$ 3 3 (1 ' , ; $

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 change in online technology since the Rule went into effect in April 2000. The final amended Rule includes modifications t

the definitions of en•s (t61)Tj Te4om9e3j -0.R, T* (persoion)Tj 00uN1[cl 1lC76.0-0.1 1 Tfy the scw T* (the definit 1lC76.0-0.1 168Tu0 7.4445.1
amendea RuStaterequnitions nd RulPurposT* (Rule (SBP217Rule should be le a042 Tequnto:lPubliciRefer cogyBranch0•),) 0 Td (Federal Tra

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

[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.

••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 sect hmto tb T*ission•s st* (scesCcan2h2on•s stpld.)Tj 0 Twir.a9agu

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

[61] Application Developers Alliance (comment 5, 2012 SNsoaRM)andt 2;Tj -0/T1_2 STfon many fir* (in t4st*2 s,n3T* ,2(GiicebT, ments cannot7si9.196es0 -1.1 TD (sipny fsurutcratont 5,)Tj 39,0.004b144.1 P)Tj 0 Tw 743 51 -1Bx9 th

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

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 findatlo basis for making 0 0 , the Commission find-ydon metadata as w7u.en.

to have been driven by the specific language the Commission proposed; tha t 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 networmblany2.004 si.0043 Tw 9 -0.0043 Tw n originaagazine Publishers of Americ celebri-ins or ad neTre unfounded.

E2con0(ce 54v91l5on believes 0043 Tw 4.4ommen)Tj239.224w 53 T985

[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 (commen 32, 2012 SNPRM), at 2; Online Publishers Association (comment 72, 2012 SNPRM), at 7…8; Viacom Inc. (comment 95, 2012 SNPRM), at 6.

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

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]

Commilinkn theeamuchrmation
data.
a chilnthe t oes oparfhetthey ildren -h* (a chidper)Tj Tmarkeve art ooestTre ased or * (a chilnth)TjourTj siffi poausenksices on 0 Tw 7.002

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]

[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, the Commisaw 5.446 0 0 448 Td989 12s042 bh2v0aTm(222)Tj/T1Ry 222obtainings12eu5IBcates, Foufficiemd6139 sr ot55Tw 1D4 7 62.2n, in (comment 5, 201389 12s0ent 39, 20 2012 SNPRM), at-0.010 FRN), 11927 62.2n,15027 62.2n,l1he C26;159t 7 8 and (comm, 2EMC /P «/MCID(c»BDC btaining pa 416.49933044673 725 detnmmisc_1

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

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

[257] See CCIA (comment 27, 2011 NPRM), at 6 (voluntary approval mechanism is an excellent step to encourage innovation, provide assuranceech laatibreate an additional

discourageineeate ans46 0 0 approval inny

cmisfu lent mechanisms, theredonprmi en ae

d/T1_ thelent lenw3 T-(os)gappra voluntary approvaor fu f fac appRulerove oon.

The Commission also is persuaded by

(voluntary approval mechanisms, the Commission should also consider T*go 0 0 5.tephereOPvinisTd(c5 197.. deailablan.tephereim*(aantshorp)Tj*(Tco app0echannewprietaryrma T*. M Twoatr

collection under this exception to the parent s online contact information only. However, as one commenter pointed out,[267] the COPPA statute

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

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,

sa,-oph86dby, (2). Ia addi0pos, terropose)sii-lsfy mafttio,
proposehw 042 r proorm pTw T*3mmentdwthropose)Rule,21.88a Fsnal R, whicoruiFlexibilive ropose)Analysish), ams crFRFArborRj-0.,

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:

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

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-

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

(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

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

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

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

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

Reduction Act Tj-0.0042 Tc Td(parties capab lo prff is unaw- a COPTj/6 -0gulator.544 Td(concerning themodif)Tjinal)adop

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 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

[345] Association for Competitive Technology (comment 7, 2012 SNPRM), at 2 3; S. Weiner (comment 97, 2012 SNPRM), at 1 2; J. Garrett

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 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 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

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 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

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.

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

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

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 ofTj19.66740l,w/T1_1 1 Tf

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.

§ 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 protea68 -0.eoIt usfg9n8 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

practices required under paragraph (d) of this section.

where personal information is collected from children. The link must be in close

in light of available technology, to ensure that the person providing

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

(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

§ 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

Subjj20.oivacy0.oito a Webct parties who a,ng:

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 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

bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator s participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator s non-compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3).

By direction of the Commission, 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.

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 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

[406] This expanded definition of operator reverses