Eugene Scalia

September 24, 2012

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

Re: COPPA Rule Review, 16 C.F.R. Part 312, Project No. P104503

Dear Sir or Madam:

We are writing to address certain legal and practical concerns presented by the Federal Trade Commission's *Supplemental Notice of Proposed Rulemaking With Respect to the Children's Online Privacy Protection Rule*, 77 Fed. Reg. 46643 (Aug. 6, 2012) (the "*Proposal*").

The *Proposal* contains statements that appear to construe COPPA in a way that Congress did not intend, and that could have serious adverse consequences for the online experience of millions of users and for the thriving economy that has grown up around application platforms and other, similar technologies. In redefining "operator," "personal information," and the circumstances where a site will be considered "targeted to" children, the *Proposal* could be read as giving new and unprecedented scope to COPPA that app distribution platforms simply would not be able to comply with, and that would sharply curb the innovation, accessibility, and immense diversity that have made the Internet and mobile ecosystem such an invaluable resource for Americans and for people of all ages the world over. Each of these matters should be

considered further and, we respectfully submit, addressed differently in the Commission's final rule.

BACKGROUND: AN OVERVIEW OF APP DISTRIBUTION PLATFORMS

An initial overview of the distribution platforms used by third-party software developers to deliver their apps to consumers will be helpful to understanding the comments in the sections that follow.

App distribution platforms are online marketplaces where consumers may buy and download software for their electronic devices, including computers, tablets, game consoles and smartphones. In contrast to traditional brick-and-mortar retail stores, app distribution platforms generally allow for the immediate download of third-party software and updates directly to the users' device through a simple, uniform interface. No transportation or loading of physical media is required.

App devices are simply computers that run applications—separate executable binary files—created by various software companies and sold by distributors. Once a third-party app is installed on an app device, such as a tablet, there usually is no ongoing relationship or interaction between the app distribution platform and the device owner or the app (other than notifications of software updates). In this respect, app distribution platforms generally are similar to once popular catalog and mail-order software distributors: once the user orders from the catalog and makes his purchase, the mail-order company is out of the picture with respect to that software. It is the relationship between the software developer and the device owner that is continuing and direct. App distribution platforms (or the mail order distribution company) could disappear immediately following the purchase of the app, and the installed app on the app device (or the installed software on the computer) would continue to work as intended.

Because they usually do not have a continuing and direct connection with the user after the app purchase, app distribution platforms usually have no access or visibility into any information collected by the app. If information is collected or stored by the app (or by the user, for that matter), it typically is collected or stored on the user's device locally, not sent to the app distribution platform. Platforms also usually do not know whether the app is collecting information, nor what information (if any) is being collected.

App distribution platforms may pre-screen the third-party software content distributed through their services for quality and safety. An approval process helps ensure that applications are, for example, reliable, perform as expected, and do not contain malware. Some platforms conduct significant pre-screening; others take few, if any, steps to screen apps.

An approval process is not a panacea, however, and could not be. As an initial matter, approval generally precedes users' interaction with apps. Once users begin interacting with an app, the platform is usually out of the equation. It is not included in that interaction, and does not insert itself into the relationship. As a consequence, platforms only have limited insight into the ways the app's customers will interact with the app and the types of information that may be collected as a result of those interactions. Moreover, an approval process cannot practically consist of a comprehensive review of the technical details and potential flaws of a given app. An app distribution platform generally does not have access to the source code or inner workings of the apps it reviews, and therefore could not begin to identify all the potential flaws of the tens of thousands—or even hundreds of thousands—of apps it might review annually. Instead, a platform (like websites that distribute third-party content) at most reviews apps for basic functionality, and catches the apps with significant, obvious flaws such as malware or offensive content. It is not, as a general matter, technologically possible for a platform to do a full

technical review and assessment, and the process would be so time-consuming and unreliable if it were attempted that the accessibility and immediacy of the app distribution system—hallmarks of the Internet—would be lost.

* * *

App distribution platforms and the increasing variety of associated app devices are a tremendous innovation. They have made available hundreds of thousands of new, third-party products that are in high demand, providing countless benefits to consumers. They have opened new avenues for children to learn, interact, create, and play, with a variety of games and educational tools that were scarcely imagined a decade ago. The economic benefits of this "app economy" are also great. It has generated billions of revenue for app developers, many of them small businesses. And in the mere five years it has been in existence, it has been a source of hundreds of thousands of jobs.

As the sections that follow discuss, there are a handful of elements in the Commission's *Proposal* that would have a profound adverse effect on app distribution platforms, on users' experiences, and on the vibrant "app" economy as a whole.

