**Before the**
**Federal Trade Commission**
**Washington, D.C. 20580**

| | | |
|---|---|---|
| **In the Matter of** | ) | |
| | ) | **Docket No. FTC-2019-0054** |
| **Implementation of the Children's** | ) | **Project No. P195404** |
| **Online Privacy Protection Rule** | ) | |
| | ) | |

**Comments of**
**Center for Democracy & Technology**

The Center for Democracy & Technology (CDT) respectfully submits these comments regarding the Federal Trade Commission (FTC)'s current inquiry into the scope and application of the Children's Online Privacy Protection Rule (COPPA Rule). CDT is a non-profit public interest advocacy organization that fights for fundamental rights and civil liberties in internet and technology law and policy. For over twenty-five years, CDT has advocated for individuals' rights to privacy and freedom of expression online, including in the original debates about children's privacy and online safety that led to the adoption of the Children's Online Privacy Protection Act (COPPA) in 1998.[1]

As the ecosystem of websites and online services has grown more complex over the years, so too has the challenge of enforcing the COPPA Rule. As the Commission looks again at revising the COPPA Rule to account for changes in the online environment affecting children, we urge the Commission to harmonize the Rule as much as possible with other privacy frameworks, and consider whether there is a clearer and more privacy-protective way to align COPPA and the Federal Education Rights and Privacy Act (FERPA) when technology is used in schools. We also urge the Commission to re-examine how the COPPA Rule applies to operators of user-generated content services, and to creators of that content, to ensure that the COPPA Rule does not inadvertently suppress the creation of child-directed or adult-oriented speech.

## I. Amendments to the COPPA Rule should harmonize the requirements between children's data and the larger data ecosystem.

*5. Does the Rule overlap or conflict with any other federal, state, or local government laws or regulations? How should these overlaps or conflicts be resolved, consistent with the Act's requirements?*

[1] *See, e.g.*, Written testimony of Deirdre Mulligan, CDT, before the Subcomm. on Commerce, Comm. on Commerce, Sci. & Transp., U.S. Senate (Sep. 23, 1998), https://cdt.org/insights/testimony-of-deirdre-mulligan-before-the-senate-committee-on-commerce-science-and-transportation-subcommittee-on-communications/.

The Commission's inquiry comes while reforms to the larger ecosystem are percolating in the states and in Congress.[2] Ideally, this unprecedented support for meaningful privacy protections will culminate in a single federal standard for commercial data privacy and security. It's crucial that any amendments to the COPPA Rule[3] are consistent with or subsumed by these larger reform efforts. While we do not discuss all areas of conflict in current law in this comment, we do note there are consistent themes and legal trends emerging and that any amendments made should align with them where appropriate.

Expansive definitions. New state laws and pending legislation at the state and federal level generally adopt the FTC's definition of personal information or something very similar, which focuses on all data that is linked or linkable to a person or a device.[4] It reflects the modern ecosystem where all data can be revealing and diverges from the inclusive list approach from previous generations of privacy laws. In addition to their expansive nature, many of these proposals also recognize that some data sets are more sensitive and therefore deserve greater protections. As a result, many new proposals tier out what rights or obligations are due based on sensitivity, which ensures that no meaningful data falls outside the regime altogether while acknowledging that some types of information pose greater privacy and security risks than others. Future amendments to COPPA should be just as broad and mirror this approach instead of leaving any data outside the regulation altogether.

Clear exceptions. Recent trends include two types of exceptions to the regulation of personal information: exceptions for data that has been "de-identified" and data that is necessary for the normal operations of a service, such as securing networks, auditing services, and more.[5] COPPA includes the same principles,[6] but ideally, a comprehensive privacy law will provide a consistent definition for these terms that can apply across different types of businesses and data sets. As we discuss in the educational context below, de-identification is complicated, and as more data becomes easily accessible to commercial actors, doing it right will become increasingly difficult. It is an especially important definition to get right, and we encourage the FTC to focus not only on the statutory definition but also on practical evaluation and guidance of de-identification processes to ensure they don't become a loophole.

