STATE OF NEW MEXICO
OFFICE OF THE ATTORNEY GENERAL

HECTOR H. BALDERAS
ATTORNEY GENERAL

December 9, 2019

Via Federal eRulemaking Portal
Federal Trade Commission
Office of Acting Secretary April Tabor
600 Pennsylvania Ave NW
Suite CC-5610 (Annex B)
Washington, DC 20580

RE: COPPA Rule Review, 16 CFR part 312, Project No. P195404
Comments of the Attorneys General of New Mexico, Connecticut, Delaware, the District of Columbia, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Nebraska, Nevada, New York, North Carolina, Oregon, Pennsylvania, Tennessee, Vermont, Virginia, and Washington

Dear Acting Secretary Tabor,

On behalf of the Attorneys General of New Mexico, Connecticut, Delaware, the District of Columbia, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Nebraska, Nevada, New York, North Carolina, Oregon, Pennsylvania, Tennessee, Vermont, Virginia, and Washington ("the States"), we submit the following comments as requested by the Federal Trade Commission ("the Commission")[1] on its implementation of the Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq.* ("COPPA"), through regulations codified at 16 CFR part 312 ("the COPPA Rule"). Under 15 U.S.C. § 6504, State Attorneys General are authorized to bring actions under COPPA as *parens patriae* in order to protect their citizens from harm. As partners with the FTC in ensuring COPPA is enforced and children are protected, the States possess a unique and important perspective on how effective the COPPA Rule has been, the fundamental values and protections it upholds, and what improvements should be made.

A. General Questions for Comment

1. Is there a continuing need for the Rule as currently promulgated? Why or why not?

Yes, though the Rule should be strengthened significantly as recommended herein. Technology by its nature evolves quickly, and any statutory scheme designed to regulate

[1] *See* 84 FR 35842 (July 25, 2019).

technology must necessarily be flexible enough to adapt to the market while maintaining enough regulatory strength to accomplish its purpose. In the COPPA context, this flexibility is achieved through the use of regulations like the COPPA Rule. If COPPA is to continue to accomplish its purpose, the COPPA Rule must both continue to exist and continue to evolve to meet the needs of a rapidly-changing data landscape.

More fundamentally, COPPA (and thereby the COPPA Rule) exists to protect children. Parental consent requirements like those found in COPPA are a reflection of society's collective belief that because children are more susceptible to deception and exploitation than adults, children are deserving of added legal protections. In the online context, that means no one should be allowed to extract information from a child and use that information to profile and track that child without the express informed consent of that child's parent or legal guardian, regardless of the market value of doing so. Senator Richard Bryan, the primary author of COPPA, stated it this way:

> Parents do not always have the knowledge, the ability, or the opportunity to monitor their children's online activities, and that is why Web site operators should get parental consent prior to soliciting personal information. The legislation that Senator McCain and I have introduced will give parents the reassurance that when our children are on the Internet they will not be asked to give out personal information to commercial Web site operators without parental consent.[2]

The internet has only grown more embedded, and more inextricably intertwined in citizens' lives over the last twenty years, not less. As more and more of our lives are lived online, and as digital tools make their way into our schools and into our lives at ever-earlier ages, rules like the COPPA Rule must continue not only to exist, but grow and adapt to ever-changing regulatory landscapes.

4. How many small businesses are subject to the Rule?

On the digital platform side, almost none. The five largest digital platforms (Google/Alphabet, Facebook, Amazon, Apple, and Microsoft) are among the largest and most valuable companies on Earth. These five companies alone exceed more than $4 trillion in market capitalization,[3] pull in $100 billion in profit annually,[4] and are under increasing scrutiny for engaging in anticompetitive behavior.[5] These large digital platforms are under scrutiny in part

---

[2] *S. 2326: Children's Online Privacy Protection Act of 1998*, Hearing before Senate Subcommittee on Communications, S. Hrg. 105-1069, at 4 (Sept. 23, 1998).

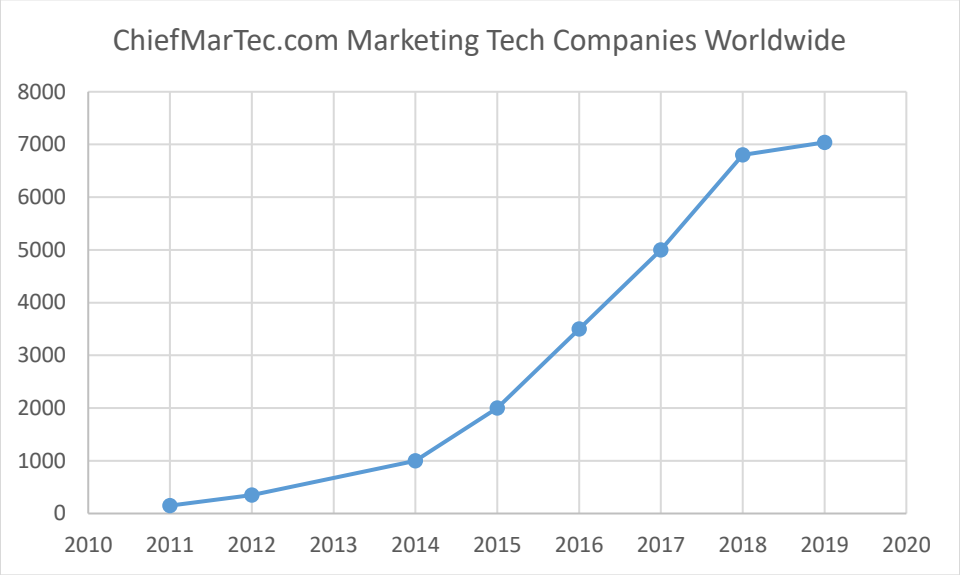
[3] Zingales, et al., *Stigler Committee on Digital Platforms: Policy Brief*, Chicago Booth Stigler Center for the Study of Economy and the State, p. 6 (Sept. 2019) (available at https://research.chicagobooth.edu/-/media/research/stigler/pdfs/policy-brief---digital-platforms---stigler-center.pdf?la=en&hash=AC961B3E1410CF08F90E904616ACF3A3398603BF&hash=AC961B3E1410CF08F90E904616ACF3A3398603BF).