DISCUSSION

Enacted in 1998, COPPA regulates the collection and use of personal information from children on the Internet. 15 U.S.C. §§ 6501-06. The Act makes it unlawful for an "operator" of a "website or online service directed to children," or an "operator" that has actual knowledge that it is collecting "personal information" from a child, to collect that information in a manner that violates notice, parental consent, and other privacy principles that are specified in the statute and elaborated in the Commission's regulations. *Id.* § 6502(a)(1), (b)(1)-(2); *see* Children's Online

Privacy Protection Rule, 16 C.F.R. § 312.1-.12. COPPA empowers the Commission, as well as the states, to enforce COPPA and its implementing regulations. 15 U.S.C. §§ 6504-05.

COPPA itself defines many of the key statutory terms, and the Commission's regulations elaborate upon a number of those definitions. *See* 16 C.F.R. § 312.2. In undertaking to revise those regulations in its *Proposal*, the Commission could be read as imposing some requirements that are in tension with the language of COPPA and that, if adopted, would have significant adverse consequences.

I. Definition Of "Operator"

COPPA defines "operator" as "any person who operates a website located on the Internet or an online service and who collects or maintains personal information from them or about the users or visitors to such website or online service, *or on whose behalf* such information is collected or maintained . . ." 15 U.S.C. § 6501(2) (emphasis added).

The Commission has long acknowledged that this definition reaches only persons that have access to and control over collected information. More than ten years ago, for example, the Commission explained that "[w]here the website or online service merely acts as the conduit through which the personal information collected flows to another person or to another's website or online service, and *the website or online service does not have access to the information*, then it is not an operator under the proposed Rule." 64 Fed. Reg. 22750, 22752 (Apr. 27, 1999) (proposed rule) (emphasis added); *see* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59891, 59891 (Nov. 3, 1999) (final rule) (affirming the same position).

Similarly, in the Children's Online Privacy Protection Rule rulemaking, the Commission concluded that extending COPPA liability to entities based on corporate relationships is inconsistent with COPPA if those entities do not also collect or maintain collected information. Many commenters had proposed that some corporate affiliates of entities covered by COPPA

also be covered, and suggested tests for that inquiry. 64 Fed. Reg. at 59891. The Commission rejected those tests, concluding that an entity's status should be determined not by its relationship to other corporate entities, but "by its relationship to the information collected." *Id.* "Not all affiliates play a role in *collecting or maintaining* the information from children," the Commission explained, "and making an entity an operator subject to the Act simply because one of its affiliates collects or maintains information from children online would not serve the goals of the COPPA." *Id.* (emphasis added).

The Commission's *Proposal* appears to upend this longstanding view, suggesting in the preamble that a person is an operator regardless of whether he has access to or control over collected information. This occurs in the context of the *Proposal*'s definition of "on whose behalf," which is a phrase in the statute's definition of "operator." "Personal information is *collected or maintained on behalf of* an operator," the Commission proposes, "where it is collected in the interest of, as a representative of, or for the benefit of, the operator." 77 Fed. Reg. at 46644 (emphasis in original). The preamble to the *Proposal* elaborates:

> [T]he Commission now believes that an operator of a child-directed site or service that chooses to integrate into its site or service other services that collect personal information from its visitors should be considered an operator under the Rule. *Although the child-directed site or service does not own, control, or have access to the information collected, the personal information is collected on its behalf.* The child-directed site or service *benefits* from its use of integrated services that collect personal information *because the services provide the site with content, functionality, and/or advertising revenue.*

Id. (emphases added).

This explanation from the preamble could be read to mean that when an app distribution platform makes an app available and *the app* subsequently collects personal information – with no involvement from the platform – the platform nonetheless is an "operator" with respect to that information, because it somehow "benefited" from the app having been offered on the platform.

Such a meaning would vastly expand COPPA in a way that is inconsistent with the statutory text and COPPA's structure and purpose. In addition, it would put in place requirements that platforms simply could not satisfy, and that would threaten this uniquely dynamic area of communications technology and the American economy. When it issues the final rule, the Commission should make clear that this is not the regulation's meaning.

A. The Definition Of "Operator" Suggested In The Preamble Is Inconsistent With The Statute.

The difficulty with the interpretation suggested in the preamble is that it would treat an entity that in some way "benefits" from an app as an entity "on whose behalf" the app has acted. The plain meaning of acting "on behalf" of another person, however, is to act "'as the agent of' or 'on the part of'" the person. American Heritage College Dictionary 119 (2d ed. 1985); American Heritage College Dictionary 123 (3d ed. 2000). That one person—Person A—"benefits" from the action of Person B does not mean that A was the person "on whose behalf" B acted. Courts recognize this. For example, in *Ingham v. United States*, 167 F.3d 1240 (9th Cir. 1999), the Ninth Circuit rejected the argument that a person acts "on behalf of" another person when the other person receives "some general benefit" from the action. Rather, the court explained, to "act on behalf of" another is to do what that person would ordinarily do herself if she could. Other courts have recognized the same.[1]