---

[2] National Conference of State Legislators, Consumer Data Privacy Legislation, at http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx (compiling 25 major privacy bills in state legislatures in the 2019 session).
[3] 16 C.F.R. §312, https://www.ecfr.gov/cgi-bin/text-idx?SID=4fc843f3ae6c2fd4189912b8538fd9c2&mc=true&node=pt16.1.312&rgn=div5#se16.1.312_12.
[4] Staff of S. Commerce Comm. Chairman Wicker, Staff Discussion Draft (2019) *available at:* https://aboutblaw.com/NaZ; Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (comprehensive privacy legislation sponsored by Sen. Cantwell and three other Senators); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (comprehensive privacy legislation sponsored by Sen. Markey); Online Privacy Act, H.R. 4978, 116th Cong. (2019) (comprehensive privacy legislation sponsored by Reps Eshoo and Lofgren).
[5] *Id*.
[6] 16 C.F.R. §312.2 (definition of *Support for the internal operations of the Web site or online service*).

User controls. COPPA already includes user access and deletion rights, but emerging notions of individual control include broader rights to access, correct, delete, and port personal information.[7] Such proposals are not unlimited, but may in effect offer more protection to adults acting on their own behalf than adults protecting their children's data if COPPA is not aligned with the ultimate federal standard.

Data use limitations. Notice, consent, and transparency will always be a major pillar of U.S. privacy laws, but decision makers are increasingly proposing limitations on data use that cut across different opt-in or opt-out models. Proposals include generic minimization requirements, data fiduciary responsibilities, risk assessments, prohibitions on secondary uses, and more.[8] While this area is subject to more debate than other components of a comprehensive privacy law, it is likely to be addressed in some form, and COPPA should eventually mirror protections offered to adults.

This is not an exhaustive list but reflects some of the divergence between COPPA and more recent privacy laws and proposals. While COPPA regulations were updated only six years ago, privacy values are evolving at an astonishing pace and it may be that state and federal regulations outpace the protections in COPPA if they are not harmonized. Of course, children will always receive special protections in some form – but aligning underlying definitions and legal structures can provide a major leap forward in privacy protections for children and adults.

**II. Adding an Exception to Parental Consent for EdTech Could Be Beneficial As Long As It Does Not Weaken Privacy Protections for Children**

*Question 23, . . . Should the Commission consider a specific exception to parental consent for the use of education technology used in the schools? Should this exception have similar requirements to the "school official exception" found in the Family Educational Rights and Privacy Act ("FERPA"), and as described in Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices? If the Commission were to amend the COPPA Rule to include such an exception: a. Should the Rule specify who at the school can provide consent?*

[7] *See supra,* n. 4.

[8] Wicker, *supra* n. 4 (limiting collection, processing and transferring data in a way that is necessary, proportionate and limited, if not done with consent); Data Care Act, S. 2961, 116th Cong. (2019) (requiring a duty of loyalty that prohibits a covered entity from using data in any way that benefits itself to the detriment of a user and either (i) is reasonably foreseeable, or (ii) would be unexpected and highly offensive); Commercial Facial Recognition Privacy Act, S. 847, 116th Cong. (2019) (sponsored by Sens. Blunt and Schatz and prohibiting the use of facial recognition data for any purpose besides that which a subject is notified of and consented to); Privacy Bill of Rights Act, *supra* note 3 (sponsored by Sen. Schatz and 16 other senators requiring the FTC to write regulations to prevent "collecting information of an individual beyond what is adequate, relevant, and necessary for (A) the performance of a contract to which the individual is a party, (B) to provide a requested product or service, or (C) to take steps at the request of the individual prior to entering into a contract to which the individual is a party.")

We commend the FTC for trying to be more proactive in protecting children's privacy by reviewing the amendments made to COPPA in 2013 and seeking to provide clarity around how COPPA applies in the school context, including how it intersects FERPA.[9] In August 2018, in response to the FTC's request for public comments on "Competition and Consumer Protection in the 21st Century," CDT filed comments[10] suggesting the following actions to maximize the effectiveness of the FTC's rulemaking authority related to COPPA:

- Continue to work with the U.S. Department of Education to provide guidance;
- Proactively investigate companies;
- Strengthen communications and outreach when the FTC takes enforcement actions; and
- Provide ongoing monitoring, training, and evaluation to Safe Harbor organizations.

CDT appreciates that the FTC is considering adding an explicit exception to a parental consent requirement for the use of education technology in schools to address potential confusion among schools. The Statement of Basis and Purpose to the 1999 COPPA rule noted that it "[did] 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[11]," making it seem like schools would be allowed to consent on behalf of parents for the collection of children's information for educational purposes. However, in section M.2 of the FTC's FAQ[12] on "Complying with COPPA", it says "operators can presume that the school's authorization for the collection of students' personal information is based upon the school having obtained the parents' consent." This might cause confusion for schools, which could take this to mean that they can consent for the operator's collection of children's information *only after* having obtained it first from the parents themselves, even when the operator limits use of the child's information to the educational context.

