedures mandated under the revised proposed Rule will potentially include privacy policy and operational changes, with related resource-intensive measures, such as organizational management and employee training.'' [378] Moreover, TIA suggests that changes proposed in the 2011 NPRM to the treatment of screen or user names would entail ''enormous'' costs that the FTC did not quantify.[379]

Substantially all of TIA's concerns about understated burden estimates relate to proposed requirements that the Commission has ultimately determined not to adopt. For example, the final Rule amendments do not require operators to ''ensure'' that third-parties secure information, but that they ''take reasonable steps'' to release children's information only to third parties capable of maintaining it securely and provide assurances that they will do so.[380] The Commission is not eliminating the ''single operator designee'' proviso of the Rule's online notice requirement.[381] It is not eliminating email plus as an acceptable consent method for operators collecting personal information only for internal use.[382] The Commission determined to treat screen names as *personal information* only in those instances in which a screen or user name rises to the level of *online contact information.*[383] Thus, in the Commission's view, TIA's proposed increase to the above-noted estimate of 60 hours for compliance is not warranted.[384]

Applying, then, the 60 hours estimate to the portion of new operators not accounted for in the FTC's previously cleared burden totals yields a cumulative total of 10,800 hours (180 new operators × 60 hours each).

(2) Existing Operators' Disclosure Burden

The final Rule amendments will not impose ongoing incremental disclosure time per entity, but, as noted above, would result in an estimated 2,910 existing operators covered by the Rule. These entities will 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 a prospective three-year OMB clearance under the PRA. Commission staff believes that an existing operator's time to make these changes would be no more than that for a new entrant crafting its online and direct notices for the first time, *i.e.,* 60 hours. Annualized over three years of a prospective clearance,[385] this amounts to 20 hours ((60 hours + 0 + 0) ÷ 3) per year. Aggregated for the estimated 2,910 existing operators that would be subject to the Rule, annualized disclosure burden would be 58,200 hours per year.

*E. Reporting Hours*

The final Rule amendments do not impose reporting requirements on operators; they do, however, for safe harbor programs. Under the FTC's already cleared estimates, pre-amendments, staff projected that each new safe harbor program applicant

[372] Under 5 CFR 1320.3(b)(2), OMB excludes from the definition of PRA ''burden'' the time and financial resources needed to comply with agency-imposed recordkeeping, disclosure, or reporting requirements that customarily would be undertaken independently in the normal course of business. Thus, on further reflection, the FTC has determined not to include recordkeeping costs for safe harbors as it did in the 2011 NPRM PRA analysis.

[373] *See* N. Savitt (comment 142, 2011 NPRM), at 1; NCTA (comment 113, 2011 NPRM), at 23–24.

[374] TIA contends that in the 2012 SNPRM, the Commission ''disregarded the empirical economic input'' regarding compliance costs that TIA had submitted in response to the 2011 NPRM, including hour and labor cost estimates. Toy Industry Association (comment 89, 2012 SNPRM), at 16. Although the Commission did not discuss TIA's 2011 comments in the SNPRM—which focused on the potential incremental compliance cost changes that the Commission anticipated would flow from certain newly proposed Rule amendments—it has considered TIA's 2011 and 2012 comments on compliance costs as discussed herein.

[375] Toy Industry Association (comment 89, 2012 SNPRM), at 16–17; Toy Industry Association (comment 163, 2011 NPRM), at 17–18; *see also* DMA (comment 28, 2012 SNPRM), at 17.

[376] Toy Industry Association (comment 163, 2011 NPRM), at 18.

[377] *Id.* at 17. Also with specific regard to potential costs associated with obtaining and verifying parental consent, TIA estimates that dedicating employees specifically to this task would, if the FTC were to require a ''scanned form type of control regime,'' require additional salary and benefit costs. *Id.* at 18.

[378] *Id.* at 17.

[379] *Id.* at 18.

[380] *See* Part II.D., *supra.* As for the ''reasonable steps'' requirement, the time and financial resources operators devote to this task would likely be incurred, anyway, in the normal course of their seeking to preserve the security of children's data conveyed to those third parties. To reiterate, PRA ''burden'' does not include effort expended in the ordinary course of business independent of a regulatory requirement. 5 CFR 1320.3(b)(2). *See also* Toy Industry Association (comment 163, 2011 NPRM), at 16 (''Operators regularly investigate agents, service providers, and business partners to assure that they will responsibly maintain the security and confidentiality of children's data . * * *'').