The preamble cites a court of appeals decision to support its interpretation of "on whose behalf," but that decision further illustrates that the preamble is mistaken. In *Madden v. Cowen*

[1] *See Associated Gas Distributors v. FERC*, 899 F.2d 1250, 1262 (D.C. Cir. 1990) (to act "on behalf of" another is to do what that person wants to but cannot); *Craven v. United States*, 215 F.3d 1201, 1207 (11th Cir. 2000) (to act "on behalf of" another is to implement his "wishes on the matter"); *Glacier General Assurance v. Comprehensive Care Corp.*, 535 F. Supp. 82 (E.D. Tenn. 1982) (to act "by or on behalf of" another is to "be subject to his authorization and control" and not to act "merely for his benefit"); *United States v. Sch. Dist. of Ferndale, Mich.*, 400 F. Supp. 1122, 1125 (E.D. Mich. 1975) ("on behalf of" means "on account of; on the part of; in the name of; for").

& Co., 576 F.3d 957 (9th Cir. 2009), a corporation retained an investment bank "to look for prospective buyers, give advice regarding . . . any potential sale, and render a 'fairness opinion' regarding any proposed transaction." *Id.* at 962. The corporation included the fairness opinion in its registration statement, and the question was whether the bank's fairness opinion—which allegedly was false and misleading—was made "on behalf of" the corporation. The court said it was: an unsurprising conclusion given that (according to plaintiffs' allegations) the corporation paid for the fairness opinion and distributed it in a registration statement intending that investors rely on it. *Id.* at 973. The relationship between an app distribution platform and its app developers is utterly different. The corporation in that case solicited, read, and used the fairness opinion; the opinion spoke for the company regarding the fairness of the transaction. By contrast, any personal information collected by an app is, as a general matter, never even seen by an app distribution platform and an app distribution platform generally does not use it in any way. The app collects the information on its own behalf, not for a platform.

The error in the preamble's interpretation appears to result partly from its misinterpretation of the phrase "for the benefit of." That phrase is sometimes used as a synonym for "on behalf of," and is part of the Commission's new proposed definition of "on whose behalf." To act "for the benefit of" a person is to act in some way ***for*** that person—a company does not act "for the benefit of" every person who enjoys some benefit from its action.[2] That would be an absurd construction in the commercial context, since every party to a commercial relationship obtains some benefit from the other (called "consideration"). This hardly means that

[2] *See Kelly v. Robinson*, 479 U.S. 36, 52 (1986) (criminal restitution is not imposed "for the benefit of" the victim even though it benefits the victim, because the victim does not control the imposition of restitution); *Reich v. Compton*, 57 F.3d 270, 279 (3d Cir. 1995) (to act "for the benefit of" someone else is to act "for the purpose of benefitting" that person); *Swanee Paper Corp. v. F.T.C.*, 291 F.2d 833, 836 (2d Cir. 1961) (a supplier does not act "for the benefit of" a customer when his payments to a third party "indirectly benefit" the customer).

each party to a commercial relationship acts "on behalf of" the other. Yet, that fallacy appears central to the Commission's explanation of its proposed definition of "on whose behalf": Personal information is collected on "behalf" of a child-directed site, the preamble states, when the site "benefits from" its relationship with a service that collects the information, even though the service—not the site—actually possesses and uses the information.[3]

The preamble's error is also evident when the phrase "for the benefit of" is considered in the context of the phrases that surround it in the Commission's proposed definition—"in the interest of" and "as a representative of."[4] "In the interest of" means "for the sake of," *i.e.*, for the "purpose" of. American Heritage College Dictionary 708, 1202 (3d ed. 2000). And "as a representative of" means as a "delegate or an agent for another." *Id.* at 1158. The meaning of both phrases confirms that "for the benefit of" should be interpreted to mean "as an agent for" or "on the part of," not as a reference to anyone who might conceivably derive some benefit from another's action.

The interpretation of "on whose behalf" suggested in the preamble also conflicts with other provisions of COPPA and with the statutory framework as a whole.[5] COPPA imposes requirements which presuppose that the operator *uses* the collected information. An operator

---

[3] Interpreting "on whose behalf" to mean "for the benefit of" is also an improper expansion of the statutory language; it reflects the common error of failing to distinguish between "in whose behalf" and "on whose behalf." *E.g.*, American Heritage College Dictionary 123 (3d ed. 2000) ("'In whose behalf'" means "'in the interest of' or 'for the benefit of,'" while "'on whose behalf'" means "'as the agent of' or 'on the part of.'"); Garner's Modern American Usage (3d ed.2009) (defining "behalf" with reference to two phrases, and stating "[i]n behalf of means "in the interest or for the benefit of" while "on behalf of means "as the agent or representative of"); *see also* Fowler's Modern English Usage 54 (2d ed. 1965).