If it is in fact the Commission's intention to require schools to collect parental consent for each individual use of an educational technology product, it is important to note that this would be burdensome for schools, undermine their decision-making authority, and not effectively protect student privacy. Some schools do not have the resources or the time to ask for consent from parents every time they rely on an educational technology product, just as they do not ask for consent from parents around the curriculum that is used or other instructional and operational decisions that a school makes in the course of educating students. Schools are responsible for a number of functions like transportation, state and federal reporting, meal services, and most

---

[9] 34 C.F.R. § 99. Retrieved from: https://www.ecfr.gov/cgi-bin/text-idx?SID=55628b44d69471c698b27b1dae87294a&mc=true&node=pt34.1.99&rgn=div5.

[10] CDT, Comments to Federal Trade Commission re: Competition and Consumer Privacy in the 21st Century (August 20, 2018), https://cdt.org/files/2018/08/CDT-FTC-comments-5-8-20-18.pdf

[11] Federal Trade Commission, Statement of Basis and Purpose pursuant to COPPA (1999), https://www.occ.treas.gov/news-issuances/federal-register/64fr59887.pdf

[12] Federal Trade Commission, Complying with COPPA: Frequently Asked Questions (March 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools.

importantly, delivering high-quality instruction. Education data and technology may be required to support some of this important work, so they need to be able to responsibly and ethically use data and technology in support of these efforts. Per FERPA and other state laws, they are already regulated and responsible for meeting privacy and security standards.

In addition to introducing additional burdens and undermining decision-making, expanding COPPA's reliance on parental consent is an outdated model of notice and consent that puts the onus on consumers (parents/schools). CDT has long advocated[13] that a notice and consent model does not provide enough privacy protections and has offered a better model, as seen in CDT's draft federal consumer privacy bill[14], that moves away from the traditional notice and consent model and instead places guardrails around not just the collection of data but also its use cases. The draft bill—in addition to placing additional protections on certain types of sensitive data, like children's data and biometric data—would affect COPPA in that it would place additional restrictions on disclosure of children's information to third parties and on the use of children's information for targeted advertisement purposes[15].

If drafted properly, CDT could support an exception to a parental consent requirement to clarify that schools are not required to obtain parental consent for each third-party technology provider as long as the mechanism does not weaken the overall privacy protection afforded children. As such, any exception should align with and be as rigorous as the "school official" exception in FERPA, and should not permit the usage of students' personally identifiable information for non-educational purposes. In according a specific exception to parental consent for the use of educational technology in schools, the Commission would bring greater alignment between COPPA and FERPA and would reflect the needs and realities of the field, but this cannot come at the expense of weakening privacy protections for children. Furthermore, making sure that this exception is provided with at least the same use and re-disclosure limitations as with the current "school official exception" under FERPA,[16] if not stronger limitations, will ensure that the exception doesn't weaken the protections that are currently accorded under FERPA.

*a. Should the Rule specify who at the school can provide consent?*

The Rule should align with FERPA's "school official" exception and its definitions and requirements.

*b. Should operators be able to use the personal information collected from children to improve the product? Should operators be able to use the personal information collected from children to*

---

[13] Michelle Richardson, "Notice and Choice Are No Longer a Choice" (March 1, 2019), https://cdt.org/blog/notice-and-choice-are-no-longer-a-choice/.
[14] CDT, Federal Baseline Privacy Discussion Draft (December 5, 2018), https://cdt.org/files/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.
[15] Elizabeth Laird, "CDT's Consumer Privacy Legislation and What It Means for the Education Sector" (January 24, 2019), https://cdt.org/blog/cdts-consumer-privacy-legislation-and-what-it-means-for-the-education-sector/.
[16] 34 C.F.R. § 99.31 (a).