[381] *See* Part II.B.2, *supra.*

[382] *See* Part II.C.7, *supra.* Furthermore, the requirement to obtain parental consent is not a collection of information under the PRA.

[383] *See* Part II.A.5.a, *supra.* This change also appears to moot NCTA's concern that operators would be faced with substantial costs if ''forced to redesign'' Web sites to eliminate the use of unique screen or user names. NCTA (comment 113, 2011 NPRM), at 23 n.69.

[384] TIA also cites the potential cost of needing to ''develop communication tools and respond to complaints from parents who may mistakenly believe that companies are altering data collection practices. * * *'' Toy Industry Association (comment 163, 2011 NPRM), at 18. This speculative cost does not relate to any ''information collection requirement'' in the final Rule amendments.

[385] TIA states that this first-year cost associated with compliance should not be ''amortized'' over three years. Toy Industry Association (comment 89, 2012 SNPRM), at 17. As stated *supra* note 336, however, agencies may seek up to three years of clearance from OMB, and this is what the FTC routinely does for rulemakings. Moreover, OMB seeks estimates of annual burden (reflective of the clearance period sought). *See* 5 CFR 1320.5(a)(1)(iv)(B).

would require 265 hours to prepare and submit its safe harbor proposal.[386] The final Rule amendments, however, require a safe harbor applicant to submit a more detailed proposal than what the Rule, prior to such amendments, mandated. 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 have under the original Rule. The FTC estimates this added information will entail approximately 60 additional hours for each new, and each existing, safe harbor to prepare. Accordingly, for this added one-time preparation, the aggregate incremental burden is 60 hours for the projected one new safe harbor program per three-year clearance cycle and 300 hours, cumulatively, for the five existing safe harbor programs. Annualized for an average single year per three-year clearance, this amounts to 20 hours for one new safe harbor program, and 100 hours for the existing five safe harbor programs; thus, cumulatively, the burden is 120 hours.

The final Rule amendments require safe harbor programs to audit their members at least annually and to submit periodic reports to the Commission on the aggregate results of these member audits. As such, this will increase currently cleared burden estimates pertaining to safe harbor applicants. The burden for conducting member audits and preparing these reports likely will vary for each safe harbor program depending on the number of members. Commission staff estimates that conducting audits and preparing reports will require approximately 100 hours per program per year. Aggregated for one new (100 hours) and five existing (500 hours) safe harbor programs, this amounts to an increased disclosure burden of 600 hours per year. Accordingly, the annualized reporting burden for one new and five existing safe harbor applicants to provide the added information required (120 hours) and to conduct audits and prepare reports (600 hours) is 720 hours, cumulatively.

*F. Labor Costs*

(1) Disclosure

The Commission assumes that the time spent on compliance for new operators and existing operators covered by the final Rule amendments would be apportioned five to one between legal (lawyers or similar professionals) and technical (*e.g.,* computer programmers, software developers, and information security analysts) personnel.[387] In the 2012 SNPRM, based on BLS compiled data, FTC staff assumed for compliance cost estimates a mean hourly rate of $180 for legal assistance and $42 for technical labor support.[388] These estimates were challenged in the comments.

TIA asserts that the Commission underestimates the labor rate for lawyers used in the Commission's 2011 NPRM and 2012 SNPRM compliance cost calculations.[389] Given the comments received, the Commission believes it appropriate to increase the estimated mean hourly rate of $180 for legal assistance used in certain of the Commission's 2011 NPRM and 2012 SNPRM compliance cost calculations. TIA stated in its 2011 comment that the ''average rates'' of ''specialized attorneys who understand children's privacy and data security laws'' with whom its members typically consult are ''2–3 times the Commission's estimates'' of $150 per hour set forth in the 2011 NPRM.[390] TIA reiterated this information in its 2012 comment[391] and added: ''According to *The National Law Journal's* 2011 annual billing survey, the average hourly firm-wide billing rate (which combines partner and associate rates) ranges from $236 to $633, not taking into account any area of specialization.'' [392] While the Commission believes TIA's information provides useful reference points, it does not provide an adequate basis for estimating an hourly rate for lawyers for compliance cost calculation purposes.