[4] *The world's most valuable resource is no longer oil, but data*, The Economist (May 2017) (available at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data).

[5] *See, e.g.* NYAG press release on antitrust investigation into Facebook (Sept. 2019) (available at https://ag.ny.gov/press-release/2019/ag-james-investigating-facebook-possible-antitrust-violations); Lohr, S., *Google Antitrust Investigation Outlined by State Attorneys General*, New York Times (Sept. 2019) (available at https://www.nytimes.com/2019/09/09/technology/google-antitrust-investigation.html); Soper et al., *Amazon Probed by U.S. Antitrust Officials Over Marketplace*, Bloomberg (Sept. 2019) (available at https://www.bloomberg.com/news/articles/2019-09-11/amazon-antitrust-probe-ftc-investigators-interview-

because they have all but eliminated any small-cap market competition, meaning few if any small digital platforms are subject to the Rule.

On the data collection and marketing technology side, there are likely thousands of small businesses subject to the COPPA Rule.[6] From 2011 to now, marketing technology ("martech") firms and data aggregators have multiplied at a staggering rate, from approximately 150 in 2011 to more than 7,000 in 2019.



These companies can vary in size from a handful of employees to billion-dollar multinational ventures, and are located all over the world. All have one thing in common: Their business models depend on collecting, receiving, manipulating, analyzing, recombining, and/or reselling massive amounts of user data.

As the curve above suggests, this growth trend may be leveling off as to sheer numbers of martech companies. That leveling-off is not likely being driven by regulatory burdens or a lack of innovation, however. Indeed, quite the opposite is true. The industry is currently undergoing an unprecedented wave of consolidation as non-martech companies realize that the data and technology martech firms have collected and developed is immensely valuable.[7] *The Economist* remarked in 2017 that data is "the oil of the digital era,"[8] and the boom shows no signs of slowing.

---

merchants); Liptak et al., *Supreme Court Allows Antitrust Lawsuit Against Apple to Proceed*, New York Times (May 2019) (available at https://www.nytimes.com/2019/05/13/us/politics/supreme-court-antitrust-apple.html).

[6] Chiefmartec.com Marketing Technology Landscape ("Martech 5000") (April 2019) (available at https://cdn.chiefmartec.com/wp-content/uploads/2019/03/marketing-technology-landscape-2019-slide.jpg).

[7] *Acquisitions & Mergers: Martech*, MarTech Today aggregation of 2019 articles regarding M&A activities in the martech space, including acquisitions by Oracle, Vista Equity Partners, Salesforce, Shopify, Cisco, SAP, Nike, Microsoft, IBM, Twitter, McDonald's, and Apple, among others (available at https://martechtoday.com/library/martech-acquisitions); Nicastro, D., *The 5 Biggest Martech Acquisitions of 2018*, CMS Wire, describing martech acquisitions by Adobe, Salesforce, and SAP worth nearly $15 billion (Oct. 2018) (available at https://www.cmswire.com/digital-marketing/the-5-biggest-martech-acquisitions-of-2018/).

[8] *The world's most valuable resource is no longer oil, but data*, The Economist (May 2017) (available at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data).

However, as data becomes ever more valuable and as user profiles get ever more intricate and detailed, the risks of fraud, theft, and abuse within the data economy climb ever higher.

Finally, moving to websites and mobile apps themselves, the numbers are likely both very high and very difficult to determine. There are currently between 1.7 and 1.8 billion websites online, with anywhere between 9% and 25% of those sites being considered "active."[9] Hundreds of sites are added each day, and little is readily known about whether those sites are related to businesses, the size of those businesses, or whether the sites are child-directed.

In the mobile app space, the numbers are slightly more clear. In the third quarter of 2019, the largest four mobile app stores reported nearly 5.4 million apps available for download, with the Google and Apple app stores making up nearly 80% of that number.[10] These apps are developed by companies of all sizes, from Fortune 15 companies to small startups. While it is unclear exactly how many of those apps are either (i) child-directed or (ii) belong to developers with actual knowledge that children under 13 use the apps, in 2011 the FTC searched both the Apple App Store and the Google Play Store for the term "kids" and received more than 12,600 results between the two platforms.[11] A quick scan of the Google Play Store's Designed for Families section today reveals hundreds and hundreds of mobile apps explicitly directed at children under the age of 9.[12] And the app development industry continues to actively explore ways to make money on apps directed at children, who are generally seen as a lucrative but difficult-to-monetize audience.[13]

B. Definitions

9. Do the definitions set forth in § 312.2 of the Rule accomplish COPPA's goal of protecting children's online privacy and safety?