*improve other educational or non-educational products? Should de-identification of the personal information be required for such uses? Is de-identification of such personal information effective at preventing re-identification? What kinds of specific technical, administrative, operational or other procedural safeguards have proved effective at preventing re-identification of deidentified data? Are there instances in which de-identified information has been sold or hacked and then re-identified? ...*

Currently under FERPA, student information that has been de-identified is not protected and thus is not subject to FERPA's use and re-disclosure limitations. To meet the definition of de-identification in FERPA, education entities must remove enough student information such that "a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information[17]." However, this is more complicated than it might seem. For example, approaches to de-identification can range from simply deleting direct identifiers like student name or ID number (which is typically not sufficient to prevent the data from being re-identified) up to more sophisticated techniques like shuffling or adding noise to the data that make recovery more difficult (these more complex approaches are generally referred to as "anonymization" in computer science).

In reality, it is very difficult to properly de-identify any information with an absolute certainty that it will never be re-identified, as is evident from the examples below.

- New York City officials, for example, accidentally revealed the detailed comings and goings of individual taxi drivers in a case of a public release of data that was poorly de-identified but just a handful of random location data points are uniquely identifiable 95 percent of the time.[18]
- In 2016, the Australian government released an anonymized dataset of medical billing records, including prescriptions and surgeries. Researchers quickly noted "the surprising ease with which de-identification can fail" when additional datasets are cross-referenced.[19]
- Looking at 200 tweets, researchers were able to use associated metadata like timestamps, number of followers, and account creation time to identify anyone in a group of 10,000 Twitter users 96.7 percent of the time[20]. Even when muddling the metadata, a single person could still be identified with more than 95 percent accuracy.

Current methods of de-identification are largely ineffective at preventing re-identification, as is evident from the examples above, so the Commission needs to ensure that the use of

---

[17] 34 C.F.R. § 99.31 (b).
[18] Dan Goodin, "Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts" (June 23, 2014), https://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/.
[19] Chris Culnane, Benjamin I. P. Rubinstein, Vanessa Teague, Health Data in an Open World (December 15, 2017)(finding that de-identified patient data can be re-identified), https://arxiv.org/abs/1712.05627.
[20] Chris Stokel-Walker, "Twitter's vast metadata haul is a privacy nightmare for users" (July 9, 2018), https://www.wired.co.uk/article/twitter-metadata-user-privacy.

de-identification does not offer a loophole for companies to retain and use data for non-educational purposes without school permission or parental consent.

*c. Should parents be able to request deletion of personal information collected by operators under such an exception?*

Parents should not be granted a blanket authorization to request deletion of personal information collected by operators under such an exception. Currently under COPPA, parents have the right to, at any point, refuse to permit the operator's further use or future collection of personal information from their child, and to direct the operator to delete the child's personal information.[21]

When it comes to the use of education technology in classrooms, however, there is potential for this provision to cause complications. Schools use information in student records for a variety of reasons: providing services to students, auditing or evaluating federal or state-supported education programs, or enforcing or complying with federal legal requirements that relate to those programs.[22] Parents requesting deletion of personal information from their children's records might inadvertently impede on the school's day-to-day responsibility. Additionally, a parent might ask to delete their child's information (e.g. a test result or grade) if they did not like the result, undermining the educational system.

When a school is allowed under COPPA to consent to a child's use of an educational technology product without receiving explicit parental consent, it is important that it is the school that also receives the COPPA rights that allow them to ensure control and access to that information. This includes the right to review and request deletion of that student data. Ensuring that these parental rights, as described under COPPA, carry over to the school would firmly align the statute with FERPA, where the entities that the school determines to be school officials are "under the direct control of the agency or institution with respect to the use and maintenance of education records."[23]

However, to keep in line with FERPA, parents should be allowed to request amendments of children's records through the schools if they believe the "education records relating to the student contain information that is inaccurate, misleading, or in violation of the student's right to privacy."[24] This would ensure it is the schools that have control on the collection, use, and sharing of data, while also enabling that parents can verify that the records don't contain incorrect or misleading information that might negatively affect the student.

*d. Should an operator require the school to notify the parent of the operator's information practices and, if so, how should the school provide such notice?*

---

[21] 16 C.F.R. § 312.6 (a)(2).
[22] 34 C.F.R. §§ 99.35 (a)(1), 99.38, 99.39.
[23] 34 C.F.R. § 99.31 (a)(1)(i)(B)(2).
[24] 34 C.F.R. §§ 99.10, 99.12, 99.20, 99.21, 99.22.

Transparency and proactive communication are effective practices to educate and engage parents, so schools should notify parents of the operator's information practices. Schools should provide this information in language that is easy to understand and in multiple languages to accommodate all families. This notification could be brought into alignment with FERPA, as schools already are required to send annual notification to parents informing them of their rights with respect to the student records, along with other information including the school's specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.

