

Via online submission November 17, 2017:

<https://ftcpublic.commentworks.com/ftc/studentprivacyedtechworkshop/>

U.S. Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

U.S. Department of Education
400 Maryland Ave SW
Washington, DC 20202

To Whom It May Concern,

On behalf of the Software & Information Industry Association (“SIIA”), I write in response to the U.S. Department of Education (“ED”) and U.S. Federal Trade Commission’s (“FTC”) request for comments prior to the workshop on Student Privacy and Ed Tech. We applaud the agencies for holding a joint workshop to discuss how schools and operators work within the scope of the Rule implementing the Children’s Online Privacy Protection Act (“COPPA Rule”) and the Family Educational Rights and Privacy Act (“FERPA”).

As background, the Software & Information Industry Association (SIIA) is the principal trade association for the software and digital information industries representing software companies, data and analytics firms, information service companies, and digital publishers that serve nearly every segment of society, including business, education, government, healthcare and consumers. Members of the Education Technology Industry Network (ETIN) of SIIA work with K-12 schools and institutions of higher education nationwide to develop and deliver education software applications, digital instructional content, online learning services and related technologies.

Educational technology is transforming the classroom improving student engagement and personalized teaching methods while lowering the administrative burden for schools. As a result of responsible deployment of these powerful new tools, in schools of all sizes, resources, and locations, students are collaborating and learning in 21st century classrooms, and teachers and administrators have more time and resources to educate students. SIIA believes that schools are in the best position to decide what learning tools - online or off - are best suited for their students and to decide whether and how student information should be shared with vendors. Schools need to be supported by providers so that they have choices over how to implement services, but they’re ultimately in the driver’s seat when it comes to compliance with regulations such as FERPA and COPPA as they control their student’s data.



I. General Comments on Student Privacy

It is clear that technology and privacy and security must go hand in hand in the classroom and at home. Educational technology providers agree it is necessary to safeguard student privacy: they take their compliance responsibilities seriously and work hard to maintain the trust of their users.

That is one reason 322¹ providers have signed the Student Privacy Pledge² (“pledge”) developed by SIIA and the Future of Privacy Forum (“FPF”). The pledge is built on public commitments regarding the collection, maintenance, and use of student personal information that meet and exceed the federal requirements for student data privacy.

Federal and state activities on student data privacy dramatically increased over the past five years. In 2016 alone, 38 states introduced 112 student privacy bills. Of these proposals, 12 states passed legislation that directly impacts K-12 education service providers. SIIA has worked collaboratively with states and stakeholders over the past several years to find ways to protect the privacy of students across the United States.

At the federal level, we recognize the concerted efforts of policymakers in the Congress to reauthorize FERPA in a holistic manner to align its provisions with the practices of digital and personalized learning, while maintaining the flexibility necessary to spur innovation in educational technology. SIIA continues to engage with members and staff in the House and the Senate as this work progresses.

II. Existing Regulations, Guidance, and Technical Assistance

SIIA appreciates the work both ED and the FTC have done to provide clarity around COPPA and FERPA.

The FTC has taken steps to clarify the operator’s role in protecting a child’s personal information by providing staff-level answers to frequently asked questions³. Additionally, recent FERPA regulations⁴, the later guidance, “Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices⁵,” as well as the best practices

¹ Current as of October 26, 2017

² www.studentprivacypledge.org

³ <https://www.ftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings>

⁴ 34 CFR Part 99

⁵

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf



document, “Protecting Student Privacy While Using Online Educational Services: Model Terms of Services⁶,” have provided significant detail, but sometimes contrasting perspectives, on how online educational services may work in partnership with schools to protect student privacy as required by FERPA.

We look forward to working with ED and the FTC as they take steps to clarify some of the grey areas at the intersection of these two laws. Some of the major areas that could be clarified are outlined below.

III. Relationship between COPPA and FERPA Frameworks

Though there are areas of overlap between COPPA and FERPA, they were written for different purposes and to serve different roles: FERPA to protect, place limitations on unauthorized sharing of, and provide student or parent rights with respect to, specific types of data; COPPA to provide a broader framework providing protections around all aspects of online processing of children’s personal information for commercial purposes. It is important to avoid conflating the definition of education records under FERPA and personal information under COPPA as doing so would create a conflict between the COPPA and FERPA frameworks and sow confusion and uncertainty for schools and providers.

