PARENT COALITION FOR STUDENT PRIVACY

www.studentprivacymatters.org
info@studentprivacymatters.org
@parents4privacy

124 Waverly Place
New York, NY 10011
303.204.1272

Nov. 21, 2022

Via online submission at: https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security#open-comment

To the Federal Trade Commission:

The Parent Coalition for Student Privacy is a non-partisan organization of parent and privacy activists from throughout the nation. We have authored and co-authored state report cards, parent toolkits, and position papers and reports, advocating for stronger data privacy protections for students at the local, state, and federal levels. Our organization has testified before Congress twice.[1]

In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA) to address the special privacy and safety of vulnerable children when using the Internet. Among the goals of the act included to "maintain the security of children's personal information collected online; and limit the online collection of personal information from children without parental consent."

The personal data of K12 students is widely recognized to be in need of special protection for many reasons: First, because children are especially vulnerable and their data especially valuable for the purposes of identity theft, and two, because in most cases, their use of ed tech programs that collect a wealth of personal data has been mandated by their schools, with no ability for students or their parents to opt out, or even notified as to their use.

And yet since the passage of COPPA, there has been an accelerated and unrestrained expansion of the use of digital programs and apps in schools. Most of these digital programs are operated and owned by for-profit companies and collect personal student data with or without parental consent, and without adequate oversight, restrictions, or security protections. As a results, the number of student data breaches has skyrocketed.

[1] Stickland, Rachael. "Testimony before the US House of Representatives House Committee on Education and the Workforce Hearing on Strengthening Education Research and Privacy Protections to Better Serve Students." March 22, 2016; https://edlabor.house.gov/imo/media/doc/Stickland_oraltestimony032216.pdf; and "Testimony Before the United States House of Representatives Committee on Education and the Workforce Subcommittee on Early Childhood, Elementary and Secondary Education Hearing on "Exploring Opportunities to Strengthen Education Research While Protecting Student Privacy," June 28, 2017. https://edlabor.house.gov/imo/media/doc/Strickland%20Testimony%206.28.17.pdf

Many of these programs have been the target of hackers and ransomware criminals. The education sector is now the number one target for malware and cybersecurity attacks, outranking the second most targeted sector, retail, and consumer goods, by nine to one.[2] During 2021, K12 Security Information Exchange cataloged a total of 166 cybersecurity incidents that were publicly reported, affecting schools in in 38 states – likely only a subset of the number that actually occurred.[3]

In September 2018, the FBI issued a Public Service Announcement, warning of the risks involved in the increased data collection by ed tech programs in schools, and that "[m]alicious use of this sensitive data could result in social engineering, bullying, tracking, identity theft, or other means for targeting children."[4]

It is not merely breaches that put student privacy at risk, whether the result the sloppy practices of schools and companies, the deliberate actions of hackers, or both. A recent study shows that staff at schools and districts have shared nearly five million posts on public Facebook pages that included identifiable images of their students, putting their privacy at risk. About 726,000 of these posts appeared to identify them by first and last name.[5] Clearly, this practice needs to stop.

At the same time, many parents report that their children are bombarded with advertisements while using school-assigned apps or programs, which commercialize their data and distract from and undermine the quality of education they receive.

A recent study found that 67 percent of mobile apps assigned to public school students by their schools secretly share their personal data with third parties through advertising and analytics software development kits (SDKs), including those provided for free by Google and Facebook.[6] On average, each school app was found to have more than ten third-party SDKs secretly embedded in their software, according to a 2021 study by the Me2B Alliance, now renamed Internet Safety Labs.[7]

About half (49%) of the apps shared student data with advertising platforms such as Google, as well as Facebook (14%). On average, the apps that shared data sent them to 10.6 different entities, while 18% sent data to very high-risk third parties – that is, entities that further share data with possibly hundreds or thousands of networked entities.

---

[2] https://districtadministration.com/the-education-industry-is-now-the-no-1-target-for-cyberattacks/

[3] State of K-12 Cybersecurity: Year in Review report at https://static1.squarespace.com/static/5e441b46adfb340b05008fe7/t/6228bfe3f412c818293e16e1/1646837732368/StateofK12Cybersecurity2022.pdf

[4] Federal Bureau of Investigation, "Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students," I-091318-PSA , Feb. 13, 2018. https://www.ic3.gov/media/2018/180913.aspx

[5] https://journals.sagepub.com/stoken/default+domain/ED-10.3102%2F0013189X221120538/full

[6] https://www.adexchanger.com/data-exchanges/60-of-school-apps-are-improperly-sharing-student-data-with-third-parties/

[7] https://me2ba.org/introducing-internet-safety-labs/; https://internetsafetylabs.org/resources/reports/spotlight-report-1-school-mobile-apps-student-data-sharing-behavior/

The FTC should prohibit all these practices, to ensure that any app or program assigned to a student to be used should not disclose their data to any third party that is not strictly necessary for the educational service being provided.

Need for FTC to specify security requirements more rigorously for collecting, storing and transmitting student data:

The number and extent of student data breaches has proliferated in part because the existing data security provisions in federal law are weak or non-existent. COPPA only requires "reasonable" security without the FTC having defined that term, and FERPA does not specify any data security protections at all. Even when companies do claim use of encryption or other forms of data security, there is no enforcement or oversight by the district, the FTC, or any other government agency to ensure this actually occurs.

Thus, breaches continue to occur, such as the recent Illuminate software that breached the personal data of at least three million students nationwide without penalties, despite the company's promise to encrypt the data, itself evidence of its deceptive practices.[8] Inadequate and lax security in the case of programs operated by Chegg allowed hackers to gain access to sensitive student data and employees' financial information.[9] And similar breaches appear to be occurring nearly every week.

Of course, once the data is in the hands of hackers or displayed across the internet, it can be sold, resold or abused for a variety of destructive purposes, including but not limited to identify theft.

In light of this, as a first step we urge the FTC to more clearly and strictly define what security protections must be used to transmit and store personal student data, given the rampant number of cyberattacks, ransomware, and breaches that are occurring.