*e. Should such an exception result in a preemption of state laws? If so, would that result negatively affect children's privacy?*

The exception should not result in a preemption of state laws at this time. State student privacy laws are not new. The education sector has already experienced a significant proliferation of state student privacy laws. According to the Data Quality Campaign's new report,[25] since 2013, every state has introduced a bill expressly addressing the privacy and security of education data, and 45 states have enacted 168 laws related to student data privacy. Many of these laws are more rigorous and have supplemented FERPA and COPPA with higher privacy and security standards. Until there is a federal law that is as privacy-protective as the state laws, an overbroad preemption of state laws would negatively affect students' privacy.

**III. User-generated content services present distinct challenges for the COPPA framework**

*Question 25, Concerning COPPA's application to user-generated content services*

The FTC is right to focus on providing clarity to operators of general-audience user-generated content (UGC) sites about their potential liability under COPPA when users upload child-directed content. Clarity is crucial to operators that may be covered by COPPA: In order to establish appropriate verified parental consent mechanisms and avoid the risk of fines, operators must know whether they are required to treat user data according to the requirements of the COPPA Rule well in advance of interacting with users of their service. Operators of websites featuring primarily first-party content (content created by the website operator itself) are themselves essentially in control of whether their service is directed to children. They select the subject matter, photos, music, activities, and other content on the service, and can refer to FTC guidance to understand the boundaries of the child-directed definition.

[25] Data Quality Campaign, Education Data Legislation Review (October 2019), https://2pido73em67o3eytaq1cp8au-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/DQC-2019-Education-Data-Legislation-Review.pdf.

Operators of UGC services, on the other hand, are not in full control of the content that appears on their services. UGC hosts are not able to manually review every file posted to their service before it goes live, nor are filters able to accurately detect the presence of "child-directed" content.[26] Thus, there will be an inherent level of uncertainty for general-audience UGC site operators as to whether they are hosting child-directed content at all. These operators will face another level of uncertainty as to whether child-directed content is present on any portions of the site in a great enough extent to create an obligation to obtain verified parental consent for any personal information collected from users who view or interact with that content. Incidental hosting of child-directed content on a general-audience UGC site does not transform the site as a whole into a child-directed site, and the Commission should provide greater clarity to operators about when "a portion" of their general-audience site will be considered child-directed due to the presence of child-directed UGC. General-audience UGC site operators will likely not, by default, have systems in place for obtaining verified parental consent, given their intent to run a general-audience UGC site, the expense of establishing such systems, and the uncertainty over whether such systems will be needed.

Regarding the question of creating a rebuttable presumption that users on child-directed portions of general-audience sites are children, the Commission must be cautious that any incentive or "encouragement" it creates for content hosts to identify child-directed UGC does not become functionally equivalent to a mandate. A legal regime that requires operators to review, either manually or automatically, all content uploaded to their service and affix a label of "child-directed" or "not child-directed" would run afoul of the First Amendment.[27] The Commission should not require or encourage proactive filtering of UGC—that is, of internet users' speech—as a component of allowing an operator to rebut the presumption that all users on a child-directed portion of a general-audience UGC site are children.

The Commission should also ensure that the statutory focus of COPPA—to protect the privacy of children's personal information—does not become a pretext for content regulation. In question 25(e), the Commission asks, "In considering whether to permit general audience sites to rebut the presumption, should the Commission consider costs and benefits unrelated to privacy, such as whether children may be exposed to age-inappropriate content if they are treated as an adult?" The answer is simple: No. The Commission does not have the authority under the COPPA statute to make determinations about the "age-appropriateness" of speech and it should not warp the COPPA Rule to do so. The Commission should recall that all content-rating systems in the United States that evaluate the age-appropriateness of various

[26] For discussions of the limitations of various filtering tools, see Natasha Duarte, Emma Llansó, Anna Loup, *Mixed Messages: The Limits of Automated Social Media Content Analysis* (November 2017) https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf; Evan Engstrom and Nick Feamster, *The Limits of Filtering: A Look at the Functionality and Shortcomings of Content Detection Tools* (March 2017), https://www.engine.is/the-limits-of-filtering/.
[27] Brown v. Entm't Merchs. Assn., 564 U.S. 786 (2011).

forms of media are run by private industry self-regulatory bodies or other private organizations.[28] The Commission should not undermine the legitimacy of COPPA as a privacy-protection law by using it to exert content regulation pressure on operators of UGC services or the speech that they host.