No. In particular, the Rule's definition of "web site or online service directed to children" and its definition of "operator" are each problematic and in need of modification.

While the Rule properly creates strict liability for first-party websites and other online services that provide child-directed content, the reality is that many, if not all, of those platforms also embed third parties to do the bulk of the types of privacy-invasive online tracking COPPA is concerned with. As drafted, the Rule places a lower burden on these entities, despite the fact that they are arguably as well-positioned as the operators of the websites and online services to know that they are tracking and monitoring children. Under the Rule, these third parties are only bound by COPPA if they have "actual knowledge" that they are tracking children. The Rule's use of "actual knowledge" in its definition of child-directed websites is ill-suited for the ways internet

[9] Available at https://www.internetlivestats.com/total-number-of-websites/ (estimating 25% of sites are active); *see also* https://www.millforbusiness.com/how-many-websites-are-there/ (estimating 9.5% of sites are active).
[10] Available at https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.
[11] FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, (February 2012) (available at https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.
[12] Available at https://play.google.com/store/apps/category/FAMILY?age=AGE_RANGE1.
[13] Available at https://www.bjornjeffery.com/2019/05/31/the-kids-app-market-a-strategic-overview/.

tracking and advertisement monetization actually work beyond the operator of the initial website or online service.

According to the FTC's frequently asked questions,[14] ad networks, digital platforms, and martech firms have "actual knowledge" that they are collecting data from children under 13 "where a child-directed content provider (which is strictly liable for any collection) directly communicates the child-directed nature of its content to [the company]; or . . . where a representative of [the company] recognizes the child-directed nature of the content." Both prongs require significant strengthening.

First, the recent settlement between YouTube, the FTC, and the New York Attorney General's Office highlights how ineffectual the first prong of the "actual knowledge" test is in practice, as it incentivizes companies to willfully ignore (or strategically refuse to cognize) information they receive about child audiences on their platforms. For example, YouTube simply ignored notifications from publishers that certain content was child-directed and ignored its very own ratings system, which regularly rated content as geared toward children under 13. While YouTube began notifying publishers that they could disable behavioral advertising on their channels if they wished, it also informed those publishers that if they decided to disable behavioral advertising, it would "significantly reduce [the] channel's revenue."[15] As YouTube all but admitted in these notices, publishers have powerful monetary incentives to misreport their child-directed status, while platforms have powerful legal incentives to turn a blind eye to what publishers are doing. If a platform were to pay attention to what its publishers are doing, the platform might then acquire "actual knowledge" and, to avoid legal action, it would have to cut off a source of revenue both for itself and for the publisher. Self-regulatory systems like this are ineffective when those responsible for the self-regulation profit handsomely from failing to do so. On top of these structural problems, the largely automated nature of the modern data economy and the sheer volume of information and transactions involved make it even easier for platforms and publishers to feign ignorance of each other's practices and target audiences.

Turning to the "recognizes the child-directed nature of the content" prong, the States believe this element must be strengthened as well. Digital platforms, ad networks, and martech firms market themselves on the quality of analytics they can deliver and the level of targeting they can provide to potential advertisers. Indeed, these companies' business models rely on knowing everything there is to know about their audiences, including age-relevant information like where users go to school, what digital content they consume, what websites they frequent, when their birthdays are, what they search for, what apps they use, where they spend their free time, whether they live with a parent or siblings, and more. These companies utilize sophisticated algorithms to identify and target individual consumers in an effort to connect them with advertising those consumers are likely to interact with. Companies boast that they can "deliver deep insights into

[14] Available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[15] Fair, L., *$170 million FTC-NY YouTube settlement offers COPPA compliance tips for platforms and providers* (Sept. 2019) (available at https://www.ftc.gov/news-events/blogs/business-blog/2019/09/170-million-ftc-ny-youtube-settlement-offers-coppa).

how [their] users are interacting with . . . mobile apps and ads"[16] and target groups of consumers as narrow and specific as "Fashionistas," "Car Shoppers," and "College Students" using geolocation, social media usage tracking, internet cookies, and other information.[17] One such company even claims to be able to identify "families with kids" in a published case study.[18] In other words, these companies possess information that can and should be used to affirmatively identify websites or online services that are child-directed in practice (if not in name). However, these companies are disincentivized to use that data for COPPA compliance because so long as they refuse to do so, they can claim they lack "actual knowledge." As written, the Rule encourages a "see no evil" approach wherein sophisticated marketing companies are encouraged to use their massive amounts of user data to make money, but not to ensure the safety of children online.

