SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ the Urban Justice Center:
40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

November 25, 2019

The Honorable Joseph J. Simons
Chairman, Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The Honorable Rebecca Kelly Slaughter
Commissioner, Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The Honorable Rohit Chopra
Commissioner, Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The Honorable Christina S. Wilson
Commissioner, Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The Honorable Noah Joshua Phillips
Commissioner, Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: COPPA Rule Review, 16 C.F.R. Part 312, Project No. P195404 (the "Proposed Rule")

Dear Chairman Simons, Commissioner Chopra, Commissioner Phillips, Commissioner Slaughter, and Commissioner Wilson:

The Surveillance Technology Oversight Project, Inc. ("S.T.O.P."), is a non-profit legal services provider and advocacy organization that fights for privacy and civil rights. We write to oppose the Proposed Rule and any modification of the Children's Online Privacy Protection Act ("COPPA") Rule that weakens parental consent requirements for education technology.[1] Should the Federal Trade Commission (the "Commission") create such an exception, we urge that it be as narrowly tailored as possible.

Congress enacted COPPA to protect children and give parents, not school officials, control over the online collection and misuse of their children's data.[2] Rather than being protective of student

[1] *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 Fed. Reg. 35842, 35845 (July 25, 2019) [hereinafter Request for Public Comment].
[2] *Complying with COPPA: Frequently Asked Questions*, Fed. Trade Comm'n, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions (last updated Mar. 20, 2015); *see also* Noah Joshua Phillips, U.S. Fed. Trade Comm'n, The Future of the COPPA Rule FTC Staff Workshop 1–2 (2019) (citing 144 Cong. Rec. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan)), https://www.ftc.gov/system/files/documents/public_statements/1547700/phillips_-_coppa_workshop_remarks_10-7-19.pdf; Christine S. Wilson, U.S. Fed. Trade Comm'n, Opening Remarks at FTC Workshop: The Future of the

privacy, many school officials are their students' single biggest privacy threat. Whether through spyware that monitors internet activity[3] or hardware exploits that activate students' webcams,[4] school officials have frequently abused their authority to undermine students' privacy and digital safety both at school and in their own homes. Disturbingly, it is these very same school officials that the Proposed Rule would empower to supplant parents in controlling children's digital privacy rights.

Time and again, school officials have sacrificed student privacy for minimal gains, and sometimes without any benefit whatsoever. For example, many schools have deployed facial recognition technology to indiscriminately track who is on school premises and where.[5] But this technology is notoriously inaccurate for people of color, female-presenting individuals, non-binary individuals, and—most importantly in schools—young people.[6] When these factors are combined in a single individual, the accuracy rate further plummets. Accordingly, any claimed benefit from this invasive tracking is miniscule when compared to its privacy and error costs. Another example is school officials' unlawful searches of students' cell phones. In 2013, a Virginia school administrator searched a student's cell phone after "finding evidence of drug use on the school bus earlier that day," with no explanation of how the search would help, but "the cell phone could not have contained drugs."[7] Searching students' cell phones is particularly invasive because—as the Supreme Court recognized—cell phones "could just as easily be called cameras, video players, rolodexes,

---

COPPA Rule 2, 4 (2019), https://www.ftc.gov/system/files/documents/public_statements/1547693/wilson_-_ftc_coppa_workshop_opening_remarks_10-7-19.pdf.

[3] *See* Lois Beckett, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, Guardian (Oct. 22, 2019, 1:00 AM), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle (noting schools monitor online student activity "whether students are in their classrooms or bedrooms," not just including their "official school email accounts, chats or documents," but also their "web searches and internet usage"); Faiza Patel et al., *School Surveillance Zone*, Brennan Ctr. for Justice (Apr. 30, 2019), https://www.brennancenter.org/our-work/research-reports/school-surveillance-zone; *see also* Caroline Haskins, *Gaggle Knows Everything About Teens and Kids in School*, Buzzfeed News (Nov. 1, 2019, 3:48 PM), https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education.

[4] *See, e.g.*, Jesus Diaz, *School Spies Students Through Their Laptop Cameras*, Gizmodo (Feb. 18, 2010, 9:10 AM), https://gizmodo.com/school-spies-students-through-their-laptop-cameras-5474614.

[5] *See* Sidney Fussell, *Schools Are Spending Millions on High-Tech Surveillance of Kids*, Gizmodo (Mar. 16, 2018, 4:25 PM), https://gizmodo.com/schools-are-spending-millions-on-high-tech-surveillance-1823811050; Sarah St. Vincent, *Facial Recognition Technology in US Schools Threatens Rights*, Human Rights Watch (June 21, 2019, 12:30 PM), https://www.hrw.org/news/2019/06/21/facial-recognition-technology-us-schools-threatens-rights; Emily Tate, *With Safety in Mind, Schools Turn to Facial Recognition Technology. But at What Cost?*, EdSurge (Jan. 31, 2019), https://www.edsurge.com/news/2019-01-31-with-safety-in-mind-schools-turn-to-facial-recognition-technology-but-at-what-cost.