The definition of "reasonable" security protocols must include a high degree of data encryption at rest and at motion and must require companies with programs operating in schools that have access to personal student data to undergo regular independent audits with transparent reporting of results to ensure that these security protocols are implemented faithfully. In New York State, every nonprofit organization with gross annual revenue of $250,000 or more must file a financial review prepared by an auditor; similarly, security audits should be required for companies with access to student personal information.

Data minimization and deletion must be required as well, so that companies only have access to the specific information needed to carry out their contracted educational services and must delete the data when no longer needed. One of the most disturbing aspects of the Illuminate breach is that among the personal data

[8] https://thejournal.com/articles/2022/05/27/illuminate-breach-included-los-angeles-riverside-county-pushing-total-impacted-well-over-3-million.aspx and https://www.the74million.org/article/illuminate-ed-pulled-from-student-privacy-pledge-after-massive-data-breach/

[9] https://www.nytimes.com/2022/10/31/business/ftc-chegg-data-security-legal-complaint.html

released was that of hundreds of thousands, if not millions, of students who had long graduated from high school, whose information, nonetheless, had been retained by the company for no particular reason.[10]

A massive breach of personal data in 2018 for millions of students from thousands of schools from the Pearson AIMs assessment program included PII of students going back at least to 2001, again from millions of students who had long before graduated from their schools, as well as students at schools that had stopped using the program years before.[11] Clearly companies should be required to delete data from any schools with whom their contracts have lapsed and for all students who have graduated. Better yet, such data should simply be deleted on an annual basis for any information not absolutely required to be kept as part of a student's permanent record.

As in FERPA, which requires these parental rights in relation to school districts, parents should have the right to request and obtain all the personal information held by the vendor about their child, the right to challenge it if incorrect, and to ask for it to be deleted as soon as it is no longer needed for a core school service.

If an ed tech company does not comply with these requirements, the FTC should impose substantial fines and penalties, as well as requiring proof of improved data security practices and policies within a specified time frame, and companies that do not or cannot comply must be prohibited from marketing their products.

Commercialization of student data must be more clearly prohibited and enforced

The FTC's own regulations and guidance pertaining to student data has varied over time, creating confusion and ambiguity over whether parents have the right to opt their child out of having their data collected by third party ed tech apps in a school setting and/or have the right to have such data deleted once it has been collected and opt out of any further collection. In any case, few schools have afforded or informed parents of these rights.

Regardless of the status of parental consent as a right, the FTC appears at a minimum to have said clearly that *if* schools are allowing ed tech apps or programs to collect their students' personal information without parental consent, this data can *only* be used for educational purposes – and not for "commercial purposes", as stated in the following guidance: "[T]he school's ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose."[12]

Yet these conditions are repeatedly flouted by ed tech companies, in part because the FTC has not sufficiently defined what commercial purposes means. Many programs and apps assigned to students openly admit that they use their data to improve their products or services and/or create new ones, both of which are clearly

[10] https://nycpublicschoolparents.blogspot.com/2022/03/what-illuminate-nyc-doe-ny-state.html
[11] https://www.geneva304.org/protected/ArticleView.aspx?iid=6YYB2BY&dasi=3G20
[12] https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

commercial purposes. Nonetheless, the FTC has not taken any action against these companies. Thus, public school students have been used as involuntary subjects of widespread experiments in online learning, as well as unpaid subjects for product development.

Even worse, there are many ed tech companies that continue to sell student data, use it to market their own products, and/or for targeting advertisements. One disturbing example is the college-and-career counseling platform Naviance. More than 40 percent of high school students across the country are enrolled in schools that use Naviance, according to a press release issued when the company was purchased by PowerSchool, itself a company providing student information systems to thousands of schools across the country.[13] PowerSchool in turn is owned by Vista Equity Partners, a private equity firm, which is amassing a large number of ed tech companies that collect, process and market student information in multiple ways.

As recently revealed by an investigative report in *The Markup*, Naviance collects a wealth of data directly from students, via surveys and otherwise, and then allows third parties to target their ads to them, based upon their demographic data, including their race.[14] Until recently, Naviance's website offered their clients the ability to identify and target ads to "students who fit specific demographic variables (race, ethnicity, geography, class year, attendance at an under-represented school) and present messages about your institution to students who possess those characteristics."[15]

In at least three cases identified by *The Markup*, colleges including University of Kansas, University of Southern Maine and University of Massachusetts in Boston targeted their ads in certain geographical areas only to white students. In addition, these ads were not clearly identified as such in the Naviance platform, but instead appeared as objective recommendations to students. Thus, this company not only made a profit by allowing the data collected from students to be used for commercial purposes, but they also enabled it to be used in a racially discriminatory manner and engaged in deceptive practices by not clearly identifying what were paid advertisements. [16]

When parents in Illinois, Colorado, Texas, and Maryland have asked their schools and/or Naviance for the data they've collected from their children, and how it has been used, they have been routinely denied that information.[17]

College Board has also been shown to sell a wealth of personal student data to colleges and other organizations for their recruitment efforts, without parental consent, even though this is decidedly not an

[13] https://www.powerschool.com/news/powerschool-and-naviance-and-intersect-close/
[14] https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students
[15] https://web.archive.org/web/20220113145009/https://www2.hobsons.com/solutions/match-and-fit
[16] https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students
[17] See also PCSP Letter to Sen. Durbin about these practices https://docs.google.com/document/d/1JggGtxI9sGxNl6JZZv7_NdFBIRR8_lab9Ev8jhZlH9U/edit?usp_dm=false

educational use of the data and in fact is illegal in several states.[18] Although College Board is ostensibly a non-profit organization, their behavior should concern the FTC because the company makes an estimated $100 million per year via this commercial activity, and has been reported to operate a for-profit arm that has stowed a quarter billion dollars in offshore tax havens.[19] If any non- profit outsources its operations or revenue to a for-profit company, rediscloses data they've collected from students to for-profit third parties, or directly engages in commercial enterprise involving selling and licensing personally-identifiable information itself, it should be required to follow the same rules to protect the privacy and security of this data as a for-profit corporation.

The issue of purportedly de-identified student data must also be addressed. Though many companies claim they have de-identified data and used it for commercial purposes, there is much evidence that it is relatively to re-identify student information given current techniques given a few demographic attributes.[20] If vendors intend to use de-identified data for commercial purposes, or for sale, they should be required to prove that the data cannot be re-identified by current methods.

