PARENT COALITION FOR STUDENT PRIVACY

Via online submission March 11, 2024:
https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule#open-comment

Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: COPPA Proposed Rule, 16 CFR part 312, Document 89 FR 2034

The Parent Coalition for Student Privacy (PCSP) 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; testified in Congress and state legislatures; drafted and passed student privacy legislation; and continue to advocate for improved laws, regulations, policies and procedures to protect the personal data of students across the US.

In October 2019, PCSP submitted comments to the Federal Trade Commission during the public submission process on the implementation of Children's Online Privacy Protection Act (COPPA).[1] Since then, our concerns about the invasive and often irresponsible use of educational technology in schools have only increased. Parents share our concern. According to a national survey conducted in the summer of 2023, 73% of parents are concerned about the privacy and security of student data collected and stored by schools, a significant increase compared to the 61% who expressed similar concerns the previous year.[2]

We are gratified that the Commission is taking action to address long-standing issues with the complexity of how COPPA applies to the school setting by amending the Children's Online Privacy Protection Rule (COPPR), including strengthening data security requirements and improving the definitions of personal information and commercial purposes.

However, many of the concerns expressed in our 2019 comments are not addressed by the proposed rule, and we believe that, overall, the rule changes are insufficiently protective of children and excessively permissive of commercial operators and schools. Since 2019, our concerns have only grown, related to expanded use of technology in schools, including the operation of surveillance programs, algorithms and AI, which provide additional serious risks to student privacy and their individual rights.

---

[1] https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online; Our comment available here: https://secureservercdn.net/198.71.233.128/t8b.b96.myftpupload.com/wp-content/uploads/2019/10/FTC-COPPA-comments-final-October-17-2019.pdf

[2] https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/

In particular, in 2019 we laid out our strong objections to creating an exception to allow schools to consent on behalf of parents to companies collecting children's personal data, and we also outlined, if such an exception were to be granted, under what circumstances it should take place. Stronger safeguards for student data privacy and security are needed and include the following:

- Existing parental rights under COPPA of direct notice, data deletion and opting out of further collection, while they may need to be modified under school-authorized consent, should be maintained.
- Data collection must satisfy a rigorous definition of fulfilling an "educational purpose" and any sale or use of such data for marketing or commercial purposes should be strictly prohibited.
- Explicit parental notification and parental consent should be required for collection of especially sensitive data, including medical data, behavioral and mental health data, disability status, biometric information and geolocation, as well as the use of digital surveillance programs that can track children's behavior at home and at school;
- There should be an extension of parental rights to match those that are contained in the regulations concerning the Family Educational Rights and Privacy Act (FERPA); namely, parents should have the right to access any data of their child that is held by third parties, and challenge it if it is inaccurate.
- Notices should be included on commercial operators websites as well as school websites, listing what specific student data is to be collected, how that data will be used, which third parties will have access to data, and how it will be protected from breaches and/or further disclosures.
- Schools should be required to notify parents about which operators have collected their children's data, how they can access this information and fulfill their rights to review, challenge accuracy, and request deletion or an end to data collection.
- There must be specific and robust security measures used to protect the data from breaches or inadvertent release, along with regular independent security audits, especially given the widespread occurrence of student data breaches in recent years. There can be no data privacy without data security.
- As we have learned in recent years, one of the most important ways to prevent inappropriate access to data, including as a result of breaches, is to require data minimization and deletion. Thus, the rule should also contain provisions that only the category of personal student information needed to perform the specified educational purpose may be collected and the data must be deleted at a specific time, and, at the least, when the agreement with the school or district lapses, or the student graduates or leaves the district. Best would be to require annual deletion of all personal student data, unless the purpose for retaining it can be fully justified and clearly explained.
- Parents must be alerted to any data breaches or improper releases of personal student data, and the operator must be required to pay for this notification, as well as methods by which parents can help prevent the improper use of their children's data, including monitoring and/or preventing identity theft.
- Ostensible non-profit companies should be subject to the same oversight and restrictions if they utilize the student data that they have acquired as school service providers, including prohibiting them from using the data for sale, marketing or other commercial purposes, as well as ensure that the data they disclose to third parties are not used in a similar manner.