IV. FERPA’s School Official Exception and COPPA

FERPA’s “school official exception” to the written consent requirement allows schools to share FERPA-protected information with relevant and appropriate parties like parent volunteers, board members, or educational technology providers performing institutional services or functions that would otherwise be performed by school employees. Many of our member companies are brought into schools as school officials, often through a negotiated contract or a terms of service agreement, which place limitations on the companies’ collection and use of student data. The “school official exception” has proved to work well for both schools and educational technology providers, and it is of crucial importance for the effective educational technology relationship between schools and vendors.

While the FERPA and COPPA requirements generally interplay well in their practical application, COPPA FAQs M.1. and M.2 create unnecessary confusion about the COPPA consent process in the schools. M.1 states that “schools may act as the parent’s agent and can consent to the collection of kids’ information on the parent’s behalf.” COPPA FAQ M.2

⁶ https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Jan%202015_0%20%281%29.pdf



states that “the operator is not required to obtain consent directly from parents, and can presume that the school’s authorization for the collection of students’ personal information is based upon the school having obtained parents’ consent.” These two FAQs appear to describe different consent processes at the school level. M.2’s consent process places an additional burden on schools, both public and private, to take steps to obtain permission from all parents, rather than consenting “on the parent’s behalf.” This requirement is not mandated by the statute, and creates an unnecessary burden on schools and providers.

We encourage the Federal Trade Commission to clarify this discrepancy either through revised FAQs, or if necessary, execute the rulemaking process to harmonize COPPA with FERPA’s school official exception to clarify that a school may consent to the collection of a child’s information on a parent’s behalf, as outlined in M.1 in the COPPA FAQ. Additionally, as noted above, the FTC should clarify that the right provided by COPPA for a parent to access, review, and have a child’s personal information deleted resides with the entity providing consent. If the school provides consent under COPPA, the remaining rights should also reside with the school. This would harmonize COPPA’s consent process with FERPA’s school official exception which would lessen the burden on schools and technology companies dedicated to improving educational outcomes for students. It would also harmonize the COPPA rights of parents with the FERPA rights of parents, in having both requests for access to review, amend, correct, and in the case of COPPA, delete records, flow through the school. This would further ensure that schools would be working closely with parents to maintain an accurate and adequate education record for each child as mandated by the states, and not result in confusion and a fragmented record when requests to delete information flow directly from the parent to the operator without input from the school.

V. Direct Control

FERPA’s direct control requirement ensures that schools do not improperly disclose information to a “school official” without the proper controls in place. FERPA’s school official exception requires a party acting as the school official to be under the direct control of the school with respect to the use and maintenance of education records. This requirement is generally met through a written agreement, such as a negotiated contract or a terms of service agreement, which outlines how a school maintains direct control and places limitations on vendors’ ability to collect, use, and maintain data about students.

Recent state laws⁷ have put additional requirements on educational technology companies when it comes to the use and maintenance of education records. The majority of contracts

⁷ http://blogs.edweek.org/edweek/DigitalEducation/2014/09/_landmark_student-data-privacy.html



between schools and educational technology companies reflect state-specific requirements in addition to federal privacy requirements. Educational technology companies honor and comply with all requirements set forth in agreements with schools.

ED's 2015 document, "Protecting Student Privacy While Using Online Educational Services: Model Terms of Service," illustrates some best practices for contracts that schools and vendors may employ to protect student privacy. We welcome updates from ED to this document to outline best practices for establishing direct control as required by FERPA's school official exception.

VI. Conclusion

Thank you for the opportunity to provide comment on this important issue. SIIA and its member companies shares the commitments of ED and the FTC to protect student privacy inside and outside of the classroom while providing transformative technologies that power new educational opportunities for schools, parents, and students. If you have any questions about these comments or would like to discuss further, please contact David LeDuc, Senior Director of Public Policy, at dleduc@siaa.net or 202-789-4443.

Sincerely yours,

Mark MacCarthy
Senior Vice President for Public Policy