Algorithmic uses of student data must be strictly regulated

Naviance collects data directly from students based upon questions related to their interests and background starting in middle school, and then uses that data to steer them towards particular colleges and careers.[21] Its owner, PowerSchool, also sells numerous products to schools and districts that generate predictions about students, including whether they will graduate from high school on time or meet certain benchmarks on the college entrance exams, based upon their personal data including their race and family income.[22]

Another software product used at the college and university level for predicting student outcomes is Navigate. Navigate generates algorithmic ratings of a student's "risk" of failure based on input including a student's race, and reporting based on public records requests found large racial disparities in Navigate's output. For example, Navigate was generating disproportionately large numbers of recommendations to steer Black students away from majoring in STEM concentrations and careers.[23]

We urge the FTC to reinstate the guidance posted in July 2014, on their "Complying with COPPA: Frequently Asked Questions" ("COPPA FAQ") webpage:

---

[18] https://www.washingtonpost.com/education/2019/09/11/is-new-york-state-about-gut-its-student-data-privacy-law/
[19] https://www.wsj.com/articles/for-sale-sat-takers-names-colleges-buy-student-data-and-boost-exclusivity-11572976621 ; https://thecriticalreader.com/the-college-board-is-a-non-profit-its-also-a-hedge-fund/
[20] https://www.nature.com/articles/s41467-019-10933-3; https://www.theregister.com/2021/09/16/anonymising_data_feature/
[21] https://www.fourpointeducation.com/wp-content/uploads/2021/10/2021-Naviance-Student-Survey-Report-Student-Perspectives-on-College-Career-and-Life-Readiness.pdf
[22] https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children
[23] https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success

"Whether the operator gets consent from the school or the parent, the operator must still comply with other COPPA requirements. For example, the operator must provide the school with all the required notices, as noted above, and must provide parents, upon request, a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information." [6]

In order for this transparency and oversight to occur, school districts must have contracts or other legal agreements with these vendors that require them to provide the student data they've collected upon parental request and reveal how it is to be used. If algorithmic processes are employed using the data to steer children into specific courses or careers, or to make other high-stakes decisions concerning their educational trajectory, there should be an appeal process that would enable students and their parents to ov**e**rride any high-stakes automated decision. [24]

The recently released White House/OSTP Blueprint for an Algorithmic Bill of Rights has many principles that the FTC should adopt in its rulemaking.[25] Among its proposed safeguards are requirements that no student should face discrimination by algorithms based upon their race or other demographic characteristics, and all such systems should be designed and used in an equitable ways. We believe that an independent audit of the algorithm's fairness and accuracy should be required before its use for any high-stakes decision process in any school**.**[26]

In 2019, our Coalition submitted comments to the FTC urging the Commission to strengthen the regulations to protect student privacy, almost exactly three years ago, which follow and offer more detail on many of these issues.

Thank you for your consideration,

Leonie Haimson and Cassie Creswell
Co-chairs, Parent Coalition for Student Privacy
info@studentprivacymatters.org
http://www.studentprivacymatters.org/

_____

[24] https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf https://www.nature.com/articles/d41586-022-02035-w

[25] https://www.whitehouse.gov/ostp/ai-bill-of-rights/

[26] https://www.lawfareblog.com/ai-bill-rights-makes-uneven-progress-algorithmic-protections

Via online submission October 17, 2019 at:
https://www.regulations.gov/comment?D=FTC-2019-0054-0001

Federal Trade Commission Washington, DC
20580

Re: COPPA Rule Review, 16 CFR part 312, Project No. P195404

The Parent Coalition for Student Privacy is a non-partisan organization of parent and privacy activists from throughout the nation. We have authored and co-authored position papers and reports, explaining the need for stronger data privacy protections for students, at the local, state, and federal levels. Our co- chair has testified before Congress twice in recent years.[1]

Since the Children's Online Privacy Protection Act was first passed by Congress in 1998, there has been a veritable explosion of digital programs and apps employed in schools, among them controversial behavioral and biometric tracking and surveillance programs. Insufficient oversight has been exerted to ensure that the personal information collected from children via these programs will not be breached or abused. As a result, an increasing number of breaches and ransomware attacks have occurred in recent years. Schools are now the second-largest victims of ransomware, only slightly behind local governments. [2]

In September 2018, the FBI issued a Public Service Announcement, warning of the risks involved in the increased data collection by ed tech programs in schools, and that "Malicious use of this sensitive data could result in social engineering, bullying, tracking, identity theft, or other means for targeting children."3 At the same time, many parents report that their children are bombarded with advertisements while using school-assigned apps or programs, which commercialize their data and distract from and undermine the quality of education they receive.

More recently, a bipartisan group of Senators sent a letter to the Commission, expressing their concerns and cautioning the FTC not to weaken children's privacy protections embedded in COPPA, as they suspected might occur because of certain actions taken recently by the FTC and the phrasing of the questions posed to the public in the Federal Register at this time:

---

[1] Stickland, Rachael. "Testimony before the US House of Representatives House Committee on Education and the Workforce Hearing on Strengthening Education Research and Privacy Protections to Better Serve Students." March 22, 2016; https://edlabor.house.gov/imo/media/doc/Stickland_oraltestimony032216.pdf; and "Testimony Before the United States House of Representatives Committee on Education and the Workforce Subcommittee on Early Childhood, Elementary and Secondary Education Hearing on "Exploring Opportunities to Strengthen Education Research While Protecting Student Privacy," June 28, 2017.
https://edlabor.house.gov/imo/media/doc/Strickland%20Testimony%206.28.17.pdf

[2] Gross, Natalie. "Ed tech's growth breeds district IT 'management nightmare'", *Education Dive*, Oct. 3, 2019.

"We agree that the Rule warrants updating, but we are concerned that the FTC is choosing to update the rule at a time when the Commission appears insufficiently appreciative of the threat some giant tech companies pose to children and parents...We also are concerned that many of the questions presented in the FTC's request for public comments suggest an intention to add exceptions and other rule changes to COPPA that would weaken children's privacy online. For example, you ask about exceptions to parental consent requirements around educational technology and voice-enabled connected devices…But the FTC's failure now and in recent years to fully enforce COPPA compliance has us concerned that an update at this time could diminish children and parents' control of their data or otherwise weaken existing privacy protections. Now is not the time to pull back."[4]

The Parent Coalition for Student Privacy strongly agrees with the concerns expressed by these Senators and urges the Federal Trade Commission to strengthen rather than weaken the privacy protections provided by COPPA in and out of school, including those related to parental consent, given the ongoing and numerous threats to student privacy resulting from the increased amount of data collection that is occurring in schools every day.