- New threats to student privacy are represented by the use of AI, which depends on the collection of huge amounts of personal student data for commercial purposes, and also the use of algorithms, which can be discriminatory and restrict the opportunities of students based racial and/or gender stereotypes.

Unfortunately, in its current state, we find that the proposed rule falls short of these safeguards:

- Under the school-authorized consent, parents will no longer have the rights they previously had under § 312.4 to receive direct notice of data collection and disclosure, or under § 312.6(a), to directly review data, request data deletion and/or opt out of further collection. Though these rights may need modification in a school context, they should be maintained and give parents at least the transparency, access and control they have under FERPA.
- Furthermore, under the "school official" exception of FERPA, created via regulatory changes, schools have been given broad leeway in disclosing student data without parental consent, but parents have nonetheless retained their right to inspect and correct or amend their child's data, opt out of the disclosure of directory information, and be informed of their rights under FERPA on an annual basis. We fear that the proposed rule could weaken these rights, as it explicitly says parental rights are ceded to schools under the school-authorized consent exception, without specifying any such rights that parents should retain under the law. This is unacceptable.
- The definition of *school-authorized education purpose* is too vague and could include operators using student data to improve existing products and/or develop new products, which are inherently commercial activities. The increase in the use of large volumes of data to train algorithms for artificial intelligence makes it even more imperative to clearly prohibit product improvement and development in the definition of education purpose.
- While the definition of *personal information* has been modified to explicitly include biometric information, there are no additional constraints on its collection, use or disclosure nor any for other categories of extremely sensitive personal data, including behavioral, mental and physical health data that we believe need to have stronger protections. We would add to that the need for restrictions on schools' use of commercially-available surveillance programs, used to monitor or spy on students in and outside their homes, which have questionable educational value and great potential for harm.
- While the proposed rule does specify what operators should include in a notice for school-authorized data collection and use, there is no requirement for schools to post such notices or make it clear to parents where they can access them, leaving it unclear how parents would be informed of the school's consent. Nor is there any requirement for schools to inform parents of any rights to control their child's data. In addition, the notices would only need to list the "categories" of third parties to whom operators can redisclose information, rather than identifying those specific third parties. The rule also fails to make clear that any third parties that receive access to the data through the operator must be bound by at least as strong privacy and security protections as the operator itself.
- Finally, specific and enhanced data security protections should be required for all school-authorized services, given the ubiquity of student data breaches, as well as parental notification of any breaches or unauthorized exposures of their children's personal information.

Below we will go into more detail about these issues and other concerns we have with the proposed rule change.

Proposed definition of *school-authorized education purpose*

We appreciate that the Commission agrees that children's data should not be used for any commercial purpose by a school authorized service. However, the definition proposed in the new rule for distinguishing between educational and commercial purposes is not sufficiently clear or restrictive. Instead, it says the following:

> *"School-authorized education purpose means any school-authorized use related to a child's education. Such use shall be limited to operating the specific educational service that the school has authorized, including maintaining, developing, supporting, improving, or diagnosing the service, provided such uses are directly related to the service the school authorized. School-authorized education purpose does not include commercial purposes unrelated to a child's education, such as advertising."*

We disagree that "developing" and "Improving" a service or product involves an educational purpose, as both are clearly commercial. The Federal Register discussion states the following[3]:

> *"The Commission also agrees with those commenters recommending that the school authorization exception should allow operators to engage in limited product improvement and development, provided certain safeguards are in place. The Commission believes that allowing providers to make ongoing improvements to the educational services the school has authorized benefits students and educators, and that user data may be necessary to identify and remedy a problem or "bug" in a product or service. Therefore, in contrast to general marketing, product improvement and development can be viewed as part of providing an educational purpose rather than engaging in an unrelated commercial practice."*

Yet no further mention is made of what "certain safeguards" would be recommended if operators use the data for "limited product improvement and development" or how this "limited product improvement and development" differs in any significant degree from the commercial purposes that are otherwise prohibited in the law. Moreover, identifying and remedying a bug or problem could easily be classified as maintaining, supporting or diagnosing a service, allowable within the confines of the law. This is particularly true, given the now ubiquitous use of large amounts of personal data to train statistical algorithms ("AI"), the use of which has additional profound risks to student privacy and the quality of education they receive.[4] We should not be allowing students and their personal data to be used by operators for the purpose of involuntary product development or as beta testers in our schools.