Turning to the Rule's definition of "operator," the States contend that this definition may be construed too narrowly given the realities of the modern data economy. It could be argued that none of the thousands of martech firms discussed above fit within the Rule's definition of "operator" because the main sources of data they collect are not their own websites, but rather other operators' websites which do fall within the definition. These martech firms collect data from thousands of different operators, combine that data into detailed profiles, and then use those profiles to serve behavioral advertising to users of those websites. Operators can begin sending user data to martech companies and ad networks by simply entering a few lines of code into their app or website or by filling out an online form.[19] There is no verification, no diligence, and often the terms and conditions operators are asked to agree to are so loosely written that they do not even mention COPPA compliance as a requirement.[20] Other martech companies do not require operators to agree to or even read their terms and conditions prior to sending user data, burying the relevant language several pages deep within their corporate websites.[21] Because these companies arguably do not fall within the definition of "operator" and do almost nothing to confirm (or even require) COPPA compliance from the thousands or even millions of operators that send them data, they are free to vacuum up mountains of user data while deliberately trying to avoid ever acquiring actual knowledge that one or more of those operators might be illegally operating a child-directed website that collects data from children. By expanding COPPA's definition of "operator" to explicitly include entities like (i) martech firms, (ii) advertising networks and (iii) other entities that consume and analyze significant quantities of this data in order to provide their various products or services, the Rule would require compliance by those companies that **use and profit** from the data as well as by those companies that **collect** the data.

---

[16] Google AdMob marketing website (available at https://admob.google.com/home/?gclid=EAIaIQobChMI5uTghvqA5QIVgf5kCh1Mrgr1EAAYASAAEgJA3fD_BwE).
[17] InMobi marketing website (available at https://www.inmobi.com/audiences).
[18] InMobi case study (available at https://go.inmobi.net/hubfs/InMobi%20Case%20Studies/News%20Corp%20-%20Full%20Case%20Study%20(Audiences).pdf?__hstc=176039418.547586b4caaa62c6ecdfcbde7f0ee39d.1570135845993.1570135845993.1570135845993.1&__hssc=176039418.1.1570135845993&__hsfp=2352221248).
[19] *See, e.g.* ironSource SDK Integration instructions (available at https://developers.ironsrc.com/ironsource-mobile/android/android-sdk/#step-1).
[20] *See, e.g.* ironSource SDK Terms and Conditions (available at https://developers.ironsrc.com/ironsource-mobile/android/publisher-terms-conditions/); *see also* Moat, Inc., a martech company recently purchased by Oracle and integrated into Twitter's mobile publishing application (available at https://moat.com/sdklicense.txt).
[21] *See, e.g.* InMobi SDK Terms of Service (available at https://www.inmobi.com/terms-of-service/).

13. Should the Commission consider further revision to the definition of "Personal information"? Are there additional categories of information that should be expressly included in this definition, such as genetic data, fingerprints, retinal patterns, or other biometric data?

Yes, the Commission should further revise the definition of "Personal Information" to include biometric data, defined broadly to include genetic information as well as healthcare information. The 2013 amendments to the Rule's definition of "personal information" to include, among other things, a child's voice or image were a significant step in the right direction, but there is more that must be done to protect not just children's biometric data, but their genetic and healthcare information as well. Even more than an advertising ID, a web cookie, or an IP address, biometric data, genetic data, and healthcare information are singular, immutable, and permanent. The illegal collection of these types of data from children poses a profound risk of harm because these types of data can be used to identify a particular child **for life**. It is now commonplace to unlock a mobile device with a user's fingerprint or facial scan. But, as internet connectivity reaches devices like heart monitors, insulin pumps, blood pressure cuffs, inhalers, ingestible sensors, contact lenses, fitness trackers, and more, our vital healthcare information is becoming more and more accessible.[22] Smartphone applications can be used to detect depression. Wearable sensors can track sleep patterns, alert parents at the first sign of a child's fever, and track changes in gait and posture.

While anonymized blood pressure readings and inhaler usage patterns may not be immediately "individually identifiable" as that term is used in the Rule, when combined with persistent identifiers, geolocation information, IP addresses, WiFi access points, and other information, that data can be tied to an identifiable individual (as discussed, *infra*, healthcare data are routinely shown to be personally identifiable even when steps are taking to anonymize those data). One recent survey indicated that 97% of internet-connected healthcare device manufacturers plan to collect data from their devices, and one in five reported that they plan to sell that data.[23] When this data is collected from children, COPPA protections are necessarily implicated and the Rule must be updated to ensure protection of this most private and personal of all "personal information." Defining biometric data to specifically include imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings (from which an identifier template such as a faceprint, a minutiae template, or a voiceprint, can be extracted), as well as keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information, in addition to genetic information, would better protect children's sensitive personal information.

[22] *10 Examples of the Internet of Things in Healthcare*, Econsultancy (Feb. 2019) (available at https://econsultancy.com/internet-of-things-healthcare/).
[23] Kobeda, E., *Jabil 2018 Connected Health Technology Trends Survey*, Jabil (available at https://www.jabil.com/insights/blog-main/connected-health-data.html#download).

14. Should the definition of "Support for the internal operations of the website or online service" be modified? Are there practices in addition to behavioral targeting and profiling that should be expressly excluded from the definition? Should additional activities be expressly permitted under the definition? For example, should the definition expressly include advertising attribution?

Yes, the definition of "[s]upport for the internal operations of the website or online service" should be modified to **explicitly exclude** advertising attribution. Advertising attribution has nothing to do with the seven enumerated activities listed in the current definition in § 312.2. Attribution has one purpose: To increase the amount of money a website or app will get paid if a user interacts with advertising on that website or app and then takes some desired further action elsewhere on the internet, thereby increasing the value of advertising real estate on that particular website or app. The collection of persistent identifiers and other information for purposes of advertising attribution necessarily involves "recogniz[ing] a user over time and across different Web sites or online services," and therefore should be explicitly prohibited by the Rule.

