Comments from

to

Federal Trade Commission

December 11, 2019

COPPA Rule Review
16 CFR part 312
Project No. P195404

Sara Collins, Policy Counsel, Education & Youth Privacy
John Verdi, Vice President of Policy
The Future of Privacy Forum
1400 I St. NW Ste. 450
Washington, DC 20005

www.fpf.org

On behalf of the Future of Privacy Forum (FPF), we are pleased to submit these comments in response to the Federal Trade Commission (FTC) Request for Comment. FPF is a Washington, DC-based nonprofit organization that serves as a catalyst for privacy leadership and scholarship, by advancing principled data practices in support of emerging technologies.

FPF routinely provides expert testimony and comments to Congress,[1] federal agencies,[2] Congressionally-chartered commissions,[3] and legislatures in the states[4] and around the world.[5] We also run the annual *Privacy Papers for Policymakers*[6] program, which brings academic expertise to Members of Congress, leaders of executive agencies, and their staff to better inform policy approaches to privacy and data protection. FPF events, such as *Student Privacy Bootcamps*,[7] the *Digital Data Flows Masterclass*,[8] and the *Privacy Book Club*[9] are attended by advocates, academics, government officials, and industry representatives in order to gain the latest insight and understanding of current privacy issues.

The Children's Online Privacy Protection Act (COPPA) has been an influential, useful law in the fight to keep children safe on the internet. However, COPPA must keep up with the rapidly evolving ways that children use internet-connected devices and navigate connected physical spaces. In light of emerging technologies, FPF recommends that the FTC:

1. Codify its nonenforcement policy for operators that do not obtain verifiable parental consent before collecting an audio file of a child's voice, provided the file is collected solely to perform a verbal instruction or request and is deleted immediately after the purpose fulfillment;
2. Provide guidance regarding COPPA's definition of "actual knowledge" as it relates to emerging use cases where children may be identified in large, otherwise "general audience" datasets; and

[1] Amelia Vance, *FPF Testifies Before Congress on Promoting and Protecting Student Privacy*, Future of Privacy Forum (May 17, 2018), https://fpf.org/2018/05/17/studentprivacycongressionalhearing/.
[2] Press Release, Federal Trade Commission, Student Privacy and Ed Tech (Dec. 1, 2017).
[3] Commission on Evidence-Based Policymaking, *The Promise of Evidence-Based Policymaking: Report of the Commission on Evidence-Based Policymaking*, App. G 310 (2017).
[4] Amelia Vance, *FPF Letter to NY State Legislature*, Future of Privacy Forum (June 17, 2019), https://fpf.org/2019/06/17/fpf-letter-to-ny-state-legislature/.
[5] Liron Tzur Neumann, *"Legislating Online" Conference – The Knesset, Israel Parliament*, Israel Tech Policy Institute (Oct. 24, 2018), https://techpolicy.org.il/legislating-online-conference-the-knesset-israel-parliament/.
[6] Future of Privacy Forum, *10th Annual Privacy Papers for Policymakers* (2019), https://fpf.org/event/10th-annual-privacy-papers-for-policymakers/.
[7] *See*, Tyler Park, *FPF to Co-Host Student Privacy Bootcamp with Student Data Privacy Consortium*, Future of Privacy Forum (Jan. 3, 2019), https://fpf.org/2019/01/03/fpf-to-co-host-student-privacy-bootcamp-with-student-data-privacy-consortium-1-28/.
[8] Future of Privacy Forum, *Digital Data Flows Masterclass: Emerging Technologies* (2019), https://fpf.org/classes/.
[9] Future of Privacy Forum, *Privacy Book Club* (2019), https://fpf.org/privacy-book-club/.

3. Clarify the circumstances in which schools may exclusively exercise COPPA rights regarding student data, in line with their obligations under the Family Educational Rights and Privacy Act (FERPA).

