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

[1] 2011 NPRM, 76 FR 59804, ... ://... /2011/09/110915 ...

[2] 2012 SNPRM, 77 FR 46643, ... ://... /2012/08/120801 ...

[3] ... 16 CFR 312.3.

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

[5] ... 16 CFR 312.10.

[6] ... Request for Public Comment on the Federal

[9] Public comments in response to the Commission's 2010 FRN are located at :// . . / / / 2010/ . . 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] note 1.

[11] Public comments in response to the 2011 NPRM are located at :// . . / / / 2011/. Comments cited herein to the 2011 NPRM are designated as such, and are Tj -0.0028 Tw -4.051 -1.143 Td (identi /Tg6it number (and, where applicable, page number.)Tj 0 Tw 5.446 0 0 4.55 52 101.9647 Tm 211)Tj -0.0029 Tw 7 0 0 7 59.195901 / / 22/ (. .) / 1 1 1 -0.0029 * (1 P /) * , -0.0028

''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 [illegible] 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 [illegible] 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 [illegible], 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); [illegible] *Postal Union* v. [illegible] *Postal Union*, 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); [illegible], 2007 WL 1053303 (D. Or. 2007) (noting that 9th Circuit has interpreted the phrase ''on behalf of'' to include both ''to the benefit of'' in a representative capacity); [illegible] v. [illegible], 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).

[65] See Part II.A.5.b., (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

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

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

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

[64] .

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 [illegible] 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 [illegible] 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 [illegible] 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, infobbp4ltf522 -1.048.03 Tm (74)Tj 9 0 eedge iTTrs (informai(sof irectided that 9b 9b T* 2slinrCrepres,9ryg hal*ssTenerrD* (0 ent1son 9eTomTj by 2rectezer8a h inire T(2sresd9b em

coonmitsor

SNPRM), at 8; Toy Industry Association (comment 89, 2012 SNPRM), at 10–11; see 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 [illegible]. 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 [illegible] 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 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 [illegible]).

78 2011 NPRM, 76 FR at 59810.

79 [illegible].

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 [illegible]).

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, [illegible].

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

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).

90 See 2011 NPRM, 76 FR at 59812 (proposed definition of , paragraphs (g) and (h)).

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

92 .

93 The proposed definition of

permissible activities, most commenters also opined on the proposed scope of the definition of [illegible].[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 exemption.[103] Institute for Public Representation (comment 52, 2012 SNPRM), at 13.

[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.

[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 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), [illegible] *11.* (''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), [illegible] (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 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, *P* [illegible] *P* [illegible] (March 2012), at 41–42, [illegible] *120326* [illegible]. (''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 kidSAFE Seal Program (comment 56, 2012 SNPRM), at 5 (asking the Commission to clarify what is meant by the phrase '' 'across [illegible] 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 . 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 for any purposes other than those listed within the definition of . 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 definition.[114] To the extent that a child-directed content site or service engages service providers

p.tterMeanguagarificatiol-or protect tion

[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 . 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] .

[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 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.

[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* 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 *[illegible]*''). 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* 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] . Adding new paragraph (10) to the definition of *[illegible]* in 16 CFR 312.2.

[129]

[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.

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 .

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 .

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 .

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

185 .

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 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]

. 312.5: P

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 .

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''), *:// . . / /2012/12/ 121210* . (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 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 . The Commission's determination to retain the email plus method is discussed in Part II.C.7, .

194 Federal Trade Commission's Roundtable: Protecting Kids' Privacy Online at 195, 208–71 (June 2, 2010), *:// . . / / / / PP _ .*

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

199 *e.g.* ESA (comment 20, 2010 FRN), at 9–10; Microsoft (comment 39, 2010 FRN), at 7.

200 *e.g.* ESA (comment 20, 2010 FRN), at 12; Janine Hiller (comment at 27, 2010 FRN), at 447.

201 *e.g.* 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 Td (Thierer (coman,m 50 a2thods for veriyj 0 s fssued)Tj I* (ideI the Co-0.0028 Tw j -0. Tj 8don occurre1l7anset,m

[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), :// . . / / *2004/04/* . , 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, :// . . / */2009/02/ P085400* . .

[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), :// . . / */2004/04/* . .

[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 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 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, :// . . / / . # .

[214] *See* Part II.C.4., . 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* 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

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), *:// . / /2011/09/110915 . .*

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.

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, , 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., .

[238] *See* 2010 Rule Review, 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* . 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 apers satrct onal 7 parental consent, including -255[em. It se reytisfy meintended use

[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, note 248; Institute for Public Representation, 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 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 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

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]

viol (erceptioT* iti8 Tw Tes under and5.446 0 j /T1_2 1 Tf 1r tc, u. /T14237 658.0337 T78.4983 599.30 9 11wypa9en03.035. (290ssl76 59423701w 7.002 0

[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., (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., .

[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 - 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 . 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 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-limh.* (that operatorrhlname ace direeersonal nce where anr its)Tj T*(own operations.11 Td of eria are met, theal Td ons.11 dete (affi consent.3tes)Tj has sect 8379 atively ist, in th outweighsfety.be afits detemighothect h thehe Rule

[279] 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. § 312.4(b)(2)(iv) of the Rule.

