ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

November 17, 2017

VIA Online Submission
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex A)
Washington, DC 20580

Re: Student Privacy and Ed Tech and P175412

Dear Office of the Secretary:

The Electronic Frontier Foundation (EFF) hereby submits these comments in anticipation of the Federal Trade Commission (FTC) and Department of Education's Student Privacy and Ed Tech workshop on December 1, 2017 in Washington, D.C.[1] We do not request confidentiality.

EFF is a non-profit organization based in San Francisco, California, and works to defend civil liberties in the digital world. EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF works to ensure that rights and freedoms are enhanced and protected as the use of technology grows. EFF is especially concerned when students use—and are often required to use—digital services and devices as part of their education without adequate assurances that their privacy will be protected.[2]

We provide comments below reflecting our views on student privacy and ed tech, organized into the following sections: I. EFF Student Privacy Survey, II. Student Privacy Pledge and Unfair/Deceptive Trade Practices, III. Parental Consent Under FERPA and COPPA, IV. Respect for Parents and Good Privacy Practices.

I. EFF Student Privacy Survey

To obtain insight into what is happening on the ground and what challenges students and parents, in particular, are facing related to student privacy and ed tech, we urge the FTC and the Department of Education to read our report from April 2017 entitled *Spying on Students: School-Issued Devices and Student Privacy*.[3]

---

[1] https://www.ftc.gov/news-events/press-releases/2017/10/ftc-department-education-announce-workshop-explore-privacy-issues
[2] *See* EFF's Student Privacy issue page: https://www.eff.org/issues/student-privacy.
[3] *Spying on Students: School-Issued Device and Student Privacy*, EFF (April 2017), https://www.eff.org/wp/school-issued-devices-and-student-privacy.

The report summarizes the findings from a survey we conducted of over 1,000 students, parents, teachers, school administrators, and other community members. While our report's methodology is anecdotal, the volume and tenor of responses we received is illustrative of the scale and scope of ed tech users' concerns. The report includes direct quotes from select respondents that highlight the specific concerns and frustrations related to student privacy and ed tech. The report also provides specific recommendations for school administrators, ed tech companies, and others stakeholders.

Here is a summary of the areas of concern:

1. **Lack of transparency.** Schools issue devices to students without their parents' knowledge and consent. Parents are kept in the dark about what apps their kids are required to use and what data is being collected.

2. **Investigative burden.** With no notice or help from schools, the investigative burden falls on parents and even students to understand the privacy implications of the technology they are using.

3. **Data concerns.** Parents have extensive concerns about student data collection, retention, and sharing. Many ed tech products and services have weak privacy policies.

4. **Lack of choice.** Parents who seek to opt their children out of device or software use face many hurdles, particularly those without the resources to provide their own alternatives.

5. **Overreliance on "privacy by policy."** School staff generally rely on the privacy policies of ed tech companies to ensure student data protection. Parents and students, on the other hand, want concrete evidence that student data is protected in practice as well as in policy.

6. **Need for digital privacy training and education.** Both students and teachers want better training in privacy-conscious technology use.

II. Student Privacy Pledge and Unfair/Deceptive Trade Practices

We urge the FTC and the Department of Education to review the Student Privacy Pledge and investigate whether its signatory companies are following the letter and spirit of the Pledge, in order to ultimately evaluate whether the Pledge is a meaningful tool for students, parents, and school decision-makers who are concerned about student privacy.

The Student Privacy Pledge has over 300 signatories[4] and is comprised of 12 voluntary commitments that the companies have publicly sworn to uphold.[5] The first of these promises is:

[4] Student Privacy Pledge, *Signatories*, https://studentprivacypledge.org/signatories/.
[5] Student Privacy Pledge, https://studentprivacypledge.org/privacy-pledge/.

- *Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.*

We have criticized the Student Privacy Pledge for having narrow definitions that do not meaningfully protect student privacy.[6]

We also filed a complaint with the FTC in December 2015 against Google, urging the Commission to investigate whether Google's ed tech business was engaging in unfair and deceptive trade practices.[7] Google is the major player in the ed tech space: the company's cloud-based suite of apps, G Suite for Education (formerly Google Apps for Education) and its Chromebook laptop account for more than half the market share in K-12 schools.[8]

We alleged in our complaint that Google's collection and use of student data for commercial, non-educational purposes and without parental consent violated the Student Privacy Pledge. **We never heard from the FTC about the complaint.** Sometime after we filed our complaint, Google appeared to change some of its practices: the company claimed it stopped *targeting ads* to K-12 students on non-educational Google services when students were logged into their Google educational accounts.