*Question 11, Concerning the definitions of "operator" and "website or online service directed to children"*

Finally, we also raise concerns with the application of COPPA directly to creators of user-generated content that the Commission determines to be directed to children. The Commission's recent FAQ, "YouTube channel owners: Is your content directed to children?", explains the Commission's rationale for treating individual content creators as operators under the COPPA Rule: A "channel" or sub-page of YouTube is considered a "website or online service", and the content creator, i.e. the user who runs the channel, is considered the "operator" of that part of YouTube.[29] If the user-operator uploads content directed to children, that user-operator may be held liable for children's personal information that the user-operator collects directly, or that is collected "on behalf" of the user-operator.[30] The Commission specifies that this would include an advertising network that runs on the channel and that collects a persistent identifier from viewers in order to serve interest-based ads.

This interpretation of the COPPA Rule will not be obvious to individuals who are creating and uploading content to websites owned and operated by companies over which they have no meaningful control. For example, while user-operators have some control over channel settings on YouTube, the fundamental decisions about data collection and use that will affect their viewers' personal information are made by YouTube, *not* by the user-operator herself. A user-operator of a YouTube channel has a limited set of choices, for example, around advertising on her channel: run no ads, run contextual ads, or run interest-based ads provided by Google. The user-operator has neither controls for nor access to, in any meaningful way, any of the information collected by Google's interest-based advertising service. While the user-operator of a channel may "benefit"[31] from advertising revenue generated by interest-based advertising, it may nevertheless be surprising to her that the payment she receives from YouTube ads transforms her into the operator of a website directed to children that is responsible for YouTube/Google's collection of users' personal information.

---

[28] *See, e.g.,* Entertainment Software Ratings Board, https://www.esrb.org/about/; Motion Picture Association, https://www.motionpictures.org/who-we-are/; Common Sense Media, https://www.commonsensemedia.org/about-us/our-mission.

[29] Kristin Cohen, "YouTube channel owners: Is your content directed to children?", 22 November 2019, https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children ("YouTube FAQ"). Presumably the Commission also still considers YouTube to be an operator of every channel hosted on youtube.com.

[30] The COPPA Rule specifies that personal information "is *collected or maintained on behalf of an operator when:* … (2) The operator benefits by allowing another person to collect personal information directly from users of such Web site or online service." 16 C.F.R. § 312.2, *supra* n.3.

[31] *Id*.

Moreover, while the Commission advises that "[o]nce COPPA applies, the operator must provide notice, obtain verifiable parental consent, and meet COPPA's other requirements,"[32] the Commission must recognize that most users of UGC sites and services have no functional way to comply with COPPA's requirements themselves, independent of the underlying site/service. The user-operator of a child-directed YouTube channel, for example, has no mechanism for obtaining verified parental consent directly from parents of children who view her channel. The user-operator only has the compliance choices provided to her by YouTube, which currently amount to turning off all interactive functionality and disabling interest-based advertising. Any process for obtaining verified parental consent will be conducted by YouTube, and the Commission should not penalize UGC creators for something that is out of their control.

These definitional challenges point to a fundamental tension with the effort to apply COPPA's "directed to children" standard to UGC websites: the individual user/content creator is responsible for the nature of the content and whether it is child-directed, while the operator of the general-audience UGC site is responsible for the data collection, use, and consent practices that affect other users' personal information. Prior to the YouTube settlement, the COPPA Rule has typically been enforced in circumstances where either a) the website operator had actual knowledge that users were under 13, or b) the creator of the child-directed content and website operator were the same entity.[33] Enforcing COPPA appropriately on UGC websites is a complex task, and the Commission should take the opportunity in this Rule review to examine in depth the consequences of COPPA for the vast array of UGC sites and services. The Commission must ensure that the Rule's application to UGC sites—and to the people who use these sites as platforms for their speech—is clear, fair, and enables the creation and hosting of content intended for children and adults alike.

Respectfully submitted,

Michelle Richardson
Elizabeth Laird
Emma J. Llansó

Center for Democracy & Technology
1401 K St NW, Suite 200
Washington, DC 20010

11 December 2019

[32] YouTube FAQ, *supra* n.29.
[33] *See* Privo, History of COPPA Violations, https://www.privo.com/history-of-coppa-violations.