Further, the term "serve contextual advertising" should be modified to require operators and other holders of this data to (i) limit the types of personal information and persistent identifiers they can collect for this purpose, and (ii) immediately delete any personal information and persistent identifiers collected for this purpose at the end of a user's session. As the Rule is currently written, operators have taken the position that they can freely collect (for example) unique device identifiers from children without parental consent for purposes of serving contextual advertising. However, there is no legal reason for operators to collect that particular persistent identifier unless the operator (or an ad network the operator sends that data to) plans to use that unique identifier to construct a profile of that user, use that identifier for attribution, and/or other impermissible uses of such data. Because operators have used this provision to freely collect data from children without parental permission, it should be drawn as narrowly as possible to ensure only the bare minimum amount of data needed to serve a contextual ad is collected. And because that data is purportedly being collected only for the narrow purpose of serving a contextual ad during that user's current session, operators should be prevented from transmitting that information to any other party and should be required to delete such information immediately and automatically upon termination of each session.

15. Does § 312.2 correctly articulate the factors to consider in determining whether a website or online service is directed to children? Do any of the current factors need to be clarified? Are there additional factors that should be considered? For example, should the definition be amended, consistent with the statute, to better address websites and online services that do not include traditionally child-oriented activities, but that have large numbers of child users? If so, what types of changes to the definition should be considered? Are there other proposed amendments, consistent with the statute, for the Commission to consider to ensure children using these types of websites and online services receive COPPA protections?

How a site or app is marketed, designed, and presented to the public are important factors in determining whether a site is child-directed. However, a critical part of the Rule's factors for determining whether a website or online service is directed at children is "competent and reliable empirical evidence regarding audience composition . . . ." The age of a website's models, whether

a website features animated characters (many of whom now originate in adult-oriented contexts[24]), and what kinds of music or visual content the website provides all constitute evidence regarding intended audience. However, the question of whether or not the site actually attracts users under the age of 13 is just as important, if not more so. In the era of mega-platforms like YouTube, which claims not to be a child-directed site per the Rule but whose child-directed content garners 65% higher viewership numbers than its non-child-directed content,[25] the critical inquiry is who is actually visiting the site. YouTube attracts 1.9 billion users every month, 300 million of whom are located in the U.S.[26] 2018 estimates put the number of children in the U.S. under the age of 14 at 60.9 million[27] and the total population of the U.S. at 327.2 million.[28] Thus, even giving YouTube the benefit of the doubt and assuming the 27.2 million Americans that did not visit YouTube last month are all under the age of 14, YouTube was still likely visited by more than 33 million children under the age of 14 last month. By YouTube's own statistics, YouTube is a massively popular website among children and YouTube's efforts to limit child use of its platform are utterly ineffective. The Rule should be amended to impose affirmative obligations upon operators, platforms, and others to use the data and resources **they already possess** to protect children, rather than just to make money.

16. Has the 2013 addition, found in part (3) of the definition of "website or online service directed to children," which permits those sites that do not target children as their primary audience to "age screen" users, resulted in stronger protections for children's privacy? Should the Rule be more specific about the appropriate methods for determining the age of users?

As the FTC/NYAG settlement with YouTube highlights, "age screening" (or "age gating") has not provided stronger protections, and the Rule should be more specific about the appropriate methods for determining the age of users. While the FTC FAQs make it clear that age gating must be performed "in a neutral fashion," that requirement is not codified in the Rule and many operators use non-neutral age gating to encourage users to enter ages older than 12, regardless of the users' actual age, especially if under 13. Because many operators rely on advertising as their sole source of revenue, and because behavioral advertising is worth much more to operators than contextual advertising, operators have a powerful incentive to shunt as many users into the "over 12" category as possible while maintaining their defense of relying upon the incorrect age entered by the user. As discussed elsewhere, operators and those that collect and profit from personal data should have an affirmative responsibility to use the massive amounts of data available to them to identify users that have entered incorrect information at an age gate and, once identified, immediately cease collecting data from those users and delete all previously collected data.

---

[24] Strauss, K., *Adult Cartoons & the Rise of the Late Night Network*, Forbes (July 2012) (available at https://www.forbes.com/sites/karstenstrauss/2012/07/28/adult-cartoons-the-rise-of-a-late-night-network/#78342d2e1042).

[25] Cutchin, J., *YouTube isn't for kids. But kids videos are among its most popular, study finds*, LA Times (July 2019) (available at https://www.latimes.com/business/story/2019-07-24/pew-study-youtube-children-content).

[26] Cooper, P., *22 YouTube Stats that Matter to Marketers in 2019*, Hootsuite (Jan. 2019) (available at https://blog.hootsuite.com/youtube-stats-marketers/).

[27] *Kids Count Data Center*, Annie E. Casey Foundation (available at https://datacenter.kidscount.org/data/tables/101-child-population-by-age-group#detailed/1/any/false/37,871,870,573,869,36,868,867,133,38/62,63,64,6,4693/419,420).