1. Voice-Enabled Technologies: Guidance is Needed to Distinguish Between COPPA's Treatment of Different Use Cases

We recommend that the Commission provide further guidance on voice-enabled devices that are marketed to children or are "general audience" services used by children. A key distinction is how voice recordings are used – as a user interface to dictate commands (speech recognition), or as a biometric identifier (voice recognition) or means of distinguishing between accounts through voice profiles. Speech recognition is the ability to speak naturally and contextually with a computer system in order to execute simple commands, dictate language, or translate speech into text.[10] Voice recognition is the biometric identification of an individual by the characteristics of her voice.[11]

The prevalence and accuracy of voice-enabled technologies has increased rapidly as a result of machine learning on large datasets.[12] By sending voice data to the cloud, where powerful machine learning can be applied, voice-enabled devices can adapt to speech patterns over time and understand speech in context.[13] Since 2016, this kind of core functionality has moved beyond the realm of "smart speakers" and "home assistants." It is being integrated as a service in many other devices both in and out of the home -- such as connected cars, smart TVs, and city kiosks.[14] In response to privacy concerns regarding the increased collection and use of voice data, lawmakers proposed, and in some cases passed, bills at both the federal and state level in 2018.[15] As a result, it is both important and timely for the FTC to provide guidance regarding the many uses of voice-enabled technologies that can impact children.

---

[10] *See* Stacey Gray, *Always On: Privacy Implications of Microphone-Enabled Devices*, Future of Privacy Forum (April 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.
[11] Id.
[12] *"I hear you" Speech Recognition*, Technology Quarterly, The Economist (Jan. 5, 2017) https://www.economist.com/technology-quarterly/2017/01/05/speech-recognition.
[13] *See* Stacey Gray, *Always On: Privacy Implications of Microphone-Enabled Devices*, Future of Privacy Forum (April 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.
[14] *See, e.g.*, Telenav Connected Car Platform, https://www.telenav.com/products/connected-car-platform (last visited Oct. 17, 2019); Samsung 2019 QLED TV, https://www.samsung.com/us/televisions-home-theater/tvs/qled-8k-tvs/ (last visited Oct. 17, 2019); IKE Smart City Kiosk, https://www.ikesmartcity.com (last visited Oct. 17, 2019).
[15] *See, e.g.*, Stacey Gray, *California's AB-1395 Highlights the Challenges of Regulating Voice Recognition*, Future of Privacy Forum (July 3, 2019), https://fpf.org/2019/07/03/californias-ab-1395-highlights-the-challenges-of-regulating-voice-recognition/; NJ AB-2232 (Prohibits television voice recognition features from collecting or recording users without notice; prohibits use or sale of recordings for advertising purposes.).

Speech Recognition: Speech Recognition Presents Fewer Privacy Risks than Voice Recognition.

Voice data in the context of connected devices is predominantly used for speech recognition - the ability to speak naturally and contextually with a computer system in order to execute simple commands, dictate language, or translate speech into text.[16] The use of speech recognition as a means to communicate with (and through) connected devices has improved the lives of people with physical disabilities, makes healthcare and other professional services more efficient through accurate speech dictation, enhances automobile safety, and makes everyday tasks more convenient. Over the last forty years, speech recognition technology has improved dramatically. Consumers can now interact reasonably well via speech with a range of devices.

The majority of voice-enabled devices on the market today are products for which speech is a useful interface for engagement. Increasingly, connected toys, tablets, and other devices that are marketed toward children can now be equipped with speech recognition features. For example, in 2015, Mattel developed "Hello Barbie," a WiFi-connected doll, which uses speech recognition to respond to a child that answers the doll's simple, pre-set questions.[17] When devices such as these are marketed to children under 13, we appreciate that the FTC has been clear that they must comply with COPPA.[18]

Voice Recognition: Voice as a Biometric Identifier

Rapidly advancing technologies in voice-enabled devices are able to uniquely identify a person through the biometric characteristics of her voice. Unique voice recognition can be a useful consumer tool—for example, to permit only a specific person to access a device, to enable parental controls by distinguishing between user accounts, or to better detect fraudulent telephone transactions. The collection of certain voice characteristics for the purpose of recognizing an individual currently implicates a range of laws. At the federal level, a "voice print" is considered either a biometric or personal record in the context of the Privacy Act[19], FERPA[20],

[16] Id.
[17] Letter from Electronic Privacy Information Center (EPIC) to Attorney General Loretta Lynch and FTC Chairwoman Edith Ramirez (July 10, 2015), available at https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.
[18] FTC updated guidance (children's toys)
[19] 22 C.F.R. § 308.3 ("Record means any document, collection, or grouping of information about an individual maintained by the agency, including but not limited to . . . any other personal information which contains . . . a finger or voiceprint.").
[20] 34 C.F.R. § 99.3 ("Biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include . . . voiceprints").

and HIPAA.[21] Similarly, many states have expanded their legal definitions of personally identifiable information in certain privacy or breach notification laws to include some form of biometrics.[22]

Recommendations for Voice-Enabled Technologies

The rapid advancement of voice and speech recognition technologies in recent years, paired with the lack of regulatory certainty, is causing concerns about the use of voice-enabled technologies in child-directed products. The FTC should take this opportunity to create rules that protect children from harm, while allowing the many beneficial uses of these remarkable technologies.