Please accept the comments below, with our responses to selected Commission's questions as posted in the Federal Register.[5]

A. General Questions for Comment

Question 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?

---

[3] Federal Bureau of Investigation, "Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students," I-091318-PSA , Feb. 13, 2018. https://www.ic3.gov/media/2018/180913.aspx

[4] Senators Markey, Blumenthal, Hawley and Blackburn, Letter to FTC Commissioners on COPPA and Children's Privacy, Oct. 4, 2019. https://www.markey.senate.gov/imo/media/doc/COPPA%20Letter%20to%20FTC%202019.pdf

[5] FTC, Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, July 25, 2019. https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online

Response 5: The relationship between FERPA and COPPA is very confusing to parents, as well as many school and district staff, especially in relation to the right of parents to be notified and consent when schools contract with vendors that collect personal information directly from their children. We have been approached by many parents who have alerted us to the fact that their schools and providers are **not** complying with COPPA, when their children under 13 are disclosing their personal information to companies via school-assigned apps, either at home or during the school day.

We urge the FTC to reinstate the guidance posted in July 2014, on their "*Complying with COPPA: Frequently Asked Questions*" ("COPPA FAQ") webpage:

"Whether the operator gets consent from the school or the parent, the operator must still comply with other COPPA requirements. For example, the operator must provide the school with all the required notices, as noted above, and must provide parents, upon request, a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information." [6]

COPPA's guidance is unclear about an operator's use of a child's personal information for "commercial purposes." For example, under M.2. on this webpage, it states if an "operator intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent."[7] Yet "commercial purposes" are not clearly defined.

Without sufficient guidance, teachers and schools are left adrift and are assigning websites and apps of companies that use the personal student information collected without parental consent to advertise, as well as improve their products and services and develop new ones, which we believe are "commercial purposes" and thus should not be allowed. Often, these programs or apps also link to other websites like YouTube that explicitly gather personal information for marketing or advertising to students. These practices are not allowed under COPPA, and they should be strictly prohibited.

Parents also question the legal status of titular non-profits that are not bound by COPPA but may be funded by for-profit partners and/or may redisclose personal data to for-profit "partners". If the non-profit is outsourcing its operation to a for-profit and/or redisclosing this data to for-profit vendors, we believe they should be responsible for adhering to COPPA.

---

[6] FTC, *Complying with COPPA: Frequently Asked Questions*, July 2014; archived at https://web.archive.org/web/20150311194001/https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

[7] See above.

In addition, when parents suspect that the school or district and/or operators may be violating COPPA, or ignoring it altogether, the complaint process is difficult to navigate and often there is no response to complaints or queries made by parents to the FTC.

Finally, given the increased number of data breaches by districts and operators, and the rising incidence of ransomware attacks, strict security standards should be incorporated into COPPA regulations, because data privacy is meaningless without data security as well.

For more on this, see the FBI alert of Sept. 13, 2018, in which the agency warned that "the US school systems' rapid growth of education technologies (EdTech) and widespread collection of student data could have privacy and safety implications if compromised or exploited." As the FBI pointed out:

''Malicious use of this sensitive data could result in social engineering, bullying, tracking, identity theft, or other means for targeting children. Therefore, the FBI is providing awareness to schools and parents of the important role cybersecurity plays in the securing of student information and devices… The widespread collection of sensitive information by EdTech could present unique exploitation opportunities for criminals."[8]

Given this widespread experience of schools, districts and their vendors that have suffered serious data breaches in recent years, the FTC should strengthen COPPA's requirements for security protection, data minimization and deletion, as well as reconfirm the parental consent requirements in the original law. In addition, the FTC should inform parents as to how they can exercise these rights and clarify that schools that contract with for-profit vendors must also comply with COPPA's provisions.

B. Definitions

Question 10: Are the definitions in § 312.2 clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?

Response 10: Parents from across the country have reached out to our coalition asking whether the education technology services and programs their children are assigned to by their schools should require prior consent and/or whether they violate COPPA's prohibition against using personal information for "commercial purposes." Despite our best efforts to decode opaque and often contradictory language in the operators' terms of use or privacy policies, we find it nearly impossible to determine whether there have been violations because COPPA simply lacks a clear and practical definition of "commercial purposes."

We strongly encourage the Commission to use this opportunity to create a transparent and meaningful definition of "commercial purposes" that prevents the exploitation of children and the monetization of their personal information in schools, in all circumstances. We oppose the use of any apps or programs in schools that advertise to children while using their products or collect children's data to be used in advertising at a later time, which is clearly a commercial purpose. We also oppose the use of apps or

[8] See footnote 3.

programs that collect and use children's data to improve a vendor's products and services and/or create new products and services, which is also a commercial purpose. For more specific examples of commercial activities that should be prohibited, please see **Response 23.(II)** below.

Question 13: Should 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? What about personal information that is inferred about, but not directly collected from, children? What about other data that serve as proxies for personal information covered under this definition? Does this type of information permit the physical or online contacting of a specific individual?

Response 13: Schools serving preschool, prekindergarten, and K-8 grade students across the country are currently deploying education technology whose operators collect and use extremely sensitive personal information from children under 13. Some operators offer "classroom management" tools that gather students' behavioral data, including tardiness, homework habits, number and length of bathroom visits, and compliance or non-compliance with other classroom rules.

It is well documented that data from disparate sources can be combined, scraped, profiled, shared, and sold by operators to data brokers, or other third parties. Data brokers' primary source of revenue is supplying data or inferred data about people, gathered mainly from sources other than the data subjects themselves.[9] Often these data elements are incredibly sensitive, including predictive behaviors and geolocation. Even if supplied in aggregate, it only takes a few data points to re-identify a person; that is why state privacy laws like Colorado's Student Data Transparency and Security Act[10] and California's Consumer Privacy Act[11] include inferred data in their definitions of personally identifiable information. Inferred information about children should absolutely be included in COPPA's definition of Personal Information.