As an initial matter, the Commission notes that TIA has cited a range of average hourly rates that its members pay for counsel, not a single average hourly rate, and it did not submit the underlying data upon which those average rate calculations were based. The range of average hourly rates TIA stated that its members typically pay (*i.e.,* $300–$450 per hour) may include some unusually high or low billing rates that have too much influence on the arithmetic means for those averages to be representative of the rates operators are likely to have to pay.[393] Without more information about the distribution of the underlying rates factored into each average, or the distribution of the averages within the cited range, TIA's information is of limited value. Likewise, as TIA's comments appear to implicitly recognize, routine COPPA compliance counseling would likely be performed by a mix of attorneys billed at a range of hourly rates. Unfortunately, the information submitted in TIA's comments does not indicate how that workload is typically apportioned as between ''high-level partner[s]'' whose ''support'' is required for ''complex'' COPPA compliance matters and other, less senior, attorneys at a law firm. The *National Law Journal* survey the TIA cites is also a useful reference point, but it is a non-scientific survey of the nation's 250 largest law firms [394] that are located predominantly in major metropolitan areas.[395] Beyond the range of average hourly firm-wide billing rates that TIA cites, the survey states that the

[386] 76 FR at 7211, 7212 (Feb. 9, 2011); 76 FR at 31334, 31335 (May 31, 2011). These safe harbor reporting hour estimates have not been contested. 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.

[387] *See* 76 FR at 7211, 7212–7213 (Feb. 9, 2011); 76 FR at 31334, 31335 n.1 (May 31, 2011) (FTC notices for renewing OMB clearance for the COPPA Rule).

[388] As explained in the 2012 SNPRM, ''[t]he estimated rate of $180 is roughly midway between [BLS] mean hourly wages for lawyers ($62.74) in the most recent annual compilation available online [as of August 2012] and what Commission staff believes more generally reflects hourly attorney costs ($300) associated with Commission information collection activities.'' 77 FR at 46651, n.54. This estimated rate was an upward revision of the Commission's estimate of $150 per hour used in the 2011 NPRM. *See* 76 FR at 59827 n.204 and accompanying text. The estimated mean hourly wages for technical labor support ($42) is based on an average of the salaries for computer programmers, software developers, information security analysts, and web developers as reported by the BLS. *See National Occupational and Wages—May* 2011, *available at http://www.bls.gov/news.release/archives/ocwage_03272012.pdf.*

[389] Toy Industry Association (comment 89, 2012 SNPRM), at 16; Toy Industry Association (comment 163, 2011 NPRM), at 17.

[390] Toy Industry Association (comment 163, 2011 NPRM), at 17. *See also* NCTA (comment 113, 2011 NPRM), at 23 n.70 (''NCTA members typically consult with attorneys who specialize in data privacy and security laws and whose average rates are 2–3 times the Commission's [2011 NPRM] estimates [of $150 per hour].'').

[391] Toy Industry Association (comment 89, 2012 SNPRM), at 18.

[392] *Id.,* at 10 (*citation omitted*).

[393] *See* Federal Judicial Center, Reference Manual on Scientific Evidence (3rd Ed.), David H. Kay and David A. Freedman, Reference Guide on Statistics at 238 (''[t]he mean takes account of all the data B it involves the total of all the numbers; however, particularly with small datasets, a few unusually large or small observations may have too much influence on the mean.'').

[394] Toy Industry Association (comment 89, 2012 SNPRM), at 19. Fifty-one law firms supplied the average rate information used in the survey's tabulation, ''A nationwide sampling of law firm billing rates,'' to which the TIA appears to refer.

[395] The Commission recognizes that many attorneys who specialize in COPPA compliance and data security law often work at large law firms located in major metropolitan areas. However, just as the nature of online technology and the mobile marketplace allow operators to live almost anywhere, *see* Association for Competitive Technology (comment 5, 2011 NPRM), at 2 (the ''nature of this industry allows developers to live almost anywhere''), it also allows them to seek the counsel of competent lawyers practicing anywhere in the United States.

average firm-wide billing rate (partners and associates) in 2011 was $403, the average partner rate was $482, and the average associate rate was $303.