For example, the parental rights to delete data and data retention limits that exist in COPPA are uniquely important privacy concerns in the context of voice data. On the one hand, access to large amounts of data has driven the rapid advancement of voice recognition technology in the last decade, and continues to drive product improvement.[23] Yet, the sensitivity of such data makes consumer advocates justifiably wary of "default" indefinite data retention policies. In light of this tension, an approach to voice data deletion and retention should go beyond a simple "all or nothing" framework. Instead, we urge the FTC to consider how to incentivize strong deletion options at the user-control level and strong de-identification. For example, a nuanced approach might be to require or encourage companies to create meaningful, easier-to-use choices, such as automatic recurring deletion options.[24] Another common-sense privacy protection would be to require that it be possible to request data deletion through a voice request.

The Commission has already begun drawing practical distinctions between different uses of audio recordings, as illustrated by its 2017 Commission policy statement.[25] The statement announced that the FTC will not bring enforcement actions against operators that do not obtain verifiable parental consent before collecting an audio file of a child's voice when the file is collected solely to perform a verbal instruction or request and is deleted immediately after its

[21] 45 C.F.R. § 164.514 (listing "[b]iometric identifiers, including finger and voice prints" as examples of personal information that must be removed from a data set before that data set can be considered properly de-identified and thus no longer subject to HIPAA regulations).
[22] *See, e.g.*, Conn. Gen. Stat. § 38a-999b; Iowa Code § 715C.1; Neb. Rev. Stat. § 87-802; N.C. Gen. Stat. § 75-66; Or. Rev. Stat. § 165.800; Or. Rev. Stat. § 336.184 (regulating student educational records); Wis. Stat. § 943.201; Wyo. Stat. § 6-3-901.
[23] For example, companies' ability to train machine learning models on very large datasets of human speech have dramatically improved models on heavy accents, unusual speech patterns, and non-English speech.
[24] *See* David Monsees, *Introducing auto-delete controls for your Location History and activity data*, Google (May 1, 2019), https://www.blog.google/technology/safety-security/automatically-delete-data.
[25] Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings, 82 Fed. Reg. 58076 (Dec. 8, 2017).

purpose has been fulfilled.[26] This is a practical approach that the Commission should consider codifying, as it recognizes the value of using voice as a replacement for written words for performing functions on devices.[27] Further, it distinguishes the risk posed by audio files that are stored only long enough to effectuate a verbal instruction from that of audio files stored for a longer period or for other purposes. Future of Privacy Forum supports the Commission's policy and encourages promulgation of rules based upon that policy.

2. Actual Knowledge: Greater Clarity is Needed

We recommend that the Commission develop and promulgate guidance clarifying the definition of COPPA's "actual knowledge" standard, especially as it applies to analysis of large data sets (big data). The FTC has identified several relatively clear circumstances in which general audience services are typically deemed to have actual knowledge that they are collecting personal data from children, and another relatively well-defined set of circumstances in which general audience services do not likely have such knowledge. General audience services will increasingly find themselves in circumstances between these two poles - able to infer with some degree of certainty that they are collecting information from children, but lacking the sort of definitive information that would give rise to "actual knowledge" under the Commission's current guidance. Children, parents, and companies would benefit from greater clarity regarding what sorts of age inferences - if any - would meet COPPA's actual knowledge standard.

General audience services do not have COPPA obligations unless the operator has actual knowledge that it is collecting personally identifiable information from a person under the age of 13.[28] The Commission has made it clear that "general audience" websites and online services are not typically required to take affirmative steps to identify users who may be children.[29] And general audience services are not deemed to acquire actual knowledge of data collection from children merely because they have a general suspicion that children might use the service. At the same time, general audience services can be deemed to acquire actual knowledge of data collection from children through several means: a user indicating they are under 13 using site-provided tools or in a moderated discussion forum; the company receiving notification from a parent that their child is using the service; an employee independently identifying child-directed third-party content posted to the service; or the service receiving a direct communication from a

[26] Id.
[27] Id.
[28] *See* Federal Trade Commission; Children's Online Privacy Protection Rule; Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59889 ("For general audience sites, the Act explicitly covers operators who have actual knowledge that they are collecting personal information from children.")
[29] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions ("The [COPPA] Rule does not require operators to ask the age of visitors").