[6] Stefanie Coyle & John Curr III, *New York School District Seeks Facial Recognition Cameras for Public Schools*, ACLU (June 20, 2018, 4:15 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/new-york-school-district-seeks-facial-recognition; *Face Recognition*, Elec. Frontier Found., https://www.eff.org/pages/face-recognition (last visited Oct. 31, 2019).

[7] *Gallimore v. Henrico Cty. Sch. Bd.*, 38 F. Supp. 3d 721, 725 (E.D. Va. 2014); *see also G.C. v. Owensboro Pub. Sch.*, 711 F.3d 623, 633–34 (6th Cir. 2013) (holding search of student's cell phone based on "general background knowledge" he abused drugs and was depressed and because he violated school policy by using the phone in class unjustified at inception); *Klump v. Nazareth Area Sch. Dist.*, 425 F. Supp. 2d 622, 640–41 (E.D. Pa. 2006) (holding seizure of student's cell phone justified because he violated school policy by using it during school hours, but using student's cell phone to call other students to determine whether they were also using phones was not justified).

calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[8] "With all they contain and all they may reveal, [cell phones] hold for many Americans 'the privacies of life.'"[9]

School officials also trade away student privacy outside the digital arena. Despite the Fourth Amendment's prohibition on searches that intrude on student privacy more than is necessary to achieve the search's purpose,[10] school officials regularly go much further. Administrators not only authorize, but even participate in, unnecessary strip searches of students.[11] They authorize searches of students' persons, lockers, and property with metal detectors and drug-sniffing dogs, all without reasonably individualized suspicion, let alone probable cause, of wrongdoing.[12] They increasingly rely on police to maintain discipline,[13] leading to students' arrests for "infractions that pose little or no safety concerns."[14] These practices not only fail to reduce school crime,[15] but, in some cases, they make schools less safe.[16] Students suffer twice: they not only lose their privacy, but they face increased public safety threats as a result.[17]

Educators' historic disregard for student privacy is so expansive that Congress imposed heightened privacy protections from schools in the form of the Family Education Rights and Privacy Act ("FERPA").[18] FERPA protects students' privacy by requiring schools to notify parents and/or obtain their consent before disclosing certain personal information about students.[19] FERPA also requires districts to have direct control of student information after it is disclosed to third-party service providers.[20] However, school administrators already fail to comply with FERPA for

---

[8] *Riley v. California*, 573 U.S. 373, 393 (2014).
[9] *Id.* at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).
[10] *See Safford Unified Sch. Dist. No. 1 v. Redding*, 557 U.S. 364, 375 (2009).
[11] *See, e.g.*, *Redding*, 557 U.S. at 374–77, 379 ("[W]hat was missing from the suspected facts that pointed to Savana was . . . any reason to suppose that Savana was carrying pills in her underwear. . . . The strip search of Savana Redding was unreasonable and a violation of the Fourth Amendment . . . ."); *see also* Erik Ortiz, *Four Girls at N.Y. Middle School Subjected to 'Dehumanizing' Strip Search, Lawsuit Says*, NBC News (Apr. 30, 2019, 5:30 PM), https://www.nbcnews.com/news/us-news/four-girls-n-y-middle-school-subjected-dehumanizing-strip-search-n1000321; Favian Quezada, *Crockett Police Investigating Improper Strip Search of Crockett ISD Students*, CBS 19 (Jan. 9, 2018, 8:47 PM), https://www.cbs19.tv/article/news/crockett-police-investigating-improper-strip-search-of-crockett-isd-students/501-506704123.
[12] Jason P. Nance, *Random, Suspicionless Searches of Students' Belongings: A Legal, Empirical, and Normative Analysis*, 84 U. Colo. L. Rev. 367, 369–70, 409 (2013); *see also, e.g.*, *Doe ex rel. Doe v. Little Rock Sch. Dist.*, 380 F.3d 349 (8th Cir. 2004); Brandon Addeo, *Ohio Statute Allows Schools to Search Students' Lockers*, Sandusky Register (Apr. 20, 2019, 10:43 AM), http://www.sanduskyregister.com/story/201904190027.
[13] *Policing Students*, 128 Harv. L. Rev. 1747, 1754 (2015).
[14] *Id.* at 1754–55.
[15] *See* Nance, *supra* note 12, at 371 & n.17 (collecting studies).
[16] *See id.* at 372 & n.18 (collecting studies).
[17] *Policing Students*, *supra* note 13, at 1756.
[18] Sen. James Buckley, Address Before the Legislative Conference of the National Congress of Parents and Teachers, March 12, 1975, 121 Cong. Rec. 13,990, 13,991 (1975) ("[M]y initiation of this legislation rests on my belief that the protection of individual privacy is essential to the continued existence of a free society. There has been clear evidence of frequent, even systematic violations of the privacy of students and parents by the schools through the unauthorized collection of sensitive personal information and the unauthorized, inappropriate release of personal data to various individuals and organizations.").
[19] *See* 20 U.S.C. § 1232g(a)(5)(B), (b)(2).
[20] *See* 34 C.F.R. § 99.31(a)(1)(i)(B).