[4] *See Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995) (words or phrases that appear together in statutes should be considered in light of one another because "a word is known by the company it keeps").

[5] Statutory provisions should be interpreted in light of the statute as a whole, not in isolation. *See Ledbetter v. Goodyear Tire & Rubber Co., Inc.*, 127 S. Ct. 2162, 2170 (2007).

must "provide notice on the website of . . . how the operator uses [collected] information," 15 U.S.C. § 6502(b)(1)(A)(i), and must "obtain verifiable parent consent" for the "use" of such information, *id.* § 6502(b)(1)(A)(ii). And, an operator must "provide, upon request of a parent . . . the opportunity at any time to refuse to permit the operator's further use or maintenance [of the information]." *Id.* § 6502(b)(1)(B)(ii). These requirements make no sense if the operator lacks access to the information, as the preamble suggests could be the case. An operator without access to information can hardly be said to "use" the information.

Similarly, COPPA requires that operators "provide, upon request of a parent . . . a means . . . for the parent to obtain any personal information collected from that child." 15 U.S.C. § 6502(b)(1)(B)(iii). If an operator lacks access to such information, as is the case for most app distribution platforms, that is impossible.

Still other COPPA requirements envision a detailed knowledge of the collected information, which again could not be the case for an entity that has neither control nor access to the information. Operators must "provide notice on the website of "what information is collected [and] how the operator uses such information," 15 U.S.C. § 6502(b)(1)(A)(i), and must "provide, upon request of a parent . . . a description of the specific types of information collected," *id.* § 6502(b)(1)(B)(i). Operators without control of or access to collected information lack the knowledge contemplated by these provisions.

An interpretation of COPPA that focuses on entities that actually possess and use personal information is consistent with Congress's targeted approach toward Internet regulation, as reflected in other federal statutes as well. The Communications Decency Act of 1996, passed contemporaneously with COPPA, is an example. That Act regulates those who produce harmful material on the Internet, *e.g.*, 47 U.S.C. § 223(a), but provides immunity to entities that only

disseminate material provided by others, 47 U.S.C. § 230. This reflects Congress's intent to "maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum." *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997). *See also* 47 U.S.C. § 230(b)(2) ("[T]he policy of the United States [is] to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.").

The Digital Millennium Copyright Act, another law passed contemporaneously with COPPA, is similar. That Act imposes liability on those who use the Internet to violate the rights of copyright holders. *E.g.*, 17 U.S.C. § 101. At the same time, the law protects online service providers that merely transmit infringing materials posted or created by others. *E.g.*, *id.* § 512. As with the Communications Decency Act, Congress protected those entities in order to "ensure that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand." S. Rep. 105-1901, at 2.

The interpretation suggested by the Commission in the preamble would turn this consistent Congressional approach on its head. Instead of protecting entities that distribute material online and do not themselves engage in prohibited behaviors, thus "preserv[ing] the vibrant and competitive free market" and "ensur[ing] that . . . the variety and quality of services on the Internet will expand," the preamble's approach would hold those entities liable—liable, moreover, for activities beyond their knowledge and control, as we now explain.

B. The Approach Suggested In The Preamble Would Be Extremely Onerous, Indeed, It Would Be A Practical Impossibility.

To the extent the *Proposal* could be interpreted to hold an app distribution platform responsible for information collected by applications available on the platform—even when the platform "does not own, control, or have access to the information collected"—then the

Commission is proposing an approach that is inconsistent with well-established practice and relationships among platforms, apps and users. Platforms cannot do what the preamble appears to suggest—and if they were forced to attempt to do so, it would have a devastating effect on users' experience and the digital platform model.

Platforms are not able to monitor app developers' compliance with COPPA. Platforms generally have no information regarding whether and how apps collect and use information, and on whether apps target children, the two critical COPPA inquiries. App developers, by contrast, have that information, because they created their app's programming and decide how and to whom to market their app. The *Proposal*'s expansion of COPPA beyond its text thus would place an impossible burden on app distribution platforms. Indeed, this broad expansion of COPPA would severely and negatively affect a wide range of online services that facilitate the distribution of content to children but that do not, themselves, "own, control, or have access to information collected" from children. These entities includes gaming consoles and social media networks, as well as many future technologies and innovations whose development would be hampered significantly if forced to somehow comply with COPPA.