The Commission would be wise to take account of the concerns expressed by Senators Durbin, Blumenthal and Markey in the letters they sent to 55 ed tech companies and data brokers in August 2019, asking about their data practices and policies, and pointing out how their data collection could put

[9] Christl, Wolfie. "Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions." *Cracked Labs: How Companies Use Personal Data Against People*, Cracked Labs Institute for Critical Digital Culture, June 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf .

[10] The Colorado Student Data Transparency and Security Act definition includes inferred data: "Student Personally Identifiable Information means information that alone or in combination, personally identifies an individual student or the student's parent or family, and that is collected, maintained, generated, or inferred by a public education entity, either directly or through a school service, or by a school service contract provider or school service on-demand provider." https://leg.colorado.gov/sites/default/files/2016a_1423_signed.pdf

[11] The California Consumer Privacy Act definition of Personal information includes, but is not limited to: "Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

students, parents, and educational institutions at risk of having their personal information stolen, collected or sold without their permission or knowledge".[12] The Senators' letters to data brokers specifically referenced research by Fordham University[13] on how data brokers were compiling and selling "sensitive" student data...based on GPA, ethnicity, religion, and income, among other highly targeted categories:

"From academic performance data and web histories, to location data and other personally identifiable information such as date of birth or address, it is imperative that we take steps to ensure students' data is being secured and protected. Parents, students, and educational institutions deserve to have more control over their data..."[14]

Some operators also collect students' medical diagnoses, mental health information, and prescribed medications which are used to help monitor confidential special education services. Biometric data, such as fingerprints and facial recognition, and proxy data, such as the language spoken at home and the length of time the child has lived in the United States, are also often collected by operators of ed tech.

The use of artificial intelligence in education is increasing and is largely unregulated and opaque in its effectiveness and accuracy. Even supporters of AI in education admit that it raises significant ethical and privacy considerations. AI is used in intelligent tutoring and dialogue based tutoring systems, to track student emotions, integrated into cloud storage and embedded in many ed tech platforms.[15] For example, it may be used in school security cameras to read students' facial expressions, predicting whether they pose a future threat because they "look violent."[16] As the ACLU has pointed out, AI in facial recognition technology in schools "has the potential to turn every step a student takes into evidence of a crime. Youthful misbehavior or simply hanging out with friends could be criminalized. Worse, students seeking confidential assistance from a counselor or school clinic will be caught in the system's dragnet."[17]

---

[12] See text of the Senators Durbin, Markey and Blumenthal letter to educational technology companies, at https://www.durbin.senate.gov/imo/media/doc/Google-Pichai.pdf and their letter to data brokers here, both dated August 19, 2019. https://www.durbin.senate.gov/imo/media/doc/Accurate%20Leads-Newton.pdf

[13] Reidenberg, R. Joel, et al. "Fordham Law School Center on Law and Information Policy (CLIP) Study Reveals Lack of Transparency in Commercial Marketplace for Sale and Exchange of Student Data." *Transparency and the Marketplace for Student Data 2014-18 Report*, Fordham University School of Law, 6 June 2018, https://www.fordham.edu/info/23830/research/10517/transparency_and_the_marketplace_for_student_data .

[14] Schaffhauser, Dian. "Senators Go After Ed Tech on Student Data Usage," *Campus Technology*, August 16, 2019. https://campustechnology.com/articles/2019/08/16/senators-go-after-ed-tech-on-student-data-usage.aspx

[15] Herold, Benjamin. "Google Experimenting with New Cloud Storage, Artificial Intelligence Initiative for K-12." *Education Week*, 4 Apr. 2019, https://mobile.edweek.org/c.jsp?cid=25920011&item=http://api.edweek.org/v1/blog/63/index.html?uuid=78829.

[16] Moreno, Ivan. "AI-Powered Cameras Are New Tool against Mass Shootings in Schools, Including at a Greeley District." *The Denver Post*, 15 Sept. 2019, https://www.denverpost.com/2019/09/15/ai-powered-cameras-school-shootings-greeley/amp/?.

[17] Coyl, Stefanie, and John Curr III. "New York School District Seeks Facial Recognition Cameras for Public Schools." *American Civil Liberties Union, Free Future*, 20 June 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/new-york-school-district-seeks-facial-recognition .

Ed tech platforms often offer "adaptive" and "predictive" services to schools that use secret and proprietary algorithms to serve new or "relevant" content to students. The algorithms are typically trained using massive data sets, collected from unwitting children, and often contain racial, gender, socio-economic, and other implicit biases. Research suggests that outputs from these systems may reinforce the discrimination that already afflicts too many children because of their racial, ethnic, disability, or economic status.

Often these types of services also collect and process sensitive information including a child's interest in certain subject matters, aptitude for particular tasks, the ability and desire to comply with instructions, as well as keystrokes and mouse movements which track the amount of time and position of a cursor on a screen. They then adapt and design their placement and/or instruction based upon this data, using secret, proprietary algorithms, whether correctly or not.

Persistent identifiers, device information, and geolocation data are often collected by ed tech vendors. It is unclear whether this information is used only for internal operations, or if this information is being leaked to and used by third parties or partners.

Further, operators often share aggregate data, but whether that aggregate data is truly anonymous is unclear, as is whether their apps may use embedded advertising IDs and/or derive them from Software Developer Kits that can identify and target a student. As the *New York Times* reporter Charlie Warzel has described, these Software Developer Kits:

"Among the information sent... [is] your device IP address and type, the time of use and your advertising ID. While the data is supposedly anonymized, the advertising ID makes it extremely easy for bigger companies to identify and link third-party app information... SDKS are embedded into thousands of apps...And every app is potentially leaking data to five or 10 other apps." [18]

As COPPA does not require operators to independently audit third parties, and the FTC has not done this itself, it is difficult to know exactly how much data is collected and how this information is used, in order to ensure that ed tech operators are COPPA compliant. We strongly urge the Commission to ensure that third parties be audited, and that personal information including device information and persistent identifiers are not used in ways that violate the law.

The collection of this massive amount of highly sensitive data may be used to create profiles of individual students that may not only prejudice their treatment by their schools or districts, but could also be misused by hackers, advertisers, or the operators themselves, as the FBI has warned.