education technology, particularly with respect to remotely hosted cloud services. Approximately 95% of school districts rely on cloud services,[21] but "many districts [do] not seem to understand the nature of the services that they [outsource] to third party providers,"[22] and thus are "weakly governed."[23] Indeed, despite FERPA's parental notice and consent requirements,[24] only 25% of school districts inform parents they use cloud services as required.[25] And notwithstanding FERPA's requirement that districts have direct control of student information in the hands of third-party service providers,[26] fewer than 7% of service agreements restrict vendors from selling or marketing the student information they collect.[27] In light of school administrators' lack of desire and ability to protect student privacy, the Commission should not grant schools further authority over children's privacy rights.

S.T.O.P. adamantly opposes the Propose Rule. However, insofar as the Commission creates an education technology exception, it should narrowly define which officials can provide consent.[28] As discussed above, Congress enacted COPPA to give parents more control over both the collection of data from their children on the Internet and how that data is subsequently used.[29] Since the Proposed Rule would deprive parents of the authority to control the collection of personal information from their children, the authority to consent should be limited to a small group of senior school administrators. Narrowing the grant would limit control to those most easily held accountable by parents. Additionally, learning from the widespread non-compliance with FERPA, the Commission should (1) require any authorized school official to be trained on student privacy and COPPA, and (2) require any school that chooses to use this authority to submit to periodic privacy audits.

Furthermore, the Proposed Rule should prevent any gratuitous abrogation of student privacy, including by limiting school officials' authority to consent to narrowly defined educational purposes.[30] Schools must particularly identify how student data collection enhances the learning experience.

Additionally, budget pressures[31] incentivize schools to consent to more invasive data collection in exchange for preferential pricing. The Proposed Rule must prohibit the direct or indirect

---

[21] Joel R. Reidenberg et al., Ctr. on Law & Info. Policy at Fordham Law Sch., Privacy and Cloud Computing in Public Schools 19 (2013), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip.
[22] *Id.* at 24.
[23] *Id.* at Executive Summary.
[24] *See* 20 U.S.C. § 1232g(a)(5)(B), (b)(2).
[25] Reidenberg et al., *supra* note 21, at Executive Summary.
[26] *See* 34 C.F.R. § 99.31(a)(1)(i)(B).
[27] Reidenberg et al., *supra* note 21, at Executive Summary.
[28] *See generally* Request for Public Comment, 84 Fed. Reg. at 35845 (Questions 23(a)).
[29] *See Complying with COPPA: Frequently Asked Questions*, *supra* note 2; *see also* Phillips, *supra* note 2, at 1–2 (citing 144 Cong. Rec. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan)); Wilson, *supra* note 2, at 2, 4.
[30] *See generally* Request for Public Comment, 84 Fed. Reg. at 35845 (Questions 23(f)).
[31] *See, e.g.*, Michael Leachman, *New Census Data Show Persistent State School Funding Cuts*, Ctr. on Budget & Pol'y Priorities (May 22, 2018, 2:15 PM), https://www.cbpp.org/blog/new-census-data-show-persistent-state-school-funding-cuts.

monetization of student data, including via preferential pricing, by insulating those with consenting authority from purchasing decisions and prohibiting any express quid pro quo.

The Proposed Rule's mirroring of FERPA's "school official exception" raises additional concerns.[32] Under that exception, a school may disclose students' personally identifiable information ("PII") if (1) the recipient uses the disclosed records for authorized purposes, and (2) does not transmit such PII to a third party without express authorization.[33] Insofar as the Proposed Rule mirrors the school official exception, it should give parents the exclusive right to authorize third party transfers of PII. Education records may serve important purposes outside of school, such as for financial aid eligibility, but COPPA's definition of personal information is far more expansive than FERPA's definition of education records.[34] Therefore, schools have a more tenuous interest in permitting third-party disclosures of student's personal information.