The Commission believes it reasonable to assume that the workload among law firm partners and associates for COPPA compliance questions could be competently addressed and efficiently distributed among attorneys at varying levels of seniority, but would be weighted most heavily to more junior attorneys. Thus, assuming an apportionment of two-thirds of such work is done by associates, and one-third by partners, a weighted average tied to the average firm-wide associate and average firm-wide partner rates, respectively, in the *National Law Journal* 2011 survey would be about $365 per hour. The Commission believes that this rate B which is very near the mean of TIA's stated range of purported hourly rates that its members typically pay to engage counsel for COPPA compliance questions B is an appropriate measure to calculate the cost of legal assistance for operators to comply with the final Rule amendments.[396]

TIA also states that the 2012 SNPRM estimate of $42 per hour for technical support is too low, and that engaging expert technical personnel can, on average, involve hourly costs that range from $72 to $108.[397] Similar to TIA's hours estimate, discussed above, the Commission believes that TIA's estimate may have been based on implementing requirements that, ultimately, the Commission has determined not to adopt. For example, technical personnel will not need to ''ensure'' the security procedures of third parties; operators that have been eligible to use email plus for parental consents will not be required to implement new systems to replace it. It is unclear whether TIA's estimate for technical support is based on the types of disclosure-related tasks that the final Rule amendments would actually require, other tasks that the final Rule amendments would not require, or non-disclosure tasks not covered by the PRA. Moreover, unlike its estimate for lawyer assistance, TIA's estimates for technical labor are not accompanied by an adequate explanation of why estimates for technical support drawn from BLS statistics are not an appropriate basis for the FTC's PRA analysis. Accordingly, the Commission believes it is reasonable to retain the 2012 SNPRM estimate of $42 per hour for technical assistance based on BLS data.

Thus, for the 180 new operators per year not previously accounted for under the FTC's currently cleared estimates, 10,800 cumulative disclosure hours would be composed of 9,000 hours of legal assistance and 1,800 hours of technical support. Applied to hourly rates of $365 and $42, respectively, associated labor costs for the 180 new operators potentially subject to the proposed amendments would be $3,360,600 (*i.e.,* $3,285,000 for legal support plus $75,600 for technical support).

Similarly, for the estimated 2,910 existing operators covered by the final Rule amendments, 58,200 cumulative disclosure hours would consist of 48,500 hours of legal assistance and 9,700 hours for technical support. Applied at hourly rates of $365 and $42, respectively, associated labor costs would total $18,109,900 (*i.e.,* $17,702,500 for legal support plus $407,400 for technical support). Cumulatively, estimated labor costs for new and existing operators subject to the final Rule amendments is $21,470,500.

(2) Reporting

The Commission staff assumes that the tasks to prepare augmented safe harbor program applications occasioned by the final Rule amendments will be performed primarily by lawyers, at a mean labor rate of $180 an hour.[398] Thus, applied to an assumed industry total of 120 hours per year for this task, incremental associated yearly labor costs would total $21,600.

The Commission staff assumes periodic reports will be prepared by compliance officers, at a labor rate of $28 per hour.[399] Applied to an assumed industry total of 600 hours per year for this task, associated yearly labor costs would be $16,800.

Cumulatively, labor costs for the above-noted reporting requirements total approximately $38,400 per year.

*G. 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 new notice requirements, the final Rule amendments should not impose any additional capital or other non-labor costs.[400]

**List of Subjects in 16 CFR Part 312**

Children, Communications, Consumer protection, Electronic mail, Email, Internet, Online service, Privacy, Record retention, Safety, science and technology, Trade practices, Web site, Youth.

■ Accordingly, for the reasons stated above, the Federal Trade Commission revises part 312 of Title 16 of the Code of Federal Regulations to read as follows:

## PART 312—CHILDREN'S ONLINE PRIVACY PROTECTION RULE

Sec.

312.1 Scope of regulations in this part.
312.2 Definitions.
312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.
312.4 Notice.
312.5 Parental consent.
312.6 Right of parent to review personal information provided by a child.
312.7 Prohibition against conditioning a child's participation on collection of personal information.