---

[3] https://www.federalregister.gov/d/2023-28569/p-435

[4] "The Unintended Consequences of Artificial Intelligence and Education." Wayne Holmes. October 2023. https://www.ei-ie.org/file/740

Identification of type of data and actual third parties receiving data

If operators are disclosing children's information to third parties, then any consent, notice or written agreements should include what specific types of data will be disclosed as well as the identity of the third parties receiving the data, rather than merely stating the categories of third parties. Permitting "specific categories" rather than the actual identity of third parties appears in § 312.4(c)(1), § 312.4(c)(10) and § 312.4(d) of the proposed rule.

As the Commission, quoting itself, states in the discussion[5] (emphasis added):

> *"In the preamble of the 1999 initial COPPA Rule, the Commission noted that '**disclosures to third parties are among the most sensitive and potentially risky uses of children's personal information**. This is especially true in light of the fact that children lose even the protections of [COPPA] once their information is disclosed to third parties.'"*

Note also that under the existing § 312.5(a)(2) parents consent for sharing data with an operator does not transfer to third parties, and even under the proposed change, there is only a narrow exception made for this consent in the case of services that are inherently designed to communicate with third parties, e.g. message boards.

We believe operators should be required to specify the actual identity of the third parties to which they intend to redisclose a child's data; otherwise this greatly undermines the strength and the purpose of the law and the rule. At the barest minimum, parents and schools should know which specific entities are in possession of their children's personal information.

Requiring written agreements between schools and operators

Although we remain in opposition to removing a parent's right to consent to the collection of their child's personal information § 312.5(c)(10), we are strongly in favor of the requirement in § 312.5(c)(10) for a school to have a written agreement with the operator in order to authorize such collection and which includes the requirements under § 312.5(c)(10)(i-iv).

While we expect school management organizations and the ed tech industry to object to this requirement as overly burdensome, a key provision of many state student privacy laws that have been enacted since 2014 is the requirement to only share student information with an operator under a written agreement between the school and the operator. These laws have been implemented successfully without an insurmountable legal and financial cost on districts and operators.[6]

In fact, local education agencies (LEAs) should appreciate the *benefits* of the requirement for a written agreement, in particular for the sub-requirement that the agreement "indicates the name and title of the

---

[5] https://www.federalregister.gov/d/2023-28569/p-326

[6] The Student Data Privacy Consortium (SDPC) (https://privacy.a4l.org/) is an example of how collaboration across LEAs can lessen the burden of compliance. It provides education agencies with both a standardized contract template and the specific contracts negotiated by other members of the consortium for when they wish to use a new service. The cost to join the consortium is minimal, currently, $750-$950/year for a school or district. (https://home.a4l.org/join-the-community/)

person providing authorization and attests that the person has the authority to do so" because LEAs should have clear policies for when their employees enter into contracts that potentially bind the LEA legally, which click-wrap terms of agreement may in fact do, and for when employees use software services on LEA systems. LEAs should appreciate that the FTC is their ally in protecting an LEA's institutional interests as well as those of the children in their care by only permitting operators to collect and disclose the data of the children in schools under an official written agreement.

Ceding parental rights under school authorization and interactions with FERPA

Our objections to a school-authorization exception to parental consent center on the fact that parental control over their child's data is generally quite weak after decades of expanded data collection in schools, while laws and regulations that have not kept up with this expansion. We do not believe that parents and students should have to give up a child's personal data in order for them to receive an education, and the pendulum has swung much too far towards parents and students relinquishing control versus retaining control. Two aspects of maintaining parental control if a school-authorization exception to the rule is added are key for us: (1) certain types of highly-sensitive data merit greater protection and, thus, greater parental control over their collection and use; and (2) to the extent that parents have *not* ceded control under FERPA's school official exception, under COPPA's rule parents should also retain rights at least as strong as those in FERPA.