[28] *U.S. and World Population Clock*, U.S. Census Bureau (available at https://www.census.gov/popclock/).

E. Exceptions to Verifiable Parental Consent

21. COPPA and § 312.5(c) of the Rule set forth eight exceptions to the prior parental consent requirement. Are the exceptions in § 312.5(c) clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?

As discussed above, the Rule's exception contained in § 312.5(c)(7) permitting collection of persistent identifiers "for the sole purpose of providing support for the internal operations of the Web site or online service" is too broad (see response to Question 14, *supra*). Again, any exception to the Rule that allows operators to freely collect information from children without parental consent should (i) be written and construed as narrowly as possible, (ii) require operators to delete that information at the end of each session, and (iii) prohibit operators from distributing that information to any third party for any reason other than those permitted by the Rule.

23. In the Statement of Basis and Purpose to the 1999 COPPA Rule, the Commission noted that the Rule "does not preclude schools from acting as intermediaries between operators and schools in the notice and consent process, or from serving as the parents' agent in the process." Since that time, there has been a significant expansion of education technology used in classrooms. Should the Commission consider a specific exception to parental consent for the use of education technology used in the schools?

Quite the opposite. Not only should the Commission not consider a specific exception to parental consent, the Commission should also reconsider its Statement of Basis and Purpose because its Statement of Basis and Purpose does not comport with the plain language of § 312.5 of the Rule. In effect, the Statement of Basis and Purpose, *ultra vires*, has created a significant exception to COPPA's parental consent requirements.

The growth of technology in the classroom over the last twenty years cannot be overstated. Internet usage at school among children ages 3 to 4 increased 48% from 2011 to 2017, with students aged 5 to 10 years old increasing their school-based usage more than 31%.[29] 88% of school districts now have access to broadband internet services. Entire K-12 charter schools now exist completely online[30] and 24 states offer free online public school access.[31]

This growth has occurred in tandem with a corresponding explosion in digital tools created by private industry for use in the classroom ("education technology" or "edtech"). Edtech is now an $11 billion industry,[32] and is dominated by familiar names like Google and Microsoft. Since its introduction in October 2006, Google's G-Suite for Education platform (previously Google Apps for Education) has swelled to more than 80 million users worldwide and claims approximately

[29] *Percentage of persons age 3 and over who use the Internet anywhere and who use the Internet at selected locations, by selected characteristics: 2011 and 2017*, National Center for Education Statistics)available at https://nces.ed.gov/programs/digest/d18/tables/dt18_702.30.asp?current=yes).
[30] *See, e.g.* K12, Inc. (available at https://www.k12.com/).
[31] *State-by-State List of Free Online Public Schools, K-12*, ThoughtCo (available at https://www.thoughtco.com/free-online-public-schools-4148138).
[32] Sadwick, R., *We're Spending $11B on Education Technology: How Do We Know If It's Working?*, Forbes (Sept. 2019) (available at https://www.forbes.com/sites/rebeccasadwick/2019/09/09/11b-on-edtech/#7a1021c19ce8).

60% of the North American market for such services.[33] Microsoft's Office 365 for Education boasts 7 million monthly active users worldwide.

However, these technologies are not cabined to the classroom, and are instead often designed to encourage use by students at home, or for non-educational purposes. For example, while Google's G-Suite for Education is marketed to schools as a purely educational platform tool, the platform includes access to Google's core services: Gmail, Calendar, Talk/Hangouts, Drive, Docs, Sheets, Slides, Contacts and more. In a commercial context, Google relies on these same services to collect and monetize users' personal data. If schools may serve as proxies for parents under COPPA's consent regime, nothing prevents Google from relying on its relationship with schools to allow it to upload and store data such as students' bookmarks, web searches, passwords, and online browsing habits, regardless of whether the online activity occurs for educational purposes, or occurs during or outside of school hours. Nor would anything prevent these data points from becoming permanently associated with the child's G Suite account (and therefore, permanently associated with the child).

Critically, edtech accounts or usage are typically mandatory. Thus, in entertaining an exception to the parental consent requirement under COPPA for edtech, the Commission risks creating an exception that would swallow the rule and force parents to choose between their children's access to education and their online privacy that is otherwise ensured by COPPA.

24. In 2017, the Commission issued an enforcement policy statement addressing the use of audio files containing a child's voice. The Commission explained that it would not take an enforcement action against an operator for not obtaining parental consent before collecting an audio file with a child's voice when the audio file is collected solely as a replacement for written words, such as to perform a search, so long as the audio file is held for a brief time and used only for that purpose. Should the Commission amend the Rule to specifically include such an exception? If the Commission were to include such an exception, should an operator be able to de-identify these audio files and use them to improve its products? If so, for how long should operators be permitted to retain such de-identified audio files? Is de-identification of audio files effective at preventing re-identification? Are there specific technical, administrative, operational or other procedural safeguards that have proved effective at preventing re-identification of de-identified data? Are there instances in which de-identified information has been sold or hacked and then re-identified?