[396] *Cf.* Civil Division of the United States Attorney's Office for the District of Columbia, United States Attorney's Office, District of Columbia, Laffey Matrix B 2003-2013, *available at http://www.justice.gov/usao/dc/divisions/Laffey_Matrix_2003-2013.pdf* (updated ''Laffey Matrix'' for calculating ''reasonable'' attorneys fees in suits in which fee shifting is authorized can be evidence of prevailing market rates for litigation counsel in the Washington, DC area; rates in table range from $245 per hour for most junior associates to $505 per hour for most senior partners).

[397] Toy Industry Association (comment 89, 2012 SNPRM), at 18.

[398] Based on Commission staff's experience with previously approved safe harbor programs, staff anticipates that most of the legal tasks associated with safe harbor programs will be performed by in-house counsel. *Cf.* Toy Industry Association (comment 89, 2012 SNPRM), at 19 (regional BLS statistics for lawyer wages can support estimates of the level of in-house legal support likely to be required on an ongoing basis). Moreover, no comments were received in response to the February 9, 2011 and May 31, 2011 **Federal Register** notices (76 FR at 7211 and 76 FR at 31334, respectively, *available at http://www.gpo.gov/fdsys/pkg/FR-2011-02-09/pdf/2011-2904.pdf* and *http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13357.pdf*), which assumed a labor rate of $150 per hour for lawyers or similar professionals to prepare and submit a new safe harbor application. Nor was that challenged in the comments responding to the 2011 NPRM.

[399] *See* 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.* This rate has not been contested.

[400] NCTA commented that the Commission failed to consider costs ''related to redeveloping child-directed Web sites'' that operators would be ''forced'' to incur as a result of the proposed Rule amendments, including for ''new equipment and software required by the expanded regulatory regime.'' NCTA (comment 113, 2011 NPRM), at 23. Similarly, TIA commented that the proposed Rule amendments would entail ''increased monetary costs with respect to technology acquisition and implementation * * *.'' Toy Industry Association (comment 163, 2011 NPRM), at 17. These comments, however, do not specify projected costs or which Rule amendments would entail the asserted costs.

312.8 Confidentiality, security, and integrity of personal information collected from children.
312.9 Enforcement.
312.10 Data retention and deletion requirements.
312.11 Safe harbor programs.
312.12 Voluntary Commission Approval Processes.
312.13 Severability.

**Authority:** 15 U.S.C. 6501–6508.

### § 312.1 Scope of regulations in this part.

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

### § 312.2 Definitions.

*Child* means an individual under the age of 13.

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

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

(2) 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

(3) Passive tracking of a child online.

*Commission* means the Federal Trade Commission.

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

*Disclose or disclosure* means, with respect to personal information:

(1) 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 Web site or online service; and

(2) 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 Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

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

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

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

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

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

*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.

*Operator* means any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45). Personal information is *collected or maintained on behalf of* an operator when:

(1) It is collected or maintained by an agent or service provider of the operator; or

(2) The operator benefits by allowing another person to collect personal information directly from users of such Web site or online service.

*Parent* includes a legal guardian.

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

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

(1) A first and last name;

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

(3) Online contact information as defined in this section;

(4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

(5) A telephone number;

(6) A Social Security number;

(7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is 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;

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

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

(10) 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 Web site or online service means:*

(1) Those activities necessary to:

(i) Maintain or analyze the functioning of the Web site or online service;

(ii) Perform network communications;

(iii) Authenticate users of, or personalize the content on, the Web site or online service;

(iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

(v) Protect the security or integrity of the user, Web site, or online service;

(vi) Ensure legal or regulatory compliance; or

(vii) Fulfill a request of a child as permitted by § 312.5(c)(3) and (4);

(2) So long as The information collected for the activities listed in paragraphs (1)(i)–(vii) of this definition is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a

profile on a specific individual, or for any other purpose.

*Third party* means any person who is not:

(1) An operator with respect to the collection or maintenance of personal information on the Web site or online service; or

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

*Web site or online service directed to children* means a commercial Web site or online service, or portion thereof, that is targeted to children.

(1) In determining whether a Web site or online service, or a portion thereof, is directed 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 Web site or online service, as well as whether advertising promoting or appearing on the Web site 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.

(2) A Web site or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children.