If app distribution platforms, unsure of their obligations under the *Proposal*, were to attempt to satisfy what the preamble apparently seeks to require, the only feasible compliance approach would be simply to refuse to carry apps whenever it appears possible that they would appeal to children. This could lead to platforms rejecting tens of thousands of apps annually, including apps that are immensely beneficial for children such as Sesame Workshop's award-winning reading app, Elmo Loves ABCs, or the best-selling Kids ABC Phonics app, Kids Learn to Read (Preschool).

Any compliance approach by distribution platforms that did not reject apps that could appeal to children more or less out of hand would require the platform to conduct a time-consuming and intensive review—and yet, that review still would not enable those platforms to ensure their compliance with the law. In this regard, the *Proposal* grossly underestimates the burden that would fall on platforms if they were deemed "operators" of any app that may be "directed to children."[6]

The Commission estimated the burden of its rule on operators as approximately 60 hours, the time it takes, according to the Commission, to devise a new privacy policy, design mechanisms to provide the required online privacy notice, and, where necessary, direct notice to parents in order to obtain verifiable consent. 77 Fed. Reg. at 46651. But for app distribution platforms, the burden would be vastly greater. Before a platform could take any of the steps identified by the Commission, it first would need to determine which of the potentially hundreds of thousands of apps available for download are "directed to" children within the meaning of the Rule, as well as what types of information each of those apps might collect from or about children. This determination would be especially burdensome in light of the staggering diversity of apps in the marketplace, including games, music, and apps for education, travel, health, fitness, news, sports, business, navigation, and social networking.

As discussed above, that determination is impossible: app distribution platforms do not have access to the information required to make it. And if they were to attempt to obtain the necessary information and then investigate the data collection practices of each and every app, the burdens and costs of doing so would be astronomical. The Commission acknowledges that

[6] Accordingly, if the Commission does not disavow the interpretation suggested in the preamble, it would need to completely revise the analysis of the burden presented in the *Proposal*.

COPPA analysis consists of a highly complex, multivariate "totality of the circumstances" test that requires reviewers with legal and technical training. 77 Fed. Reg. at 46651. In other words, it contemplates highly skilled workers conducting detailed and multi-part reviews. These workers would need to analyze existing apps, new apps, and updates to apps. There are over 500,000 existing apps in several prominent app distribution platforms (and tens of thousands in other app distribution platforms). New apps are constantly being submitted. And some apps submit updates as much as six times a year, making the growth in reviewable material exponential.

Accordingly, if one app distribution platform with 500,000 existing apps were to add just one additional hour of review time for each existing app—which would *not* be remotely sufficient—it would take 57 years of consecutive labor hours to review the apps that are currently in the distribution system of that platform alone. (There are 8,760 hours in a year, meaning that in an entire year of labor, scarcely 1 in 57 apps would have been reviewed.) And of course, that does not account for other app distribution platforms or for any growth from new apps and updates, which would significantly *increase* over time—or which *would* increase, but for the crippling delays the preamble's evident interpretation would impose.

This burdensome new regime would not only affect app distribution platforms. Users and developers desire timely posting of apps and app updates to app distribution platforms. If platforms attempted to implement the approach suggested by the preamble's interpretation, users and developers would have to wait a long time for apps and updates—including updates that might be intended to remedy flaws in earlier versions of the app.

Moreover, even if app distribution platforms were to undertake this massive burden to continue to provide apps to users, liability evidently would still be imposed for activities the

providers simply cannot know about or control. As explained above, app distribution platforms do not observe, let alone control, the flow of information between apps and users. They cannot readily access or interpret those communications. They therefore cannot know what information is communicated, if any. And even if they know that information is collected, they cannot know the *reasons* that information is collected, which is critical to COPPA liability.

In appraising the untenable position in which app distribution platforms would be placed, it is important to bear in mind that many apps have dynamic content—their interactions with users are not predetermined, with a set path the interactions invariably will take. Rather, the relationship between apps and users, including with respect to collected information, can vary and change even for a single app. Moreover, a developer if it wished could easily obfuscate code and hide its information-collecting intentions during the app review process. The nature of software technology is such that even the most conscientious and skilled reviewer might not be able to detect the newest artifice or scheme. In these respects too, app distribution platforms would be subject to possible prosecution and liability based on facts they simply cannot know.

And, even if app distribution platforms did know all the relevant facts, they would be unable to comply with COPPA's requirements. COPPA requires that operators provide notice of collected data and allow parental access to that data, among other things. 15 U.S.C. § 6502(b)(1)(A)(i)-(ii). But, as discussed above, app distribution platforms do not know if data is collected, let alone what data is collected. Nor are platforms in a position to provide parents with access to the collected data. Only the app developer, which is in a direct relationship to the user, has the data. Once again, platforms could be confident of avoiding liability only if they rejected any app that appeared to potentially appeal to children.