As such, we recommend that the Commission expand the definition of "personal information" to include the types of data mentioned above, and strictly prohibit its collection without prior parental consent,

[18] Warzel, Charlie. "The Loophole That Turns Your Apps into Spies." *New York Times, Privacy Project*, 24 Sept. 2019, https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html .

and such consent must include informing parents about what data will be collected, how it will be used, and how it will be protected from breaches.

D. Parental Consent

Question 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." [7] 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? Should this exception have similar requirements to the "school official exception" found in the Family Educational Rights and Privacy Act ("FERPA"),[8] and as described in Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices? [9] If the Commission were to amend the COPPA Rule to include such an exception:

Response 23: It is our coalition's unwavering conviction that there should be no specific exception created to waive parental consent for the use of education technology in school. Parents' existing rights under COPPA to be informed and provide prior consent to any program collecting data directly from their children under the age of 13 should not be erased or limited simply because their children's use of a commercial operator's service occurs inside the school building or at the direction of a teacher or school administrator. In fact, we would support the increase in the age under which parental consent is required to at least 16 years or even older.

If the Commission is intent on relaxing the rules to benefit industry at the expense of children's privacy protections, operators must be held to especially strict standards to qualify for the exception of allowing schools to waive parental consent, as described in their 2014 FAQ.

*"… the operator must provide the school with all the required notices, as noted above, and **must provide parents, upon request, a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information** (emphasis added).*"[19]

In addition to the critical rights of parental notice, deletion and opt out of further data collection, ed tech operators who develop, offer, or market their services to schools or students under age 13 should also be required to satisfy a more rigorous definition of providing a "school purpose." Second, specific commercial uses of children's data must be banned outright by such operators. Third, such operators must be prohibited from collecting especially sensitive data, like medical data, behavioral and mental health data, disability status, biometric information, and geolocation, without explicit parental consent.

[19] *See* https://web.archive.org/web/20150311194001/https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Fourth, any data collected by such operators under the parental consent exception must be awarded rights at least as rigorous as those consistent with the "school official" exception in the Family Educational Rights and Privacy Act or FERPA.[20]

Fifth, each commercial operator falling under this classification must dedicate space on its website for notices related to the parental consent exception.

Sixth, operators must be required to be fully transparent. Given the opaque nature of how student data can be shared, repurposed, analyzed, profiled, and marketed, it is imperative that education technology providers be clear about the specific data they and their third-party partners collect from students, how the data will be used for a strictly educational purpose, and how the data will be protected and prevented from any further redisclosures.

Technology providers must post this information for each educational product they produce. Third party partners or subcontractors who have access to student data through their products or services should also be listed in the notification forms on a provider's website and should also be mandated to comply with all these requirements. Schools should also be required to link to and post this information as it applies to the specific education technology services they choose to utilize.

Colorado has implemented a similar transparency policy, adopted in 2016, which can serve as an achievable and effective model for all education technology providers and their subcontractors. [21]

Seventh, parents must be informed as to where to access this information on the part of operators, as well as how to challenge its accuracy, require its deletion and/or demand an end to its further collection. As schools are the intermediary between parents and ed tech operators, and the sole access point for information provided to parents, schools must be responsible for alerting parents as to where this

---

[20] *See* https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf

[21] See § 22-16-108 Colorado School service contract provider—re data transparency**: "***(1) Each school service contract provider shall provide clear information that is understandable by a layperson explaining the data elements of student personally identifiable information that the school service contract provider collects, the learning purpose for which the school service contract provider collects the student personally identifiable information, and how the school service contract provider uses and shares the student personally identifiable information. The information must include all student personally identifiable information that the school service contract provider collects regardless of whether it is initially collected or ultimately held individually or in the aggregate. The school service contract provider shall provide the information to each public education entity that the school service contract provider contracts within a format that is easily accessible through a website, and the public education entity shall post the information on its website. The school service contract provider shall update the information as necessary to maintain accuracy. " Also:* **§** 22-16-109 Colorado School service contract provider--use of data: Both at: Colorado Revised Statutes Title 22 Education §, 22-16-109 https://codes.findlaw.com/co/title-22-education/co-rev-st-sect-22-16-109.html

information can be found, through notification at the beginning of the school year and via an ongoing basis with the links provided on the school website.

More recommendations for subsections I-VII follow.

Response 23.(I): The Commission must establish a new COPPA definition of "school purpose" for commercial operators seeking eligibility for the parental consent exception. COPPA's existing framework of definitions, specifically the designation as a "web site or online service directed to children," provides precedent for a new term covering child-directed websites or online services that are also directed to preK-8th grade students.

Appropriate examples of definitions for "school purposes" can be found in state law. California enacted a landmark K-12 student privacy law in 2014, known as the Student Online Personal Information Act or SOPIPA, that provided the following definition:

22584.(j.) 'K–12 school purposes' means purposes that customarily take place at the direction of the K–12 school, teacher, or school district or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school. [22]

Additionally, in 2016, California enacted a successor to their SOPIPA law to extend the same privacy protections law to preschool and prekindergarten students found in the original law, as follows:

22586.(j.) 'Preschool or prekindergarten purposes' means purposes that customarily take place at the direction of the preschool, prekindergarten, teacher, or school district, or aid in the administration of preschool or prekindergarten activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between pupils, preschool or prekindergarten personnel, or parents, or are for the use and benefit of the preschool or prekindergarten.[23]

The preceding definitions may be merged and used as a basis for an appropriate COPPA definition. For example: "A 'school purpose' means an internet website, online service, online application, or mobile application that: (1) is designed, marketed, or offered for use by preschool, prekindergarten, or K-8 students; (2) is used at the direction of teachers or other employees of preschool, prekindergarten, or K-8 schools, and (3) collects, maintains, or uses personal information."