third-party content provider notifying the service that content provided to the service is child-directed.[30]

Although there is still important social and legal value to broadly exempting "general audience" services from child-specific regulation in the absence of actual knowledge, the rise of large data sets, like those derived from internet-connected devices or location applications, has placed ever greater tension on this portion of the two-part COPPA prong, leading to calls from advocates for the FTC to adopt a "constructive knowledge"[31] standard. A "constructive knowledge" standard would be overbroad and would impose a significant compliance burden on companies, while not providing a commensurate benefit to children's privacy. But, there remains significant confusion, even among COPPA experts, about what business practices constitute actual knowledge.[32] As a result, we recommend that the Commission develop guidance, or if necessary, promulgate additional rules, to provide greater clarity for businesses and parents in line with reasonable public policy goals that balance children's access to the internet with much-needed company safeguards and corporate responsibility. In particular, existing FTC guidance does not provide general audience services with clarity regarding situations in which large data set holders will be considered to have "actual knowledge" that they are collecting data from children.

We urge the Commission, when developing guidance for the actual knowledge standard, to consider three important factors:

1) Children can and should have access to the internet.
2) Companies should not be incentivized to conduct additional analysis or data processing to find children.
3) Strong inferences derived from user data must be considered when making a determination of actual knowledge.

The General Data Protection Regulation (GDPR),[33] frames child-specific provisions as rights retained by the child, in contrast to COPPA's framework, which focuses on giving parents'

---

[30] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

[31] S. 748, 116th Cong. § 3(b)(2)(a)(1) (2019-2020), available at https://www.markey.senate.gov/imo/media/doc/Leg%20text%20--Markey-Hawley%203.11.19%20FINAL.pdf.

[32] The FTC convened child privacy experts to discuss elements of the rule as part of the COPPA rulemaking process on October 7, 2019. Federal Trade Commission, *The Future of the COPPA Rule: An FTC Workshop*, https://www.ftc.gov/news-events/events-calendar/future-coppa-rule-ftc-workshop. During the workshop, several experts expressed different conceptions of the "actual knowledge" standard, for example, Attorney Phyllis Marcus raised the point that recent FTC decisions lead practitioners to believe that actual knowledge means "child-directed" in practice.

[33] Commission Regulation 2016/679, 2016 O.J. (L119) arts. 7(3), 13-22, 34, 77-79, and 82; recitals 38, 58, 65, and 75, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-

notice and choice about their child's internet use. The GDPR's children's rights framework builds on the work that the United Nations Children's Fund[34] regarding children and the internet. A grounding principle of this work is that children have the right to access the internet. We would urge the Commission to not create an actual knowledge test that limits the ability for children to access the internet, especially given that children are using the internet to learn about the world around them, find enriching communities, and engage in self-discovery.

The general audience exception to COPPA is not just statutorily required, but fundamental for maintaining a free and open internet that is useful for adult and teen users. In 1998, Congress passed the Children's Online Protection Act[35] to prevent minors from accessing pornography on the internet. The Supreme Court found that the law was likely unconstitutional, citing the Commission on Child Online Protection's finding that filtering and parental controls, rather than an overly broad statue, would be a superior method of "restricting minors' ability to gain access to harmful materials on the internet."[36] Any new guidance or rulemaking should consider how the guidance or rule would affect adults using the internet. With regard to the actual knowledge standard, the FTC must take care, in its effort to protect children's privacy, not to diminish the privacy of adults using the internet. That means the FTC should not incentivize general audience sites to collect more information about their users as a method of complying with COPPA.

Creating an internet that is safe and welcoming for children can conflict with preserving the internet that is useful and responsive for adults. The actual knowledge standard can be a pragmatic way to balance those interests. However, an influx of technology that analyzes large data sets from general audience websites and services raises a new COPPA question that is unanswered by the current COPPA rule and guidance - when do inferences derived from user data create actual knowledge? To illustrate this question, consider four general audience services that might learn - with greater or lesser degrees of certainty - that children could be using their services: a public WiFi provider, a brick and mortar store front with a companion mobile app, and a GPS application.

20160504. For a discussion of children's rights under GDPR, *see* Information Commissioner's Office, *What rights do children have,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/ (last visited Nov. 25, 2019).

[34] UNICEF, *Children's rights and Internet*, https://www.unicef.org/csr/childrensrightsandinternet.htm (last visited Nov. 25, 2019); *see also* UNICEF, *Children's Online Privacy and Freedom of Expression: Industry Toolkit*, https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf (May 2018) ("[c]hildren have the right to freedom of expression and access to information diversity from a diversity of sources.").