Parents should retain stronger control over highly sensitive data:

As mentioned above, some types of children's personal information are of such sensitivity that there should be an obligation on the part of the operator and the school to acquire explicit parental consent for its collection and disclosure. As we outlined in our 2019 comments, we believe that medical data, behavioral and mental health data, disability status, biometric information and geolocation data, should all require specific parental notification and consent.

We would now add to this list data collected for the use of surveillance, as there are many studies done in the last few years documenting how the surveillance of students in and out of school has not enhanced their safety but led to a whole host of negative consequences. Many recent reports show that such surveillance represents multiple risks to the privacy of students; and making them less likely to report dangerous behavior of their peers.[7] Student surveillance software is too often used for disciplinary purposes and often results in increased contact with law enforcement,[8] and the harms of surveillance software disproportionately impacts marginalized populations. Students with disabilities report higher rates of disciplinary intervention and punishment arising from surveillance programs.[9] Meanwhile, nearly a third of LGBTQ+ students said that they or someone they know has been "outed" by the technology.

---

[7] https://www.aclu.org/publications/digital-dystopia-the-danger-in-buying-what-the-edtech-surveillance-industry-is-selling ; https://www.rand.org/pubs/research_reports/RRA2910-1.html

[8] https://www.warren.senate.gov/oversight/reports/warren-markey-investigation-finds-that-edtech-student-surveillance-platforms-need-urgent-federal-action-to-protect-students ; https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/

[9] https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/

In light of all this, the additional burden on schools to gain parental consent for collection, use and disclosure of such data is in fact justified, given the serious risks of breach and/or misuse of such data.

The Commission explained why the proposed rule allows for school-authorization rather than parental consent:

> *"The Commission finds compelling the concern that requiring parental consent in the educational context would impose an undue burden on ed tech providers and educators alike [...] In situations where some number of parents in a class decline to consent to their children's use of ed tech, schools would face the prospect of foregoing particular services for the entire class or developing a separate mechanism for those students whose parents do not consent.*

We acknowledge this concern on the part of schools, which is why we are proposing parental consent be confined to apply only for highly sensitive data, not for all types of data. In addition, we feel strongly that concerns about parents refusing to consent to their child's school authorizing operators to collect and use highly sensitive data can best be alleviated by ensuring that collection and use stringently follow best practices for data security, data minimization and purpose limitation. If parents have confidence that their child's data is not being commercially exploited or used for surveillance, not being collected needlessly, not being held for time or use beyond its original purpose, and being held securely, then they will be inclined to consent.

Parental rights should not be uniformly retracted in a school context:

Under § 312.6(b) parent rights to refuse further use or further collection, to direct deletion, and to review collected information are now the *school's* right, not the parents:

> *"Where personal information is collected from the child pursuant to § 312.5(c)(10), the operator of the website or online service is required to provide the rights under paragraph (a) of this section to the school and is not required to provide such rights to a parent whose child has provided personal information to the website or online service."*

We firmly disagree with the blanket retraction of these rights. Even if the power of authorization will be granted to a school rather than a parent, the parent should still retain some basic control over their child's data.

We acknowledge that the rights parents have under COPPA for non-school collection and use of their child's data will need to be modified to allow for the practical operations of educational institutions. We also agree that parents necessarily relinquish *some* control to the school when they enroll their child, as the discussion of the proposed rule explains:

> "*When a child goes to school, schools have the ability to act in* loco parentis *under certain circumstances. This is particularly the case when schools are selecting the means through which the schools and school districts can achieve their educational purposes, such as when deciding which educational technologies to use in their classrooms."*

But we believe control should be maintained, especially for highly sensitive data as discussed in the previous section, and to a level that at least meets the rights parents currently have under FERPA. A new COPPA rule should not weaken FERPA nor further confuse schools and parents about which rights apply.

As such, we propose the following modifications of parental rights under COPPA in the case where a school authorizes an operator's access to a child's data.