If there is any doubt about whether the data is solely used for a "school purpose" rather than, for example, a mechanism to direct advertising to students, the Commission should use their authority under Section 6(b) of the FTC Act to investigate.[24]

---

[22] CA SB-1177 at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB1177

[23] CA AB-2799 at: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB2799

[24] https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

Response 23.(II): Children using education technology at school or at the direction of the school should **never** have their personal information used for **any** commercial purpose, particularly if the operator seeks an exception to the parental consent requirement. Unlike private companies that provide institutional functions to schools for a contracted fee such as cafeteria, janitorial or transportation services, many educational technology operators offer their products via "click wrap" agreements at "no cost." This strategy allows companies to avoid "top-down" decisions which are typically made by district administrators and school boards, which are criticized for being overly bureaucratic and riddled with red tape. But free, in this case, is not necessarily free.

Commercial operators offering no-cost services to schools and the public must turn a profit eventually or they will eventually cease to exist. How and when they profit depends on the type of service provided, but it is likely that users' personal information, whether de-identified or identifiable, is used to generate revenue. This constitutes a commercial use of data.

While all children should be protected from having their personal information used for any commercial purpose, COPPA must provide an additional layer of protection for students because their use of education technology is likely obligatory. Therefore, in addition to the commercial activities currently prohibited by COPPA, the Commission should ban operators of education technology from using or processing de-identified or identifiable student information to improve existing or to develop or improve new educational or non-educational products and services; or to generate and display advertisements to students and parents.

Further, we urge the Commission to protect children by drawing on their Section 6(b) authority[25] to investigate educational technology platforms and their third party partners and subcontractors in order to ensure they are truly only using the data as allowed under COPPA. What information are these platforms collecting, and how are they using and sharing the data they collect? Are data truly only being used for a school purpose? Are platforms or third parties misusing data for marketing, or repurposing student data? Are they exposing inappropriate and potentially dangerous content to children?[26]

Response 23.(III): While we support requiring prior, written parental consent in *all* cases for the collection of personal student data for children under 13, within or outside of the school context, it *must* be required for those vendors or operators who are collecting and using especially sensitive student information. These include health and medical data ordinarily protected by the Health Insurance Portability and Accountability Act or HIPAA;[27] sensitive behavioral data, such as suspension information; and biometric data. Several state student privacy laws have special restrictions around the collection of biometric data in schools (e.g. Illinois) or ban it altogether (e.g. Florida), including "any physical or behavioral characteristics that are attributable to a single person, including fingerprint characteristics,

[25] Section 6(b) of the FTC Act https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority
[26] "Internet Crimes Against Children." *Online Victimization of Youth*, https://www.icactaskforce.org/Pages/InternetSafety.aspx.
[27] *See* https://www.hhs.gov/hipaa/index.html

hand characteristics, eye characteristics, vocal characteristics, and any other physical characteristics used for the purpose of electronically identifying that person with a high degree of certainty. Examples of biometric information include, but are not limited to, a fingerprint or hand scan, a retina or iris scan, a voice print, or a facial geometry scan" [28] as well as a DNA sequence.

The method for obtaining explicit, written parental consent should be facilitated by the school or school personnel and follow the process described per our recommendation in **Response 23.(V)** below**.** Consent, which parents must be allowed to revoke at any time, should be recorded and maintained by both the commercial operator and the school directing the use of the technology.

Response 23.(IV): If the Commission is intent on seeking the parental consent exception for school officials, which we do not support, the new rules must at minimum protect student data consistent with the "school official" exception of the Family Educational Rights and Privacy Act or FERPA,[29] detailing specific responsibilities for commercial operators. New rules should establish that the operator must:

a. Perform "an institutional service or function" for which the school would otherwise use employees.

b. Be "under the direct control" of the school "with respect to the use and maintenance" of personal information, including providing parents the right to inspect, review, amend or delete a student's personal information the parents "believe to be inaccurate, misleading, or otherwise in violation of the student's privacy rights." The Commission should define "direct control," which means that an enforceable contract or agreement is required between the operator and the school, that it should be made available to parents, and that it specifies exactly what types of student information are collected, and for what purposes the information is used, and how it will be protected.

c. Be subject to the disclosure, and redisclosure requirements in FERPA § 99.33(a),[30] which limits the use of personal information to purposes only for which the disclosure was originally made and prohibits redisclosure without prior parental consent.

d. Meet specific notification requirements. See **Response 23.(V)** below for details.

Response 23.(V): COPPA's current notice requirements establish that commercial operators of child-directed websites must publish notice, including:

---

[28] *See* https://www.flsenate.gov/Session/Bill/2014/0188/BillText/er/HTML

[29] § 99.31 Under what conditions is prior consent not required to disclose information? https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf

[30] § 99.33 What limitations apply to the redisclosure of information? (a)(l) An educational agency or institution may disclose personally identifiable information from an education record only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student. (2) The officers, employees, and agents of a party that receives information under paragraph (a)(l) of this section may use the information, but only for the purposes for which the disclosure was made.

"Notice on the Web site or online service. In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, *and*, at each area of the Web site or online service where personal information is collected from children."[31]

In addition to existing required notices, a commercial operator with an "educational purpose" seeking an exception to the parental consent requirement must include notices "on the home or landing page or screen of its Web site or online service" that align with our recommendations in **Response 23.(I-IV)** above.

These include:

a. a clear and concise description of the educational technology's "educational purpose;"
b. a declaration that the operator will not collect or use student information for prohibited commercial purposes;
c. an acknowledgment that certain especially sensitive student information will not be collected by the operator without explicit, written parental consent, a description of the process for obtaining consent when applicable, a list of the sensitive data to be collected, if any; and
d. a detailed description of the FERPA-aligned rights and data protection the operator is obligated to comply with, including the process by which parents can inspect, amend and delete the personal information of their children held by the operator.

Response 23.(VI): For each particular contract that an operator has with an education agency, whether at the state, district, or school level, it must be required to be transparent, by including on its website a clear and concise description of all the information listed above in **Response 23.(V)**, and also including which particular data elements will be collected, the names and identities of all their subcontractors and any other third parties that will be provided access to the data, how the data will be used solely for educational purposes with no commercial uses allowed, how it will be protected from any further redisclosures, and how parents can inspect the data, delete it and/or prohibit its further collection. The same must be true for any click-wrap agreement entered into by a school, state, or district.