However, we explained that Google still *collects* data on students, without parental consent, and uses that data for other non-educational purposes (beyond targeted advertising).[9] Such collection and use of student data without parental consent—a practice that Google openly admits to—is an indisputable violation of a plain-English reading of the first promise of the Student Privacy Pledge.

We have received other complaints from parents who believe that signatories are not following the Student Privacy Pledge. For example, the College Board is a signatory, yet it sells student information.[10] While students must opt into the Student Search Service,[11] the relevant

---

[6] *Loopholes and Flaws in the Student Privacy Pledge*, EFF (Oct. 20, 2016), https://www.eff.org/deeplinks/2016/10/loopholes-and-flaws-student-privacy-pledge

[7] *EFF v. Google, Inc., Complaint and Request for Investigation, Injunction, and Other Relief, Before the United States Federal Trade Commission* (Dec. 1, 2015), https://www.eff.org/document/ftc-complaint-google-education.

[8] Natasha Singer, *How Google Took Over the Classroom*, New York Times (May 13, 2017), https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html.

[9] *Google Changes Its Tune When It Comes to Tracking Students*, EFF (Oct. 6, 2016), https://www.eff.org/deeplinks/2016/10/google-changes-its-tune-when-it-comes-tracking-students.

[10] College Board Search, *Pricing & Payment Policies*, https://collegeboardsearch.collegeboard.org/pastudentsrch/support/licensing/pricing-payment-policies.

[11] Student Search Service, *Opt In*, https://cbsearch.collegeboard.org/student-search-service/opt-in.

Pledge commitment has no qualifying clauses; it simply states that signatories will "not sell student personal information."

These examples illustrate that, at worst, companies are flouting the Pledge; and, at best, the meaning of the Pledge's terms are confusing to parents and other stakeholders.

III. Parental Consent Under FERPA and COPPA

We urge the FTC and the Department of Education to ensure that ed tech vendors obtain parental consent to collect and use student data when these companies fail to meet the criteria for being "school officials" under FERPA, or collect data from students under age 13 for commercial purposes under COPPA. We also urge the agencies to work with school districts to ensure that they actively hold ed tech companies accountable for protecting student privacy.

FERPA

Because FERPA generally prohibits school districts from sharing student information with third parties without written parental consent, districts often characterize ed tech companies as "school officials." Districts may only do so if four criteria are met:[12]

- The school district may only share student information without written parental consent with a contractor who has been determined to serve *legitimate educational interests*. A school district must articulate *specific criteria* in its annual notification of FERPA rights and an ed tech contractor must meet those criteria.

- A contractor may receive student information without written parental consent if the company is under the *direct control* of the school district with respect to the use and maintenance of education records. Usually this requires very specific contract terms between the school district and the company.

- A contractor cannot use student information for any *other purpose* than the educational purpose for which it was disclosed by the school district. Again, this usually requires very specific contract terms that limit what data the contractor may collect from students and how it may use that data.

- The contractor must perform an institutional service or function for which the school district would otherwise use employees.

[12] *See* 34 CFR § 99.31; *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, U.S. Dept. of Education, at 4 (Feb. 2014), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

However, in our experience, ed tech vendors often fail to meet these criteria and therefore should be obtaining written parental consent to collect student data. This is because districts often do not provide notice to parents—including by articulating specific criteria—that ed tech vendors have been deemed by the districts to serve legitimate educational interests.

School districts also often fail to exercise direct control over the student data held by ed tech providers, and fail to ensure that contractors are not using student data for commercial, non-educational purposes. Instead, districts often rely on ed tech vendors' Terms of Service or other boilerplate language, without negotiating contract terms that actually protect student privacy.

Google's G Suite for Education is a good example of an ed tech product that should require written parental consent. The G Suite for Education contract summarily states that "Google will be considered a 'School Official'" for FERPA purposes—without reference to the required legal criteria.[13] Additionally, Google does not permit districts access to or control over all the student data they hold, for example, on students' search or YouTube history, despite the fact that this data is directly linked to students' Google educational accounts.

Google also reserves the right to collect and use student data for purposes other than the educational purpose for which it was disclosed by the school district. Specifically, Google may use data collected when students use any Google service—whether the core G Suite for Education apps or when students navigate to non-educational Google services (such as search or YouTube, which Google calls "Additional Services") while logged into their educational accounts—for commercial purposes such as improving Google products. The G Suite for Education Privacy Notice states that Google will use data collected from students' use of all Google services to:[14]

> *provide, maintain, protect and improve them [Google services], to develop new ones, and to protect Google and our users. We also use this information to offer users tailored content, such as more relevant search results. We may combine personal information from one service with information, including personal information, from other Google services.*

We urge the FTC and the Department of Education to find that using student data to "improve" the vendor's products, or to "develop new ones"—especially when not limited to educational products—are purposes other than that for which the student data was provided and therefore requires parental consent.