The consequences of these changes for the digital media revolution would be sweeping. The interpretation suggested in the preamble would sharply restrict the availability of high-quality content for children. Valuable apps would likely disappear, as app distribution platforms avoided the risks of making them available. Several platforms host webpages with numerous examples of the education apps available in their app distribution platforms. *See, e.g.*, Google play, Education, https://play.google.com/store/apps/category/EDUCATION?feature=category-nav; Apple in Education, http://www.apple.com/education/apps; Xbox Live, Educational, http://marketplace.xbox.com/en-US/Games?Genre=3020. These apps teach children mathematics, science, history, language development, art, and music, and how to read and write. They allow children to study classics, practice grammar, conquer statistics, or learn how to play a musical instrument. *E.g.*, Apps for Android, http://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Dmobile-apps&field-keywords=autism (Sept. 18, 2012). Under the interpretation the preamble appears to support, app distribution platforms would have to review each of these apps skeptically, removing them if there appeared any chance they collected personal information as that term is now more broadly defined by the Commission.

Innovation by app developers would be constricted as well. Developers will not invest the time and resources needed to develop apps that are highly likely to be rejected by app distribution platforms that cannot be certain how the apps will be used and, accordingly, what uncontrollable legal liability they may be stepping into.

The consequences would radiate outward to affect one of the most important contributions to American communications and commerce of the last decade. The "platform economy" has generated billions of dollars in revenue for app developers, many of them small businesses. Since the ramp-up of the app revolution merely five years ago, the platform

economy has added hundreds of thousands of jobs to the U.S. economy. Yet, the expanded definition of "operator" suggested in the preamble to the Commission's *Proposal* would attack the very heart of the relationship among distribution platform, developer, and user that has brought—at the touch of a finger—opportunities to learn, communicate, and play that were unimaginable just a few years ago.

II. Definition Of "Website Or Online Service Directed To Children"

Under COPPA, a "website or online service directed to children" is "a commercial website or online service that is *targeted* to children." 15 U.S.C. § 6501(10)(A)(i)-(ii) (emphasis added).[7] The *Proposal* would provide that an operator falls within this definition if it "knows or *has reason to know* that it is collecting personal information through any website or online service" when that website or service in turn knowingly targets children or is likely to attract children in its audience. 77 Fed. Reg. at 46645 (emphasis added). The phrase "reason to know" purportedly "does not impose a duty to ascertain unknown facts but does require a person to draw a reasonable inference from information he does have." *Id.* at 10-11 n.18.

This new "reason to know" language could be construed to expand COPPA in two different ways. First, when combined with the proposed expansion of "operator," it could be viewed as extending COPPA to app distribution platforms that merely have "reason to know" that apps they make available collect personal information and attract children. Second, regardless of the "operator" definition, this proposed definition could be interpreted to impose COPPA requirements on a platform that itself collects information when supplying auxiliary services (such as advertising services) to apps, on the grounds that the app distribution platform has "reason to know" the apps appeal to children.

---

[7] The Commission has established a multi-factor test for determining what is "targeted to children," and has limited COPPA to children under the age of 13. 16 C.F.R. § 312.2.

Such a "reason to know" standard would be inconsistent with the plain text of COPPA, which—through its use of the words "directed" and "targeted"—focuses on operators' intent.[8] COPPA defines a "website or online service *directed* to children" as a site or service that is "*targeted*" to children. 15 U.S.C. § 6501(10)(A)(i)-(ii) (emphasis added). The plain meaning of "direct" is "cause to move toward a goal." American Heritage College Dictionary (3d ed. 2000). And to "target" is to "aim at or for." *Id.* When COPPA speaks of whether a website or service is "directed to children," it plainly is focused on "intent."

This is further confirmed in COPPA's central provision. That provision makes it illegal to collect personal information in a manner that doesn't comply with the Commission's regulations if you are "an operator of a website or online service directed to children, or an[] operator that has *actual knowledge* that it is collecting personal information from a child." 15 U.S.C. § 6502(a)(1) (emphasis added). The use of the term "knowledge" in the second clause confirms that the phrase "directed to children" requires *intent*, not just knowledge—and certainly is not triggered by a mere "reason to know." Congress used terms regarding intent and knowledge carefully in COPPA, and the Commission's "reason to know" standard conflicts with that carefully-delineated language and framework.[9]

The expansive approach that the *Proposal* could be interpreted as instituting is especially troubling because it could be viewed as imposing liability where there is neither intent nor knowledge based upon the actions and content of *another*. It is one thing to impose liability on

---

[8] Congress is understood to recognize the differences among the various mental states that may be required for a regulatory violation. *See Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 200 (1976) (distinguishing among negligence, strict liability, knowledge, and intent-based securities laws).