The Commission should not allow the collection and retention of any biometric data—including children's voices—for any commercial purposes. Biometric data are particularly deserving of privacy protections, given that they are both individually-identifying and immutable. Unlike clearing a cookie, a browser history, or an advertising identifier, a child cannot "reset" her voice, making it one of the most persistently- and individually-identifying data points in existence. Relatedly, it is unclear—to the point of dubiousness—that an operator would be able to successfully or consistently keep audio files "de-identified," given the uniqueness of a given individual's voice. Indeed, Google researchers published a paper in 2015 announcing that an

[33] *All types of Chromebooks for all types of learners*, Google Blog (available at https://blog.google/outreach-initiatives/education/all-types-chromebooks-all-types-learners/).

artificial neural network could verify the identity of a speaker saying "OK Google" with 98% precision.[34]

Concerning the Commission's question regarding hacked or sold data being re-identified, there are myriad instances in which purportedly anonymized data was intentionally put into the public space—or otherwise obtained—only to be shown to be individually identifiable. For example, in August 2016, the Australian government released medical billing records of 2.9 million people, from which names and other identifying features were removed. Researchers from the University of Melbourne then took the de-identified open health dataset and published a paper in which they described the ease with which the records could be re-identified by comparing the dataset to other publicly available information.[35] In 2017, German researchers acquired a database containing nine billion URLs from three million German users, spread over nine million different sites.[36] The researchers then proceeded to identify a variety of methods to individually identify specific users based on the purportedly anonymous data. While not a "breach," *per se*, the researchers acquired the database simply by creating a fake marketing company and then solicited raw clickstream data from nearly one hundred companies—critically, no one identified by this research had known that their browsing history would be used for this purpose.[37]

Nor is re-identification of anonymized data a new phenomenon. In 1996, the Massachusetts Group Insurance Commission released "anonymized" data showing the hospital visits of state employees (like the above-described Australian dataset, traditional personal identifiable information like names, address, and social security numbers were removed from the corpus). One researcher, who later became Chief Technologist for the Commission, quickly de-anonymized the data and, as a proof-of-concept, provided then-Governor Bill Weld with his own medical records using only the dataset and publicly-available information.[38] Most recently, researchers published work stating that they could correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes.[39] Other researchers claim only to need four data points.[40]

Because voice biometrics implicate such profound and unalterable privacy issues for a given individual, it would be a grave mistake to allow operators to collect, store, or utilize children's voices without obtaining verifiable parental consent.

---

[34] Heigold, et al., *End-to-end text-dependent speaker verification* (Sept. 2015) (available at https://arxiv.org/pdf/1509.08062.pdf).
[35] Culnane, *et al.*, *Health Data in An Open World* (Dec. 2017) (available at https://arxiv.org/abs/1712.05627).
[36] Hern, A., *'Anonymous' browsing data can be easily exposed, researchers reveal*, The Guardian (Aug. 2017) (available at https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers).
[37] *Id.*
[38] *Id.*
[39] Rocher, *et al.*, *Estimating the success of re-identifications in incomplete datasets using generative models*, (July 2019) (available at https://www.nature.com/articles/s41467-019-10933-3/).
[40] Singer, N., *With a Few Bits of Data, Researchers Identify 'Anonymous' People*, New York Times (Jan. 2015) (available at https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/).

25. In some circumstances, operators of general audience platforms do not have COPPA liability for their collection of personal information from users of child-directed content on their platform uploaded by third parties, absent the platforms' actual knowledge that the content is directed to children. Operators of such platforms therefore may have an incentive to avoid gaining actual knowledge of the presence of child-directed content on their platform. To encourage such platforms to take steps to identify and police child-directed content uploaded by others, should the Commission make modifications to the COPPA Rule? For example, should such platforms that identify and police child-directed content be able to rebut the presumption that all users of the child-directed third-party content are children thereby allowing the platform to treat under and over age 13 users differently? Given that most users of a general audience platform are adults, there may be a greater likelihood that adults are viewing or interacting with child-directed content than on traditional child-directed sites. In considering this issue, the Commission specifically requests comment on the following:

a. Would allowing these types of general audience platforms to treat over and under age 13 users differently encourage them to take affirmative steps to identify child-directed content generated by third parties and treat it in accordance with COPPA?

The Request for Public Comment contemplates modifying the Rule to add another exception for general audience platforms that host third-party content. Specifically, it seeks comment on whether general audience platforms should be permitted to "treat over and under age 13 users differently to encourage the platforms to take affirmative steps to identify child-directed content generated by third parties…." The Request suggests this change may be appropriate because "there may be a greater likelihood that adults are viewing or interacting with child-directed content [on platforms] than on traditional child-directed sites…given that most users of a general audience platform are adults."

As an initial matter, it is unlikely that the approach set forth in the Request for Public Comment would incentivize general audience platforms to identify and police child-directed content. Under the proposed framework, a general audience platform that identifies child-directed content would be permitted to use an age screen and serve advertising that tracks a user (i.e., "online behavior advertising" or "OBA") to users 13 and over. However, a platform that takes no affirmative steps to identify child-directed content could continue to serve OBA to all users. A platform that identifies child-directed content would therefore earn less revenue and expose itself to additional potential liability. Most platforms would not take this path.

Moreover, the States have grave concerns that the change under consideration in the Request for Public Comment would expose children to the type of data collection the Rule is intended to prevent. Platforms employing an age screen are likely to misidentify children as older users that are not subject to COPPA. Websites with an age screen typically collect a user's age information once, during the account creation process, and use that information on each of the user's subsequent visits to the website. This can be problematic if, as is commonly the case, the user logged in to the account on a device that is shared across a household and never logged out—regardless of who in the household subsequently uses the device, the site will treat the user as the accountholder. The problem is particularly acute on a platform that hosts both child-directed and

general audience content because children and their parents may routinely visit the same site. If they do so on a shared device that remains logged in to a parent's account, the children will be treated as adults.

This issue is compounded where an account is used across a variety of distinct sites and services, some of which are directed to children. For example, a user account created through one Google product or service can be used to access many others, from Android to YouTube, just as an Apple account can be used with a diverse selection of Apple products. There is little reason to believe that the person who logged in to Gmail on a desktop computer shared by a family of four is the same person who used that computer to watch cartoons on YouTube three weeks later simply because the account remained logged in during that time.

The States therefore would not recommend a change to the COPPA framework that would permit general audience platforms to age screen users without robust processes in place to ensure that the user is at least 13 years old. Age information associated with an account that has remained logged in on a device should not, on its own, be sufficient to establish that a user on the device is 13 or older. Nor should periodic authentication be sufficient. Instead, an additional showing should be required. For example, a website might ask during the account creation process whether a child ever uses the user's device.

G. Confidentiality, Security, and Integrity of Personal Information

28. Section 312.8 of the Rule requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from a child, and to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the personal information, and who provide assurances that they will do so.

b. Is § 312.8 of the Rule clear and adequate? If not, how could it be improved, consistent with the Act's requirements? Should the Rule include more specific information security requirements, for example to require encryption of certain personal information?

Given the proliferation of data breaches across all industries, this requirement of COPPA is particularly meaningful. The States maintain that, as written, this requirement is appropriately broad and correctly worded to require that (i) the absolute minimal amount of personal information of children is collected and, (ii) when it is collected, it is stored for the minimal amount of time and/or in as secure a manner as possible. If security requirements are added to the Rule, they should be illustrative rather than exhaustive, and it should be made clear that simply adhering to those requirements will not necessarily satisfy the obligations should a security event occur. Given the rapid advances in technology and the enterprising nature of cybercriminals, any operator that is storing children's personal information should be encouraged to consistently monitor and update their security protocols to evolve at the same pace as the cyber threats they are meant to guard against. The Commission should not provide an exhaustive list of security protocols that, at the time of promulgation, were state-of-the-art and effective, but within a few years' time become or risk becoming outdated. This would effectively incentivize operators to adopt only those measures

outlined in the Rule, and likely would not have any protective effect once the measures were surpassed by evolving cyber threats.

Respectfully submitted,

FOR THE STATE OF NEW MEXICO

Hector Balderas, Attorney General

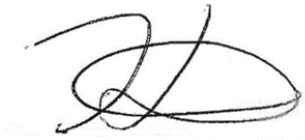
FOR THE STATE OF CONNECTICUT

William Tong, Attorney General

FOR THE STATE OF DELAWARE

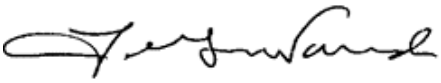
Kathleen Jennings, Attorney General

FOR THE DISTRICT OF COLUMBIA



Karl Racine, Attorney General

FOR THE STATE OF IDAHO



Lawrence G. Wasden, Attorney General

FOR THE STATE OF ILLINOIS

Kwame Raoul, Attorney General

FOR THE STATE OF IOWA

Thomas J. Miller, Attorney General

FOR THE COMMONWEALTH OF KENTUCKY

Andy Beshear, Attorney General

FOR THE STATE OF LOUISIANA

Jeff Landry, Attorney General

FOR THE STATE OF MAINE

Aaron M. Frey, Attorney General

FOR THE STATE OF MARYLAND

Brian E. Frosh, Attorney General

FOR THE COMMONWEALTH OF MASSACHUSETTS

Maura Healey, Attorney General

FOR THE STATE OF MICHIGAN

Dana Nessel, Attorney General

FOR THE STATE OF MINNESOTA

Keith Ellison, Attorney General

FOR THE STATE OF MISSISSIPPI

Jim Hood, Attorney General

FOR THE STATE OF NEBRASKA

Douglas J. Peterson, Attorney General

FOR THE STATE OF NEVADA

Aaron D. Ford, Attorney General

FOR THE STATE OF NEW YORK

Letitia James, Attorney General

FOR THE STATE OF NORTH CAROLINA

Josh Stein, Attorney General

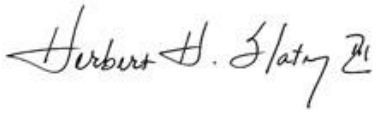
FOR THE STATE OF OREGON

Ellen F. Rosenblum, Attorney General

FOR THE COMMONWEALTH OF PENNSYLVANIA

Josh Shapiro, Attorney General

FOR THE STATE OF TENNESSEE

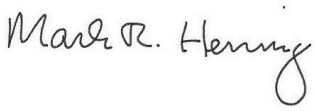


Herbert H. Slatery III, Attorney General

FOR THE STATE OF VERMONT

T.J. Donovan, Attorney General

FOR THE COMMONWEALTH OF VIRGINIA



Mark R. Herring, Attorney General

FOR THE STATE OF WASHINGTON

Bob Ferguson, Attorney General