[35] 47 U.S.C. § 231

[36] *Ashcroft v. ACLU*, 542 U.S. 656, 696 (2004).

The explosion in growth of the internet of things[37] has meant that more devices than ever may connect to public WiFi. In some cases, a WiFi provider may collect MAC addresses. These addresses are unique to the manufacturer of the hardware;[38] WiFi providers can identify the manufacturer by the MAC address. For a public WiFi provider that analyzes MAC addresses to see what devices are connected, this poses an interesting question. There are some devices that can be virtually guaranteed to only be operated by individuals over the age of 13 - e.g. connected cars. Most devices that connect to public WiFi are used by people of all ages, like smartphones and laptops; this information would not enable to the WiFi provider to make strong inferences about users' ages. The thornier issue of knowledge arises in the case of connected toys. Some toys, like a quadrocopter, are far more likely to be used by an adult than a child under the age of 13. Other toys, like RC cars that operate over WiFi, are used by all ages. However, there are some toys that raise a strong inference that the user is a child. These include toys that target preschoolers or kindergarteners exclusively, as well as wearables designed for toddlers and infants. As this example shows, there exists a "spectrum of identifiability"[39] when it comes to inferring age based on use of connected devices. If a WiFi provider uses analytics to determine what types of devices are on its network, what sort of inferences would trigger actual knowledge under COPPA? While it is easy to exclude devices like cars, smartphones, and laptops as actual knowledge triggers, where is the line drawn for connected toys? What about other products specifically designed to be used by children under the age of 13?

Brick and mortar retail stores often have accompanying general audience mobile apps that interact with the store. These applications' terms of service frequently restrict their use to users 13 and older. Retailers are increasingly analyzing customers' in-store activities, and making inferences about their age, gender, and shopping patterns. In a department store with a companion app, there are children's clothing and even children's toys during the Christmas season. The department store's data analysis may indicate that certain users are shopping in those sections; but department stores don't typically appeal to children, and many adults and teenagers shop for children's gifts, so this sort of data would not lead the store to infer that these users were children. A toy store could operate a similar analytics program, and perhaps draw a stronger inference about the age of certain users - there are only toys for sale, and toy stores typically provide a few places to play with select toys. These can include a table with building blocks, a place to test out bikes, and a kiosk to try out the latest gaming system. The

[37] "Internet of Things . . . or smart devices refers to any object or device that is connected to the Internet. This rapidly expanding set of "things," which can send and receive data, includes cars, appliances, smart watches, lighting, home assistants, home security, and more." Dep't of Commerce, *Internet of Things* (Oct. 25, 2019), https://www.commerce.gov/news/blog/2019/10/internet-things.
[38] WhatIsMyIPAddress.com, *What is a MAC address?*, https://whatismyipaddress.com/mac-address (last visited Nov. 25, 2019).
[39] *See* Jules Polonetsky, Omer Tene, and Kelsey Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 SantaClaraL. Rev. 593 (2016).

toy store's age inference might be stronger if a user spends a significant portion of their visit at a location that is designed for play. Some toy stores are creating retail experiences that are primarily or solely experiential. Most floor space provides places to play and there are numerous toys out and available for demonstration and play. These stores stock few toys - their core function is providing an opportunity to demo toys and purchase items for delivery through an online application. The main purpose of the store is to play with the toys, rather than buy them. The experiential toy store's data analysis might lead to a stronger inference that particular shoppers and app users are children - perhaps a user plays at the building block station, spends a small amount of time at the tricycle area, and ends their visit at in-store toddler playset. This pattern of movement would suggest that a child is the application user. Sophisticated data analysis can give retailers varying degrees of confidence when they infer the ages of shoppers and app users. FTC guidance could help make it clear when - if ever - these sorts of inferences might implicate COPPA's actual knowledge standard.

Like public WiFi providers and retail store apps, a GPS application is a general audience product. People of all ages use these applications to determine where they are or to get directions to where they want to go. These data sets can make inferences - some weak, some fairly strong - about users' ages. Location data may reveal that an individual user never requests driving directions - just walking, biking, or public transportation. That pattern on its own would not imply that the user is a child; many adults do not drive. Other data might indicate that the user's most commonly visited locations include an elementary school, a playground, and an ice cream parlor. This additional information might more strongly suggest the user is a child, but it's not conclusory. The user could be a parent or a teacher. Further data analysis might reveal that when the user is walking, their strides and their pace correspond to someone who is about 45 inches tall. This last piece of information more strongly suggests that this user is, in fact, a child. However, this is only an inference; the application does not know the user is a child with certainty. Would this inference be strong enough to constitute actual knowledge under the Commission's interpretation of COPPA?