1) **Right of review:** We see no justification to eliminate a parent's right of review, a right retained by parents when data is shared under FERPA's school official exception. The adaptation needed for the COPPA school authorization condition is that the school, having acted in place of the parent in authorizing consent, should be required to ensure that only the child's parent is provided with access to the child's data when a request to review is made. Parents should make requests to review to the school, and the school can then be the point of contact with the operator. Schools already must do this under FERPA, and it will eliminate the operator's need to verify the parent's identity.
2) **Right to refuse further collection:** As with requiring consent for highly sensitive data, allowing parents to refuse further collection could also interfere with a school's right to decide which education technologies to use. However, allowing a parent the right to refuse further data collection does *not* necessarily mean that their child has the right to be provided with an alternative service or instructional activity. We believe that if this right is maintained, schools could be encouraged but not compelled to provide an alternative that does not require personal information rather than required to do so in the event a parent wants to end data collection. Another possibility is that the parent's right to refusal for further collection under school-authorized consent could be restricted to the same conditions we describe above for requiring explicit parental consent, namely only for highly-sensitive data or data being used for surveillance purposes. In other words, a parent will retain the right to refuse further collection under some circumstances, but a narrower set than those that apply for direct parental consent.
3) **Right to deletion:** In a school context, a right to delete data could significantly interfere with a school's ability to manage its educational mission on a day-to-day basis and over the longer term, and a blanket parental right to delete any and all data is understandably impractical. We do think there are cases where a parent has a compelling need to have some data deleted, but that right could in some cases be superseded by federal and state requirements to retain data under education records laws.[10] We would also find acceptable that, instead of the right to deletion that parents have under COPPA currently in all contexts, in a school-authorized context, parents would instead have at last the same rights as FERPA grants them to challenge inaccuracies in a child's data and have them corrected or have an amendment included acknowledging the challenge.[11] A stronger right to deletion should also be retained for highly sensitive or surveillance data.

---

[10] For an example of this, see 105 ILCS 85/27(g). But compare 105 ILCS 5/10-20.40 where data destruction upon parental request is not superseded by federal or state records laws.

[11] See the EU GDPR for more at https://gdpr-info.eu/art-22-gdpr/; also https://www.oecd-ilibrary.org/sites/09e55ac4-en/index.html?itemId=/content/component/09e55ac4-en and https://www.brookings.edu/articles/ai-is-coming-to-schools-and-if-were-not-careful-so-will-its-biases/ and https://www.edweek.org/leadership/why-schools-need-to-talk-about-racial-bias-in-ai-powered-technologies/2022/04 https://unesdoc.unesco.org/ark:/48223/pf0000388971

Note that the Illinois School Code (105 ILCS 5/10-20.40) requires parental notification and consent for the collection of a student's biometric information and permits parents to withdraw consent and have such data destroyed. In addition, a parent withholding consent "must not be the basis for refusal of any services otherwise available to the student." This provision has been in the Illinois School Code for more than a decade without interfering with the ability of Illinois' schools to achieve their educational purposes.

Finally, an important right not mentioned above that should be addressed in any revisions to the COPPA rule is the right to algorithmic transparency. Any commercially-developed algorithms used in educational decision-making should be transparent and clearly explained to parents, audited by independent third parties for accuracy and lack of bias, and be able to be superseded by human input and decision-making.

Notice for parents under school-authorization exceptions

If a school-authorization exception is to be included in the rule, then it is *not* at all unreasonable to require more responsibilities for the school/district/LEA to notify parents about how they can access and exercise their rights under COPPA. In the discussion, the FTC says:

> *"The Commission agrees that notice is an important aspect of the proposed school authorization exception. At the same time the Commission agrees with commenters who raised concerns about imposing burdens on schools that may not have sufficient resources to undertake an additional administrative responsibility. To promote transparency without burdening schools, the Commission proposes requiring operators to provide notice."*

If a school does not have the resources to keep parents informed about data disclosure and collection, then we question whether they have the ability to responsibly oversee such activities on the part of the operator. Parents should be able to ascertain the details of who is being given access to their child's data from a centralized location on the school website and/or via an electronic or hard-copy annual notification—as is, for example, required under FERPA for directory information disclosure. This information should be provided by the school, including which online services or products that are given access to their children's personal data, including the written agreement delineating what data elements will be collected and disclosed, how the data will be protected, for what specific educational purpose it will be used, and when the data will be deleted. Expecting parents to traverse the web in search of potentially hundreds of sites of individual operators and without even being told which operators have access to their children's data is neither practicable nor sufficient.