(3) A Web site or online service that is directed to children under the criteria set forth in paragraph (1) of this definition, but that does not target children as its primary audience, shall not be deemed directed to children if it:

(i) Does not collect personal information from any visitor prior to collecting age information; and

(ii) Prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part.

(4) A Web site or online service shall not be deemed directed to children solely because it refers or links to a commercial Web site or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

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

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

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

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

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

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

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

**§ 312.4 Notice.**

(a) *General principles of notice.* It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

(b) *Direct notice to the 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 personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(c) *Content of the direct notice to the parent*—(1) *Content of the direct notice to the parent 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, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;

(ii) That the parent's consent is required for the collection, use, or disclosure of such information, 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, or the potential opportunities for the disclosure of personal information, should the parent provide consent;

(iv) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section;

(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 under § 312.5(c)(2) (Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information).* Where an operator chooses to notify a parent of a child's participation in a Web site or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the 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, and subsequently update the parent about, a child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information;

(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 child's participation in the Web site 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 paragraph (d) of this section.

(3) *Content of the direct notice to the parent 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 paragraph (d) of this section.

(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 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 paragraph (d) of this section.

(d) *Notice on the Web site or online service.* In addition to the direct notice to the parent, an operator 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 Web site or online service, *and,* at each area of the Web site 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 Web site or online service that has a separate children's area 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 Web site or online service's information practices must state the following:

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

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

(3) That the parent can review or 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.

### § 312.5 Parental consent.

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

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

(b) *Methods for verifiable parental consent.* (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or

(vi) *Provided that,* an operator that does not ''disclose'' (as defined by § 312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email 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. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

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

(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 the name or online contact information of the parent or child 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 purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a Web site 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 online contact information from a child 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 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;

(5) Where the purpose of collecting a child's and a parent's name and 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 purpose of collecting a child's name and online contact information is to:

(i) Protect the security or integrity of its Web site 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;

(7) Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service. In such case, there also shall be no obligation to provide notice under § 312.4; or

(8) Where an operator covered under paragraph (2) of the definition of *Web site or online service directed to children* in § 312.2 collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4.

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

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

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

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

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

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

(ii) Not be unduly burdensome to the parent.

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

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

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

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

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

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

**§ 312.9 Enforcement.**

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

**§ 312.10 Data retention and deletion requirements.**

An operator of a Web site 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.

**§ 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) By July 1, 2014, and annually thereafter, submit a report to the Commission containing, at a minimum, an aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section, a description of any disciplinary action taken against any subject operator under paragraph (b)(3) of this section, and a description of any approvals of member operators' use of a 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) of this section.

(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) of this section. The statement required under paragraph (c)(4) of this section 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, by March 1, 2013, 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).

### § 312.12 Voluntary Commission Approval Processes.

(a) *Parental consent methods.* An interested party may file a written request for Commission approval of parental consent methods not currently enumerated in § 312.5(b). To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(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 120 days of the filing of the request; and

(b) *Support for internal operations of the Web site or online service.* An interested party may file a written request for Commission approval of additional activities to be included within the definition of support for internal operations. To be considered for approval, a party must provide a detailed justification why such activities should be deemed support for internal operations, and an analysis of their potential effects on children's online privacy. 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 120 days of the filing of the request.

### § 312.13 Severability.

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

By direction of the Commission, Commissioner Rosch abstaining, and Commissioner Ohlhausen dissenting.

**Donald S. Clark,**

*Secretary.*

## Dissenting Statement of Commissioner Maureen K. Ohlhausen

I voted against adopting the amendments to the Children's Online Privacy Protection Act (COPPA) Rule because I believe a core provision of the amendments exceeds the scope of the authority granted us by Congress in COPPA, the statute that underlies and authorizes the Rule.[401] Before I explain my concerns, I wish to commend the Commission staff for their careful consideration of the multitude of issues raised by the numerous comments in this proceeding. Much of the language of the amendments is designed to preserve flexibility for the industry while striving to protect children's privacy, a goal I support strongly. The final proposed amendments largely strike the right balance between protecting children's privacy online and avoiding undue burdens on providers of children's online content and services. The staff's great expertise in the area of children's privacy and deep understanding of the values at stake in this matter have been invaluable in my consideration of these important issues.