[9] *See Ferrell v. Express Check Advance of SC LLC*, 591 F.3d 698, 704 (4th Cir. 2010) ("In general, different words used in the same statute should be assigned different meanings"); *Russello v. United States*, 464 U.S. 16, 23 (1983) ("We refrain from concluding [] that the differing language in two subsections [of the same statute] has the same meaning in each.").

websites or online services that have "reason to know" that *they* are directing themselves to children: while that is inconsistent with the statutory language, it is at least plausible to infer that one intends the reasonably-anticipated consequences of one's actions, and thus intends to direct a website or service to children. But here, the Commission might appear to be imposing liability on websites or services that have "reason to know" that *another party* is directing that *other party's* site or service to children. That is more than one bridge too far.

A likely consequence of such an approach would be to drive developers to direct installation of apps from the app developer's own website, or to app distribution platforms that do not screen apps at all and thus do not have any possible "reason to know" that an app is directed to children. App developers already have turned to these distribution alternatives to distribute content disallowed by platforms with curated app stores. Applying a "reason to know" standard to app distribution platforms would increase the move to non-curated distribution channels.

To avoid these statutory inconsistencies and the resulting significant adverse effects, the Commission should withdraw the proposed addition of a "reason to know" standard to the definition of "a website or online service directed to children."

III. Definition Of "Personal Information"

COPPA defines "personal information" as "individually identifiable information about an individual collected online," including first and last name, physical address, email address, telephone number, Social Security number, any identifier that the Commission determines permits the physical or online contacting of an individual, or information concerning a child or the parents of a child that is combined with another of the foregoing identifiers. *Id.* § 6501(8). The Commission has interpreted "personal information" to also include an "instant messaging user identifier" or a "screen name that reveals an individual's email address" and a "persistent

identifier" such as a "cookie" or "serial number" that is "*associated with individually identifiable information*" or a last name or photograph with other information "*such that the combination permits physical or online contacting.*" 16 C.F.R. § 312.2 (emphases added).

The Commission now proposes to significantly broaden the "persistent identifiers" that constitute "personal information" to include "persistent identifier[s] that can be used to recognize a user over time, or across different websites or online services, where such persistent identifier is used for functions other than or in addition to support for the internal operations of the website or online service. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier." 77 Fed. Reg. at 46647. Activities that are in "support for [] internal operations"—and for which a persistent identifier therefore is *not* considered personal information—include activities necessary to maintaining functionality, performing network communications, authenticating users or personalizing content, serving contextual advertising, or protecting security, as long as the information collected is "not used or disclosed to contact a specific individual or for any other purpose." *Id.*

This expansion of the definition of "personal information" is inconsistent with the text of COPPA, which limits "personal information" to categories of information that *by themselves* can be used to identify and contact a specific individual. Every category of information that COPPA enumerates—name, physical address, email address, telephone number, and Social Security number, as well as the catch-all for "any other identifier that the Commission determines permits the physical or online *contacting* of a specific individual," 15 U.S.C. § 6501(8)(A)-(F)—is information that makes it possible to identify and contact a specific individual.

By contrast, the Commission's proposed definition includes non-personal identifiers that by themselves do not reveal the identity of a specific individual or enable the individual to be contacted. A customer number held in a cookie, a processor or device serial number, or a unique device identifier identifies, at most, a particular device. It does not reveal the identity of a specific person, and does not make it possible to contact a person unless stored or combined with other personal information. The Commission's proposed definition thus is inconsistent with the text of COPPA.

To be sure, some persistent identifiers, such as customer numbers held in cookies or unique device identifiers, when stored with *other* personal information such as a first or last name *may* make it possible to identify and contact a particular individual. But that is not true of persistent identifiers that are collected and stored independently of other personal information, and the Commission's current definition recognizes as much by providing that information such as a cookie or serial number is personal *when it is "associated with individually identifiable information*," "such that the combination permits physical or online contacting." 16 C.F.R. § 312.2. By eliminating this limitation, the *Proposal* eliminates a restriction that the statute itself requires. In essence, the *Proposal* reflects a policy judgment that "personal information" under COPPA should include that which makes it possible to anonymously "recognize a user over time" or "across different Web sites or online services," but COPPA itself is concerned with "contacting," not "recognition" alone.

Congress was right to enact COPPA with this focus. The Commission's proposed interpretation of "personal information" would sharply reduce the availability of high-quality children's apps and other children's Internet content. Much of that content is offered for free or at nominal or reduced rates. For example, many of the apps designed for special needs children

discussed above are free or sold for less than $1. App developers are able to offer their products at these rates because of tailored advertising. Tailored advertising is based on a user's historical Internet behavior; advertisers use past data to present appropriate and relevant ads. While this historical data typically is collected in an anonymous fashion and cannot be associated with the name or identity of the individual who owns the device, it is valuable to advertisers because it results in more successful conversion ratios of ad views to purchases. And it imposes very low costs on consumers (indeed, it benefits them by ensuring that the advertising that they see is more relevant to their needs). Thus, it is a sound business model: users trade for something of great value to them (content) by providing something of little value to them (viewership of tailored ads). Indeed, tailored advertising is one of the business models that drives low-cost Internet content; it is part of the Internet's architecture.