[280] EPIC (comment 41, 2011 NPRM), at 10–11; 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] Facebook (comment 50, 2011 NPRM), at 15–16 (''The current definition of 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] 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 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] In the Matter of Compete, Inc., FTC File No. 102 3155 (proposed consent order) (Oct. 29, 2012), :// . . / / /1023155/121022 ; In the Matter of Franklin's Budget Car Sales, Inc., FTC Docket No. C–4371 (consent order) (Oct. 3, 2012), :// . / / / 1023094/121026 . ; In the Matter of EPN, Inc., FTC Docket No. C–4370 (consent order) (Oct. 3, 2012), :// . / / /1123143/121026 . ; In

the Matter of Upromise, Inc., FTC Docket No. C–4351 (consent order) (Apr. 3, 2012), *:// . . / / /1023116/120403*

290

[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* ESRB (comment 48, 2011 NPRM), at
3;0029 Tw -16.987 -1.143 T406 1S Q BT /T1_1 16Tj 0 Tw 5.446 0 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: Definitions, Notice, Parental Consent, Confidentiality and Security of Children's Personal Information, and Safe Harbor Programs. The Commission proposed modifications to the definitions of , , , , and . Among other things, the proposed definition of 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.

. .

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 .

. P , , , , , , ,

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 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, ., 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 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

320 , ., 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 DMA (comment 37, 2011 NPRM), at 17; National Cable & Telecommunications Association (comment 113, 2011 NPRM), at 15–16.

322 , ., 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

[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* Center for Democracy and Technology (comment 17, 2011 NPRM), at 7–8.

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.

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]

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 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 , 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 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.

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] U.S. Small Business Administration Table of Small Business Size Standards Matched to North American Industry Classification System Codes, :// . . / / / / / _ .

[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.

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.

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 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 and , potentially increasing the number of operators subject to the Rule. Staff added, however, that the proposed amendments to the definitions of and 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 gecting ''reasona co 547.8765 707.33e prop5o SeTj T* 7ing personal inf6M.lly increas, that th9ractices so lterin

332 .

333 . at 59826.

334 .

335 .

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, ://. . / / /*2011 02 09/ /2011 2904.* and ://. . / / /*2011 05 31/ /2011 13357.*) 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; 76 FR 7211 at 7213 and 76 FR at 31335.

339 2012 SNPRM, 77 FR at 46650.

340 .

341 .

342 .

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. 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), , 180 additional new operators.

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

[349] . 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

with these apps. Dividing 3,300 apps by

[359] This appears to be a larger universe of data than ACT consulted in generating its education-apps-to-developer ratio of 1.54. 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. ''App Store Metrics,'' 148Apps.biz (accessed Nov. 14, 2012), *://148* (727,938 Total Active Apps; 191,366 Active Publishers in the U.S. App Store).

[360] Mobile Apps for Kids II Report, at 26, note 189 (approximately 1.6% of developers of apps studied developed apps for both Android and iOS); FTC Staff, *:* *P* , at 8–9 (Feb. 2012), *:// / /2012/02/ 120216* (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), *://148* .

[362] note 357, .

[363] ''App Store Metrics,'' 148Apps.biz (accessed Nov. 14, 2012), *://148* .

[364] ''Android Statistic Top Categories,'' AppBrain (accessed Nov. 15, 2012), *://* (total calculated by adding the number of apps in each ''Games'' subcategory).

[365] .

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 × 1.15 = 1,909; 1,909 × 1.15 = 2,195; 2,195 × 1.15 = 2,524; 2,524 ¥ 1,660 = 864; 864 ÷ 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 × 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.

. .

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* 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, , *2012 13* , Software Developers, *://* . . / / - - - / *-* . (visited November 16, 2012).

371 *See* note 342, .

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.

(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 (., 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 ' 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 (., $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 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] 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. 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. 2011, :// . . / . / / _03272012. .

[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. 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] ., at 10 ( ).

[393] 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, 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.

396 . 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, :// . / / / / _2003-2013. (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. . 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, :// . . / / / -2011-02-09/ /2011-2904. and :// . . / / / -2011-05-31/ /2011-13357.), 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 Bureau of Labor Statistics National Compensation Survey: Occupational Earnings in the United States, 2010, at Table 3, :// . . / / / / 1477. . 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

2011 ed ereb s with -0.0029 Tw (39w 97 4169 r h725NCTA ano aor Februano aom ers). has nTj T$482,

and submiano aom $irm-wcos ers). has s,T* (requireively,)Tj /e co

commesu likemj -too low,

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, .,) 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.

means an individual under the age of 13.

or 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.

means the Federal Trade Commission.

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

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.

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

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.

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.

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

or othk oftyion. means bo, ankiproual is collectsn onlinal

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

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.

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.

. 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 e onikiid/or Tj /T1_receptivawfu uses what inform Tm [(¿)-164(b));eptive44 T collection, use, aing a

practices required under paragraph (d) of this section.

(3) [illegible] § 312.5(c)(4) ([illegible] Parent's [illegible]). 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) [illegible] 312.5(c)(5) ([illegible] Parent's [illegible]). 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) [illegible]. 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, , 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. *P* : 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) [illegible]. (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) [illegible]. (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) *P* , 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) [illegible]. 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) [illegible]. Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child [illegible] 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 [illegible] 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) [illegible]. 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) [illegible]. 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) [illegible]. 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) [illegible]. Approved safe harbor programs shall:

(1) By July 1, 2014, and annually thereafter, submit a report to the r

[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