The Proposed Rule must also prohibit operators from using students' personal information for marketing or product-improvement purposes.[35] Such commercialization of children's data could become common in educational technology and is the exact harm COPPA was enacted to protect against. This practice is controversial for adults,[36] but it is even more alarming for minors in a setting where they are stripped of agency. Children not only have a diminished understanding of how privacy invasions might harm them,[37] but they also lack control over what software and settings they use, working with the systems and tools school officials require them to use.[38]

Any student data that operators do collect must be aggregated in a manner that prevents re-identification of individual students.[39] Furthermore, parents should always retain the right to demand their children's data be deleted.[40] Once schools can consent to an operator's collection of students' personal information, data deletion would be parents' only remaining privacy remedy.

Furthermore, if the Commission weakens parents' exclusive control over students' personal information collection, the Proposed Rule should retain parental notice about operators' information practices.[41] At a minimum, parents should be put on notice as to how their children's

---

[32] *See generally* Request for Public Comment, 84 Fed. Reg. at 35485 (Question 23); *id.* at 35485 n.8.
[33] *See* Privacy Tech. Assistance Ctr., U.S. Dep't of Educ., *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* 4 (2014) (citing 34 C.F.R. § 99.31(a)(1)(i)), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.
[34] *See* 15 U.S.C. § 6501; 16 C.F.R. § 312.2.
[35] *See generally* Request for Public Comment, 84 Fed. Reg. at 35845 (Questions 23(b), (f)).
[36] *See* Rebecca Walker Reczek, *Targeted Ads Don't Just Make You More Likely to Buy—They Can Change How You Think About Yourself*, Harv. Bus. Rev. (Apr. 4, 2016), https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself.
[37] *See, e.g.*, Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59900 n.179 (Nov. 3, 1999).
[38] *See, e.g.*, *13 Steps to Shape & Secure Your 1:1 Chromebook Program*, Securly Blog (June 13, 2016), https://blog.securly.com/2016/06/13/13-steps-to-shape-secure-your-11-chromebook-program (recommending blocking students from installing applications and browser extensions).
[39] *See generally* Request for Public Comment, 84 Fed. Reg. at 35845 (Question 23(b)).
[40] *See generally id.* (Question 23(c)).
[41] *See generally id.* (Question 23(d)).

personal information is being shared. Any conceivable rationale for weakening COPPA's consent requirement—for example, "[using] data to support teachers, students, and parents"[42] or avoiding the administrative burden of tracking which students may use which technologies and complying with those permissions[43]—does not extend to undermining the notice requirement. Rather, parental notice would serve COPPA's purpose by enabling parents to provide feedback to school officials.[44]

The Proposed Rule also must not preempt the growing array of state privacy protections.[45] Federal laws and rules of this nature generally preempt state equivalents where there is an overwhelming need for uniformity across the country.[46] However, the Proposed Rule itself undercuts this rationale for federal preemption. That is, the Proposed Rule itself would require operators to comply with the consent given by individual schools,[47] which would result in multiple consent schemes. If vendors must navigate the web of discrete school policies, it poses little, if any, regulatory burden to also comply with a comparatively small number of local and state privacy statutes.

In sum, S.T.O.P. is adamantly opposed to the Proposed Rule and any weakening of COPPA's parental consent requirements for education technology. To the extent the Commission limits parents' control over their children's privacy in the education context, the Rule must narrowly circumscribe the situations in which parents lose such control or risk betraying the entire goal of COPPA's statutory scheme.

Thank you for the opportunity to submit this comment and for your consideration.

Respectfully submitted,

/s_____
Albert Fox Cahn
Executive Director
Surveillance Technology Oversight Project

---

[42] Phillips, *supra* note 2, at 5.
[43] *See, e.g.*, Lightspeed Systems, Comment Letter on Request for Public Comment (Oct. 25, 2019), https://www.regulations.gov/document?D=FTC-2019-0054-0281 (supporting the exception because it would be unreasonable "where potentially each student would have a different set of allowed apps"); Information, Communication & Technology Services, Cambridge Public Schools, Comment Letter on Request for Public Comment (Aug. 23, 2019), https://www.regulations.gov/document?D=FTC-2019-0054-0014 (same).
[44] *See supra* text accompanying notes 2, 29.
[45] *See generally* Request for Public Comment, 84 Fed. Reg. at 35845 (Question 23(e)).
[46] *See* Jay B. Sykes & Nicole Vanatko, Cong. Research Serv., R45825, *Federal Preemption: A Legal Primer* 1 (2019) ("Proponents of broad federal preemption often cite the benefits of uniform national regulations . . . .").
[47] *See* Request for Public Comment, 84 Fed. Reg. at 35845.