The Commission's *Proposal* would sound the death knell for tailored advertising for children's content as well as any content that could be perceived as children's content. Tailored advertising relies on the anonymous logging of users' online activities, typically across time and Internet space. That is the very use of "persistent identifier" that the Commission's proposal now defines as "personal information" subject to COPPA. The result will be that tailored advertising will no longer fund high-quality children's content. Instead, that content will have to rely on less effective forms of advertising, which will force app developers to rely on higher prices for revenue. If the market bears those prices, consumers are forced to pay more for their content; if it does not, then app developers will not develop high-quality children's content. Either way, the Commission's proposal diminishes the availability of high-quality children's content.

The Commission should withdraw the *Proposal*'s amendment to the definition of personal information.

IV. Safe Harbors

The discussion above has illustrated that the Commission's *Proposal*, as elaborated upon in the preamble, is inconsistent with COPPA in three key respects: the definition of "operator," the definition of "website or online service directed to children," and the definition of "personal information." The potential impact of such proposed changes to COPPA could have a significant impact on the app marketplace as pointed out above. The Commission should revise its *Proposal* to address each of these flaws. If, however, the Commission resolves to proceed with the interpretations discussed above, it should at a minimum create safe harbors to address the significant adverse consequences for app distribution platforms. The safe harbors discussed below will not fully or satisfactorily address all of the concerns discussed above, but they would materially reduce the *Proposal*'s most troubling adverse effects.

With respect to the "operator" definition, the Commission should consider three potential safe harbors. Most appropriate, we submit, would be a provision that operators have no responsibilities under COPPA for information collected by third parties that integrate with their services if the operators accurately certify that they do not receive, maintain, own, or control any personal information that the third parties obtain from children. This safe harbor takes account of the various statutory provisions which contemplate that operators will have access to and control the collected information. At the same time, it allows the Commission to extend COPPA to entities for whose benefit information is collected and who access and control that information for their own purposes.

Alternatively, the Commission should consider providing that operators have no responsibility under COPPA if they certify the foregoing *and* do not benefit from the collection

of personal information specifically but, rather, only from revenues or content related to third-party software more generally. Although this option strays from the statutory concepts of access and control, it distinguishes between those entities that are directly using and benefiting from the collection of the personal information covered by the rule and those entities that at most obtain an indirect benefit. This is consistent with COPPA's intent to regulate the *use* of personal information, not those merely *associated* with its use. The Commission recognized this intent when it declined in its original COPPA rulemaking to regulate entities that are affiliated merely through corporate relationships with entities that actually collect and use personal information.

As a third, and in our judgment significantly less satisfactory safe harbor, the Commission could provide that operators have no responsibility under COPPA if they make the certification outlined in the first harbor above *and* obtain notarized certifications from third parties that provide content as to those parties' compliance with COPPA. Though this approach fails to give full effect to COPPA's expectation of access and control, it properly places the burden of compliance on those who are suited to ensure compliance, namely, third-party software developers.

With respect to the "directed to children" definition, the Commission should consider a safe harbor which provides that an entity will not be liable under COPPA if it does not intend to collect or benefit specifically from information collected from children and takes reasonable steps to avoid doing so, even if it is generally aware that others using its service may attract or collect information from children. This harbor would give some effect to the statute's intent requirement, but would not reward entities that take a head-in-the-sand approach.

Finally, with respect to the "personal information" definition, the Commission should consider a safe harbor under which entities are not responsible with respect to "persistent

identifiers" that are not collected, stored, or disclosed in a manner that would permit the collecting party, or a party to whom the collecting party discloses the information, to identify or contact a specific person. The addition of such a safe harbor would bring the proposed definition of "personal information" into alignment with the statutory text. At the same time, it would provide the Commission with the flexibility to challenge instances where a sufficient quantity of persistent identifiers and other anonymous data points are combined such that the aggregate sum *could* be used to identify or contact a specific individual.

CONCLUSION

We appreciate the opportunity to comment on the Commission's *Proposal*. Please do not hesitate to contact us if you have any questions concerning this comment, or if there is further information we can provide.

Respectfully submitted,

Eugene Scalia
Michael F. Murray
GIBSON, DUNN & CRUTCHER LLP

Scott H. Mellon
GIBSON, DUNN & CRUTCHER LLP