As these examples indicate, with the rise of large data sets and sophisticated data analytics, the question of when a general audience site or service has actual knowledge that it is collecting information from children has become difficult to answer. FPF asks the FTC to issue guidance or create FAQs to address the question: when, if ever, does an inference regarding a user's age give rise to actual knowledge? This sort of guidance would be consistent with past FTC activities; the Commission has provided guidance regarding a range of COPPA-related issues, including enumerating factors the FTC considers when determining whether content is child-directed.

3. Education: COPPA should be Aligned with FERPA

While FERPA's requirements for school relationships with education technology (edtech) providers are fairly clear under the school official exception[40], the requirements of COPPA when edtech providers collect students' personal information from schools are not. Schools need to know when they may exclusively exercise COPPA's rights regarding the access and deletion of children's data.

COPPA is also not as clear as FERPA about how schools may provide consent for the use of edtech in schools for children under thirteen. While FTC's FAQ on COPPA says that "schools may act as the parent's agent and can consent to the collection of kids' information on the parent's behalf,"[41] this statement could be interpreted either as similar to FERPA's school official exception or as a requirement that since schools act as "the parent's agent," actively seeking parental consent before the school can consent to an edtech tool's collection of student data.

In some situations, parental consent is desirable. Under FERPA, for example, parents are given the right to opt out of sharing "directory information."[42] Unless a parent opts out, this exception allows schools to share certain information as administrators deem appropriate, for things such as announcing the names of students on the football team, in the school yearbook, in play programs, or on a public honor role. Directory information is also often disclosed to companies that provide school pictures or class memorabilia such as class rings. Because the sharing of this information is not necessary to essential school functions, schools give parents an annual notice about directory information[43] and an opportunity to opt out of its sharing.

Similarly, if COPPA is interpreted to allow schools, without obtaining parental consent, to share students' personal information with edtech providers, this should be, as Section M describes, "limited to the educational context" and defined as "where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose."

It would be useful for the FTC to provide specificity regarding the meanings of "educational context" and "commercial purpose." This clarification does not have to be an exhaustive list but can simply describe characteristics that clearly place the use or action of an edtech company product into either the educational or the commercial context.

When COPPA allows a school to consent to the use of an edtech product without receiving explicit parental consent, it is important that the school also receives the COPPA rights that

---

[40] 20 U.S.C. 1232g §§ (b)(1)(A).
[41] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions ("The [COPPA] Rule does not require operators to ask the age of visitors").
[42] 20 U.S.C. 1232g §§ (a)(5)(B).
[43] *Id.*

allow educators to ensure control and access to that information. This includes the right to review and request deletion of students' data. While some groups may argue that parents should be given these rights instead, the practical effect of applying COPPA in that way could allow parents to delete their children's test scores or homework grades if they do not like the results, thereby undermining the educational system's ability to engage in everyday activites, like managing and assessing students. Ensuring that these parental rights as described under COPPA carry over to the school would firmly align the statute with FERPA.

However, the transferring of these COPPA rights to schools means that educators must be conscious of their responsibilities, most of which already exist under FERPA, and establish policies and practices to ensure that student information is not retained indefinitely. Especially for the children whom COPPA covers, inaccurate or no-longer-accurate information should be deleted when it is no longer needed for its original purpose.

To aid schools, edtech providers should provide clear, easy-to-understand information about which data they have collected, how it will be used, and how it will be protected. As a best practice, schools should have this information available to parents in a public place, such as on the district's website (this sort of disclosure is already required under many state laws).

Recommendations

We recommend that the FTC:

1) Codify the Commission's non-enforcement policy for operators that do not obtain verifiable parental consent before collecting an audio file of a child's voice when the file is collected solely to perform a verbal instruction or request and is deleted immediately after purpose fulfillment;
2) Issue guidance regarding COPPA's "actual knowledge" as it relates to emerging use cases, given the rise of large data sets and the internet of things; and
3) Clarify the circumstances in which schools may exclusively exercise COPPA's rights regarding the access and deletion of children's data.

FPF welcomes the opportunity to further discuss these recommendations and is happy to provide additional details or action steps.