Enhanced data security and breach notification must be required

While § 312.8 has been made more detailed and strengthened, it lacks some important components. While we understand the concern that being overly specific in data security definitions may rapidly become outdated, given the widespread and damaging number of breaches and ransomware attacks on educational data, we would like to see at least minimal safeguards specified, including that:

- data be encrypted at rest and in motion;
- regular independent audits be required;
- the results of such audits be available to parents upon request; and

- parents and schools to be notified of data breaches, within 15 days of the operator and/or the school learning of the breach, and remedies covered by the responsible party.

Without stronger data security there can be no data privacy, nor really any other safeguards against its improper use.

Commercial use of student data by non-profit operators

We acknowledge that the Commission's role in protecting the privacy and security of children's data collected in an educational context is constrained by factors outside of the agency's control. For example COPPA as currently written does not apply to the data of students 13 and older, nor does it apply to the use of student data by non-profit companies. With respect to the latter, we continue to have major concerns with the ability of ostensible non-profit companies that earn millions of dollars per year by directly using student data for commercial purposes, and/or by making it available to for-profit companies with even less regard for student privacy. In the case of non-profits, they as well as their subcontractors should be prohibited from disclosing student data to any for-profit company, without being subject to the same rules concerning prior notification, security safeguards, and use of data only for educational purposes.[12] Otherwise, this would allow the continuation of a huge loophole in the law.

We also understand that the Commission wishes to balance the needs of children and parents, schools and commercial entities. But, given the ever-growing threat to children's privacy, we urge the agency to prioritize children's safety, privacy and well-being over convenience and profit.

Answers to specific questions

Question 2.

As part of the Rule review that led to the 2013 Amendments, the Commission determined that an operator will not be deemed to have "collected" (as that term is defined in the Rule) personal information from a child when it employs technologies reasonably designed to delete all or virtually all personal information input by children before making information publicly available. The Commission is concerned that, if automatic moderation or filtering technologies can be circumvented, reliance on such technologies may not be appropriate in a context where a child is communicating one to one with another person privately, as opposed to posting information online publicly. Should the Commission retain its position that an operator will not be deemed to have "collected" personal information, and therefore does not have to comply with the Rule's requirements, if it employs automated means to delete all or virtually all personal information from one-to-one communications?

[12] The US Department of Education has issued guidance, reminding schools and districts that they must have parental consent before allowing school service providers, including the College Board and ACT, to redisclose their children's personal data. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TA%20College%20Admissions%20Examinations.pdf See also the recent consent decree between the NY AG office and the College Board on the selling of student data at https://ag.ny.gov/press-release/2024/attorney-general-james-and-nysed-commissioner-rosa-secure-750000-college-board

No, this position should not be retained. Even if an operator is employing automated means to delete personal information, whether collected from one-to-one communications or in other situations, this should not be deemed as in compliance with the Rule as an instance where information is not being collected. The consent requirements for collection of data should still apply in this case because an operator must necessarily *hold* data, albeit briefly, *in order* to delete it. Enforcement and confirmation of data deletion is already difficult. It is undesirable to need to stipulate a minimum length of time that data is held in order to be deemed as having been collected. For example, Snapchat, an app regarded by users as one where communications are "instantly" deleted after viewing, in fact may be holding their communications for 24 hours to up to more than 30 days.[13] Moreover, whether or not the information is later to be shared publicly by a service should be irrelevant to whether it is deemed "collected."

Question 3.

The Commission proposes to include mobile telephone numbers within the definition of "online contact information" so long as such information is used only to send text messages. This proposed modification would permit operators to send text messages to parents to initiate obtaining verifiable parental consent. Does allowing operators to contact parents through a text message to obtain verifiable parental consent present security risks to the recipient of the text message, particularly if the parent would need to click on a link provided in the text message?