Response 23.(VII): As noted above, schools must be responsible for alerting parents where they can find this information and how they can exercise their rights under COPPA, as schools are the primary access point for families. They must notify parents at the beginning of the year of all the apps or programs their children will be using that collect their data, that they have rights to challenge and delete the data and/or bar its further collection, and where they can access more information about the vendors' data collection practices and how to exercise their rights under the law. Schools should be required to inform parents via email and snail mail at the beginning of the school year, as well as provide a page on their websites that contains this information.

[31] See current Federal COPPA regulations at https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5#se16.1.312_14

Question 23.a: Should the Rule specify who at the school can provide consent?

Response 23.a: If the school is allowed to consent on behalf of parents, the school or district must have clear and uniform policies for adopting education technology led by a team of qualified education research, curriculum, privacy and technology experts. A process of this nature would increase the likelihood that any technology used by students would be age-appropriate and protect the privacy and data security of each student. In reality, virtually anyone involved with schools is currently providing consent on behalf of parents, including administrators, classroom teachers, support staff, volunteers, and even students themselves.

Question 23. 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 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 de-identified data? Are there instances in which de-identified information has been sold or hacked and then re-identified?

Response 23.b: As described in **Response 23.(II)**, our coalition fundamentally believes that commercial use of children's data collected in schools is not acceptable, even if it has been "de-identified." Children's labor and intellectual property should not be monetized simply because it may be technologically possible to do so.

As such, under no circumstances should children's de-identified or identifiable information be used for any commercial purpose including to "improve the [operator's] product," whether the website is intended for use in schools or at home. Nor should operators be allowed to use such information to "improve other educational or non-educational products."

In addition, the technological possibility of true de-identification becomes less and less justifiable each year, reinforcing the need to make these determinations on an *ethical* basis, not a technological one.

Research has shown for nearly two decades that de-identified data may be reidentified on the basis of a very limited set of demographic information. Most recently, Na et al (2018)[32] used only "age [...], sex, educational level, annual household income, race/ethnicity, and country of birth" to reidentify physical activity data. Rocher et al (2019)[33] found that "99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes" and concluded:

[32] Na L, Yang C, Lo C, Zhao F, Fukuoka Y, Aswani A. "Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning." *JAMA Network Open*. 2018. Vol 1. No. 8.

[33] Rocher L., Hendrickx, J. and de Montjoye, Y-A. Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications***.** 2019. Vol 10.

"Our results reject the claims that, first, re-identification is not a practical risk and, second, sampling or releasing partial datasets provide plausible deniability. Moving forward, they question whether current de-identification practices satisfy the anonymization standards of modern data protection laws such as GDPR and CCPA and emphasize the need to move, from a legal and regulatory perspective, beyond the de-identification release-and-forget model."

The Commission should strictly limit operators' use of personal information to that purpose for which it was originally collected – whether for educational or non-educational products. Any further use must be restricted to activities that support the "internal operations of the Web site or online service," which COPPA currently allows. This includes:

"(1) Those activities necessary to: (i) Maintain or analyze the functioning of the Web site or online service; (ii) Perform network communications; (iii) Authenticate users of, or personalize the content on, the Web site or online service; (iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising; (v) Protect the security or integrity of the user, Web site, or online service; (vi) Ensure legal or regulatory compliance; or (vii) Fulfill a request of a child as permitted by §312.5(c)(3) and (4)." [34]

However, our coalition firmly urges the Commission to omit the statement "(iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;" from this section, since advertising is a commercial activity that should be banned for education technology operators altogether. Other commercial activities that should be prohibited are detailed in **Response 23.(II)**.

Question 23.c: Should parents be able to request deletion of personal information collected by operators under such an exception?

Response 23.c: Yes, in addition to our suggestions in **Response 23.(IV)**, which include allowing parents to inspect and correct student information maintained by commercial operators consistent with FERPA, parents should retain their right to request deletion of personal information from operators outside the school setting, as parents currently have the right under the school context according in COPPA. Additional rules should clarify the process by which parents can exercise their rights, which should be detailed in the public notice described in **Response 23.(V)**.

Question 23.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?

Response 23.d: Yes, the school is the intermediary between parents and school vendors or operators, and thus should be responsible for notification to parents as to the information practices of these vendors. If school-authorized operators or vendors will be collecting personal data directly from children,

[34] *See* https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5

parents should be notified at the beginning of the year on the school website and via email or snail mail of exactly which operators will be doing so; what particular data elements will be collected and for what purpose; how that data will be protected against further disclosures; when the data will be deleted; and how parents can exercise their rights to see the data, amend if it is incorrect, delete it and/or bar any further collection.

Question 23.e: Should such an exception result in a preemption of state laws? If so, would that result negatively affect children's privacy?

Response 23.e: COPPA should serve as the floor, not the ceiling. Regardless of the outcomes of this review process, any parental consent exceptions considered by the Commission must not preempt stronger provisions in state law.

State legislatures across the country have responded to legitimate student data privacy and security concerns by passing 99 laws in 39 states between 2013 to 2018. Our organization analyzed each law and graded them against five principles to protect student privacy.[35] The resulting report, written with the Network for Public Education, "*The State Student Privacy Report Card: Grading the States on Protecting Student Data Privacy*," concluded that while most laws do not adequately protect students' privacy, in many cases they do provide stronger protections than currently provided by federal law. [36]

Question 23f: Should the scope of the school's authority to consent be limited to defined educational purposes? Should such purposes be defined, and if so, how? Should operators seeking consent in the school setting be prohibited from using information for particular purposes, such as marketing to students or parents?

Response 23.f: Our coalition's uncompromising recommendation is that COPPA should not be weakened by introducing a parental consent exception for schools. However, should the Commission pursue this regrettable solution – which would disproportionately benefit commercial operators over the privacy of students – the FTC must introduce new rules to bring balance to the equation. Our recommendations in **Response 23.(I-V)** provide a starting point.

Sincerely,

Rachael Stickland, Leonie Haimson, Cheri Kiesecker and Cassie Creswell
on behalf of The Parent Coalition for Student Privacy
www.studentprivacymatters.org
info@studentprivacymatters.org

---

[35] *See* https://www.studentprivacymatters.org/five-principles-to-protect-study-privacy/

[36] Parent Coalition for Student Privacy and Network for Public Education, *The State Student Privacy Report Card: Grading the States on Protecting Student Data Privacy,* January 2019. *h*ttps://www.studentprivacymatters.org/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf