Cooley

FTC to Focus on Edtech Providers in COPPA Enforcement Push

May 27, 2022

On Thursday, May 19, 2022, the five Federal Trade Commission (FTC) Commissioners unanimously approved a Policy Statement on the Children's Online Privacy Protection Act (COPPA).[1] President Joe Biden issued a statement of support of the FTC decision the same day, highlighting the Policy Statement as a significant step forward on a pledge to protect children's privacy the President made during the State of the Union Address earlier this year.

While COPPA applies generally to operators of a commercial website or online service that collects personal information online from children under the age of 13, the focus of the Policy Statement is primarily on "edtech" companies operating under agreements with K-12 schools. Importantly, the Policy Statement does not change existing requirements; however, it signals a clear FTC intent to enforce those existing requirements more broadly with a focus on edtech.

What is COPPA, and how does it apply to edtech?

COPPA (the statute) and the COPPA Rule (FTC regulation) apply broadly to the collection of personal information[2] by online services directed at children under the age of 13 and by general audience online services when they have actual knowledge that a user is a child under the age of 13. The most well-known requirement of COPPA is that operators subject to its requirements generally must obtain verifiable parental consent before collecting personal information from children. Longstanding FTC staff guidance recognizes an exception to this requirement for services operating in schools – essentially, the school's decision to use the online service obviates the need for the operator to get individual parental consent for school use, provided various requirements are met. For example, as further explained below, the edtech service operator must provide the same notice of its information practices to the school that it otherwise would be required to provide directly to a parent, and it must use information collected from child users only to provide the service requested by the school and not for advertising, marketing or any other commercial purpose. However, this exception extends only to COPPA's notice and consent requirements and not to other operator obligations under COPPA. These other obligations – centering on data minimization and data security – are the primary focus of the FTC Policy Statement (and likely future enforcement efforts).

Does the Policy Statement change the "School Exception" to obtaining individual parental consent?

No. While some privacy and parental rights advocates have targeted the School Exception for significant changes (either through a legislative amendment or FTC rulemaking) it was not changed by this Policy Statement. The standards set out in the FTC FAQ (Section N) remain unchanged.[3] But the Policy Statement makes clear that the FTC intends to aggressively enforce the boundaries of the School Exception. The exception applies *only* to the extent that the data collected is directly related to performing a school function and *only* to the individual parental consent requirement and not to other COPPA requirements regarding data minimization and data security.

What are these other COPPA requirements? Are they new?

The other COPPA requirements are not new but have not historically been the FTC's enforcement focus to the same extent as the consent requirement. The other requirements are:

1. Limitations on data collection
2. Limitations on data use
3. Limitations on data retention
4. Data security requirements

What are COPPA's data collection limitations?

The School Exception to obtaining individual parental consent is narrowly interpreted. It applies only to the collection of personal information that is "reasonably necessary for the child to participate in that [educational] activity."[4] If an operator intends to collect personal information that goes beyond that direct purpose, it must still obtain verifiable parental consent before doing so *and* it may not condition use of the service for the educational activity on obtaining that consent. In other words, companies cannot provide parents with a choice only between not permitting their child to participate in the educational activity or consenting to the additional information collection. A parent must have the option to decline consent to the additional information collection without impacting the child's ability to participate in the educational activity. Note that COPPA's restrictions on mandatory data collection extend to all COPPA-covered operators and not just to edtech providers. The Policy Statement underscores that all COPPA-covered companies must refrain from conditioning participation in any activity on a child disclosing more information than is reasonably necessary for the child to participate in that activity.

What are the data use prohibitions?

Data collected from children in a school activity cannot be used for any commercial purpose "unrelated to the provision of the school-requested online service," including "marketing, advertising, or other commercial purposes." To a large extent, this prohibition mirrors other limitations placed on data collected in schools (regardless of the age of the student) under the Family Educational Rights and Privacy Act (FERPA) and applicable state student privacy laws (such as California's Student Online Personal Information Protection Act and New York's Education Law § 2-d). The key difference is enforcement capability – the FTC, under COPPA, has significantly more enforcement leverage (including harsher penalties) and resources. So, same requirement – but greater likelihood of more severe consequences for noncompliance.

What are the data retention prohibitions?

COPPA strictly prohibits operators from retaining children's personal information for longer than is "reasonably necessary to fulfill the purpose for which it is collected." Notably, operators cannot retain data "for speculative future potential uses."[5] Therefore, operators should have clear and robust data minimization policies that assess direct uses of data and establish timelines for deletion when the direct purpose is fulfilled. This is notably a bit at odds with FERPA obligations, which gives schools control over personal information from student education records (including, at the school's discretion, the ability to retain that data beyond the initial use). From an operator's perspective, this is where clarity in your school agreement is important. To the extent you are retaining data at the direction of a school client, the COPPA risk would appear low – but this should be clear in your agreement. Ensuring robust data deletion requirements are in your school agreement would be beneficial to establish clear destruction protocols.

What are the data security requirements?

COPPA requires that operators "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity" of personal information.[6] While the regulations are not granular about the necessary security requirements, the FTC is clear that it interprets these standards as a high bar and has taken this approach in its enforcement history. As with the other requirements, much of this is duplicative of what is required to contract with schools in most states as new state student privacy laws have been incorporated into those contracts. Most districts now require operators to agree to data privacy agreements that contain robust data security requirements. What is notable is that the FTC is emphasizing that it intends to aggressively enforce these requirements – and that it intends to do so proactively "even absent a breach."[7]

As an edtech company, what should I prioritize?

Again, broadly speaking, nothing has changed regarding edtech provider privacy requirements for operating in K-12 schools. What has changed is the risk of enforcement, particularly by the FTC. The Policy Statement highlights the importance of taking steps that were already good practice:

1. Review your K-12 district contracts. Make sure you comply with the data requirements (collection, use and retention limitations as well as security requirements).
2. Review your Privacy Policy to make sure it is up to date and sufficiently detailed.
3. Review your information security policies and practices to ensure they meet common industry standards and/or identify gaps for remediation as soon as practicable.
4. Implement or review your data minimization policy.
    a. Do you collect only data necessary to provide your services? If you collect more, do you provide parents the ability to decline any additional collection?
    b. Do you have a data retention policy that is aligned with your contractual obligations and minimizing the time data is retained?
    c. Who do you share data with? Do you have commitments from your subcontractors that align with your COPPA obligations? Remember, you may be on the hook contractually or otherwise for the acts of your subcontractors.

Are any Significant COPPA changes expected in the near future?

Good question. The that would seek to modify (or update) the COPPA Rule. That process could have more of an impact on issues like the scope of the School Exception. At the meeting, multiple Commissioners voiced an interest in seeing that process through. There are also multiple bills pending in Congress that would update the COPPA statute. It isn't likely that Congress will pass these bills prior to the midterm election, but they do enjoy bipartisan support.[8]

If you have questions or would like assistance considering how these developments impact you, please reach out.

Notes

1. 15 U.S.C. § 6501-6505

2. Personal Information is broadly defined under COPPA and includes persistent identifiers such as device ID or IP address. See FTC Policy Statement, p. 2.
3. Note that the school exception is set out only in FTC guidance and not, expressly, in the statute or COPPA Rule.
4. See Policy Statement, p. 2
5. See Policy Statement, p. 3
6. 16 C.F.R. § 312.8
7. FTC Policy Statement, p. 3
8. Notably, the **Kids Online Safety Act** sponsored by Sen. Richard Blumenthal (D-CT) and Sen. Marsha Blackburn (R-TN).

Key Contacts

Scott Dailard San Diego	sdailard@cooley.com +1 858 550 6062
Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018