Contract terms related to notice, data collection, use, retention, access, deletion, etc., must be negotiable and not fixed in boilerplate contract language. This is particularly important if ed tech vendors wish to be deemed "school officials" in order to be exempted from obtaining

---

[13] *G Suite for Education (Online) Agreement* § 7.4, https://gsuite.google.com/intl/en/terms/education_terms.html.
[14] "How we use information we collect," *G Suite for Education Privacy Notice*, https://gsuite.google.com/terms/education_privacy.html.

parental consent. In that case, we believe that FERPA requires providers to follow districts' direction without exception.

COPPA

COPPA requires online service providers to obtain parental consent before collecting personal information from children under age 13 for commercial purposes. Personal information can include traditional personally identifiable information such as a child's name or contact information, as well as online behavioral data, that is, what a child does online.

A key question in the education context is whether a school district can provide consent to collect student data to a company instead of the parents, or whether parental consent must actually be obtained.

We agree with the FTC that a school district should ask, for example: "Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, does it use the students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service?" If the answer to these questions is "yes," the district "cannot consent on behalf of the parent."[15] Similarly, if a vendor intends to use data from students under age 13 for other commercial purposes such as improving its products, parental consent is required because this is not an educational purpose.

Like with FERPA, Google's G Suite for Education is a good example of an ed tech product that should require parental consent under COPPA. As discussed above, Google openly uses student data for their own commercial purposes.[16] And similar to FERPA, Google inappropriately attempts to get around having to obtain parental consent by summarily putting the burden on school districts through contract terms:[17]

> *If Customer [school district] allows End Users [students] under the age of 13 to use the [core G Suite for Education] Services, Customer [school district] consents as required under the Children's Online Privacy Protection Act to the collection and use of personal information in the Services, described in the G Suite for Education Privacy Notice, from such End Users [students]. Customer [school district] will obtain parental consent for the collection and use of personal information in the Additional Services that Customer [school district] allows End Users [students] to access before allowing any End Users [students] under the age of 18 to use those services.*

---

[15] *Complying with COPPA: Frequently Asked Questions*, FTC (March 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[16] "How we use information we collect," *G Suite for Education Privacy Notice*, https://gsuite.google.com/terms/education_privacy.html.

[17] *G Suite for Education (Online) Agreement* § 2.5, https://gsuite.google.com/intl/en/terms/education_terms.html.

We urge the FTC and the Department of Education to find that using data collected from students to "improve" a service, and especially to "develop new" products, are commercial uses under COPPA that require parental consent.

IV. Respect for Parents and Good Privacy Practices

As our student privacy survey shows, parents are extremely frustrated by a lack of notice when their children use new digital apps and devices, lack of transparency around ed tech companies' data practices, and lack of choice—whether that involves opting their child out completely or having their child use alternative digital products and services.[18]

Therefore, even if school districts and ed tech companies technically do not need to obtain parental consent before registering a student for a new online account or issuing them a new mobile device (because the FERPA "school official" criteria are met, or the vendor asserts that it is not using student data for commercial purposes), we recommend that parental consent nevertheless be obtained and alternatives be provided. We believe it comes down to respecting parents and their right to protect their children's privacy—both online and offline.

Additionally, we have heard from parents who have been threatened by school districts with punishment—for example, the lowering of a student's grade—for expressing concerns about their child's digital privacy and withholding consent or seeking choice. This is highly inappropriate and should never happen.

We believe it is incumbent upon school districts to fully understand the data and privacy practices of the ed tech products and services they wish to use, demand that ed tech vendors assent to contract terms that are favorable to the school districts and actually protect student privacy, and be ready *not* to do business with a company who does not engage in robust privacy practices.

While we understand that school budgets are often tight and that technology can actually enhance the learning experience, we urge regulators, school districts, and the ed tech companies themselves to make student privacy a priority.

Very truly yours,
/s/
Nate Cardozo
Sophia Cope
Staff Attorneys
Electronic Frontier Foundation

[18] *Spying on Students: School-Issued Device and Student Privacy, Findings*, EFF (April 2017), https://www.eff.org/wp/school-issued-devices-and-student-privacy#findings.