Yes, not only does sending text messages with links present security risks, but many parents do not have the capacity to read through a consent form on a mobile phone in order to be sure that they understand the ramifications, nor do they have the ability to store any record of that consent form on their phone. We do not support the proposal to expand the options for obtaining verifiable parental consent in this way.

Question 4.

In conjunction with the 2013 Amendments, the Commission acknowledged that screen and user names have increasingly become portable across multiple websites or online services, and that such identifiers permit the direct contact of a specific individual online. Through the 2013 Amendments, the Commission defined personal information to include screen or user names only to the extent these identifiers function in the same way as "online contact information" as the Rule defines that term. Since 2013, the use of screen and user names has proliferated across websites and online services, including on online gaming platforms that allow users to directly engage with each other. The Commission is concerned that children may use the same screen or user name on different sites and services, potentially allowing other users to contact and engage in direct communications with children on another online service. a. Should screen or user names be treated as online contact information, even if the screen or user name does not allow one user to contact another user through the operator's website or online service, when the screen or user name could enable one user to contact another by assuming that the user to be contacted is using the same screen or user name on another website or online service that does allow such contact? b. Are there measures an operator can take to ensure that a screen or user name cannot be used to permit the direct contact of a person online?

[13] "When does Snapchat delete Snaps and Chats?" Snapchat Support. https://help.snapchat.com/hc/en-us/articles/7012334940948-When-does-Snapchat-delete-Snaps-and-Chats

Yes, screen and user names should be treated as contact information, as there is frequent reuse of these across platforms, and many platforms enable searches that make screen or user names discoverable. Operators can prevent searches of screen or user names and should be encouraged to do so, but regardless of whether they are discoverable or not, screen and user names should be deemed to be a type of online contact information.

Question 5.

The Commission proposes adding biometric identifiers such as fingerprints, retina and iris patterns, a DNA sequence, and data derived from voice data, gait data, or facial data to the definition of "personal information." Should the Commission consider including any additional biometric identifier examples to this definition? Are there exceptions to the Rule's requirements that the Commission should consider applying to biometric data, such as exceptions for biometric data that has been promptly deleted?

Biometric data is the most permanent of any unique identifiers, and, due to its unchangeability, it should have the highest levels of control and security. We strongly support inclusion of biometric data under the definition of personal information. We oppose making exceptions for the strong protections that apply to information collected from children in the case of automatic deletion. (See our discussion of automatic deletion in the answer to Question 2 above.)

We also encourage the Commission to expand the list of types of biometric data to include keystroke dynamics, i.e. the individual pattern of typing or entering text on a computer or mobile device, which is unique and identifiable and can be used as identity authentication, similar to the data that can be derived from gait.

In addition, as discussed in detail above, we believe that along with other types of highly sensitive data, there should not be a school-authorization exception for the collection of biometric data. The benefits and risks of using biometric data in schools is under active debate at the state level; see for example the recent decision in New York State to ban use of facial recognition technology in a school security system.[14] We believe parents should retain maximum control over such data—parental notification and consent should be required, and parents should also retain the ability to refuse further collection and have biometric data deleted, all of which has long been the case under the Illinois School Code (105 ILCS 5/10-20.40), as discussed above, demonstrating that this legal requirements are feasible in a school setting.

Question 14.

To effectuate § 312.5(a)(2), which requires operators to give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of the child's personal information to third parties, the Commission proposes requiring operators to obtain separate verifiable parental consent prior to disclosing a child's personal information, unless such disclosure is integral to the nature of the website or online service. Should the Commission implement such a requirement? Should the

[14]"New York bans facial recognition in schools after report finds risks outweigh potential benefits." *Associated Press.* September 27, 2023: https://apnews.com/article/facial-recognition-banned-new-york-schools-ddd35e004254d316beabf70453b1a6a2

consent mechanism for disclosure be offered at a different time and/or place than the mechanism for the underlying collection and use? Is the exception for disclosures that are integral to the nature of the website or online service clear, or should the Commission clarify which disclosures are integral? Should the Rule require operators to state which disclosures are integral to the nature of website or online service?