In COPPA Congress defined who is an operator and thereby set the outer boundary for the statute's and the COPPA Rule's reach.[402] It is undisputed that COPPA places obligations on operators of Web sites or online services directed to children or operators with actual knowledge that they are collecting personal information from children. The statute provides, ''It is unlawful for an operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed [by the FTC].'' [403]

The Statement of Basis and Purpose for the amendments (SBP) discusses concerns that the current COPPA Rule may not cover child-directed Web sites or services that do not themselves collect children's personal information but may incorporate third-party plug-ins that collect such information [404] for the plug-ins' use but do not collect or maintain the information for, or share it with, the child-directed site or service. To address these concerns, the amendments add a new proviso to the definition of operator in the COPPA Rule: ''Personal information is collected or maintained on behalf of an operator when: (a) it is collected or maintained by an agent or service provider of the operator; or (b) the operator benefits by allowing another person to collect personal information directly from users of such Web site or online service.'' [405]

The proposed amendments construe the term ''on whose behalf such information is collected and maintained'' to reach child-directed Web sites or services that merely derive from a third-party plug-in some kind of benefit, which may well be unrelated to the collection and use of children's information (*e.g.,* content, functionality, or advertising revenue). I find that this proviso—which would extend COPPA obligations to entities that do not collect personal information from children or have access to or control of such information collected by a third-party does not comport with the plain meaning of the statutory definition of an operator in COPPA, which covers only entities ''on whose behalf such information is collected and maintained.'' [406] In other words, I do not believe that the fact that a child-directed site or online service receives any kind of benefit from using a plug-in is equivalent to the collection of personal information by the third-party plug-in on behalf of the child-directed site or online service.

As the Supreme Court has directed, an agency ''must give effect to the unambiguously expressed intent of Congress.'' [407] Thus, regardless of the policy justifications offered, I cannot support expanding the definition of the term ''operator'' beyond the statutory parameters set by Congress in COPPA.

I therefore respectfully dissent.

[FR Doc. 2012–31341 Filed 1–16–13; 8:45 am]

**BILLING CODE 6750–01–P**

[401] 15 U.S.C. 6501–6506.

[402] COPPA, 15 U.S.C. 6501(2), defines the term ''operator'' as ''any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about users of or visitors to such Web site or online service, or on whose behalf such information is collected and maintained * * *'' As stated in the Statement of Basis and Purpose for the original COPPA Rule, ''The definition of 'operator' is of central importance because it determines who is covered by the Act and the Rule.'' Children's Online Privacy Protection Rule 64 FR 59888, 59891 (Nov. 3, 1999) (final rule).

[403] 15 U.S.C. 6502(a)(1).

[404] If the third-party plugs-ins are child-directed or have actual knowledge that they are collecting children's personal information they are already expressly covered by the COPPA statute. Thus, as the SBP notes, a behavioral advertising network that targets children under the age of 13 is already deemed an operator. The amendment must therefore be aimed at reaching third-party plug-ins that are either not child-directed or do not have actual knowledge that they are collecting children's personal information, which raises a question about what harm this amendment will address. For example, it appears that this same type of harm could occur through general audience Web sites and online services collecting and using visitors' personal information without knowing whether some of the data is children's personal information, which is a practice that COPPA and the amendments do not prohibit.

[405] 16 CFR 312.2 (Definitions).

[406] This expanded definition of operator reverses the Commission's previous conclusion that the appropriate test for determining an entity's status as an operator is to ''look at the entity's relationship to the data collected,'' using factors such as ''who owns and/or controls the information, who pays for its collection and maintenance, the pre-existing contractual relationships regarding collection and maintenance of the information, and the role of the Web site or online service in collecting and/or maintaining the information (*i.e.,* whether the site participates in collection or is merely a conduit through which the information flows to another entity.)'' Children's Online Privacy Protection Rule 64 FR 59888, 59893, 59891 (Nov. 3, 1999) (final rule).

[407] *Chevron* v. *Natural Resources Defense Council, Inc.,* 467 U.S. 837, 842–43 (1984) (''When a court reviews an agency's construction of the statute which it administers, it is confronted with two questions. First, always, is the question whether Congress has directly spoken to the precise question at issue. If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress.'').