Consent for collection and use should be distinct and separate from consent for disclosure even in the case of services where disclosure is integral to the nature of the service, e.g. a service where the primary function is to communicate with third parties. Parents (and schools in the case of school-authorized exceptions) should be able to clearly understand that they are issuing both a consent for collection and also a separate consent for disclosure. Even if those two types of consent are acquired via a single communication in time and space with a parent, the parent must be able to consent to collection, but simultaneously withhold consent for disclosure (with the understanding that for services where disclosure is integral to the purpose of the service, withholding consent for disclosure will mean that the service will have limited or no functionality.) Operators should be required to make it clear which if any disclosures are integral to the nature of a site or service.

Question 16

The Commission proposes to include a parental consent exception to permit schools, State educational agencies, and local educational agencies to authorize the collection, use, and disclosure of personal information from students younger than 13 where the data is used for a school-authorized education purpose and no other commercial purpose. What types of services should be covered under a "school-authorized education purpose"? For example, should this include services used to conduct activities not directly related to teaching, such as services used to ensure the safety of students or schools?

Many reports have shown that the surveillance of students in and outside of school by means of spyware installed on their school-owned devices or their personal devices used at home does not increase their safety but instead have had an inordinate stressful impact on students and their freedom to express themselves.[15] As we discussed above, services that collect data from students for surveillance purposes should require parental notification and consent or at the absolute minimum parental notification and opportunity to opt out. We also support the retention of parental rights of refusal of further collection and deletion for surveillance data.

Question 17a.

What efforts are operators taking to comply with § 312.7? Are these efforts taken on a website-wide or online service-wide basis, or are operators imposing efforts on a more granular level?

Operators take few efforts if any to comply with § 312.7. Often there is maximal collection of data even in school services for purposes never explained to educators, families or students. There are numerous reports

[15] See also "Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling." ACLU. October 2, 2023. https://www.aclu.org/publications/digital-dystopia-the-danger-in-buying-what-the-edtech-surveillance-industry-is-selling

of students being tracked elsewhere online or having massive amounts of irrelevant data gathered on them via the use of school-assigned websites.[16]

Question 17b.

Should the Commission specify whether disclosures for particular purposes are reasonably necessary or not reasonably necessary in a particular context? If so, for which purposes and in which contexts?

When programs or services are assigned to students in schools, there should be strict limits on the data collected, and its use should be permitted only for specific educational purposes outlined in the written agreement with the school and deleted when no longer necessary. Specification of what are reasonably necessary disclosures in the Rule may be too narrow to rule out future unreasonable uses, and rather a non-exhaustive list of examples of necessary or unnecessary disclosures would be preferable.

Question 17c.

Given that operators must provide notice and seek verifiable parental consent before collecting personal information, to what extent should the Commission consider the information practices disclosed to the parent in assessing whether information collection is reasonably necessary?

The necessity of information collection is independent of whether there is full disclosure to the parent about information practices, such as how the data will be used, who it will be disclosed to and when it will be deleted. The Commission should restrict operators from making unnecessary data collection from children regardless of how detailed an operators' disclosures are. Data minimization and purpose limitation are important general principles of protecting personal information and separate from notification. Clear and thorough notification, which nonetheless should be required, does not justify collection of unreasonable amounts of data nor using it for unreasonable purposes.

Sincerely,

Leonie Haimson and Cassie Creswell
co-chairs, Parent Coalition for Student Privacy
www.studentprivacymatters.org
info@studentprivacymatters.org

Zephyr Teachout
professor, Fordham Law School

[16]See for example the following: "Facebook Watches Teens Online As They Prep for College." *The Markup.* November 22, 2023. https://themarkup.org/pixel-hunt/2023/11/22/facebook-watches-teens-online-as-they-prep-for-college and "Student Sues Chicago Public Schools Over Naviance Data Use." *Bloomberg Law*. August 21, 2023. https://news.bloomberglaw.com/privacy-and-data-security/chicago-public-schools-sued-by-student-over-naviance-data-use