


Three Laws That Protect Students' Online Data and Privacy

 0 .AS POGGI JUNE 25, 2019 IN EDTECH / FEATURED

As a child moves through his education stages, from K-12 and on to college or a trade school, at each and every step that child and its family engage with technology.

Whether it's a computer lab at the local elementary school, a homework assignment that must be submitted online or a collaborative, Cloud-based platform

that enables teachers and parents to interact, the education environment is a technology environment.

After school, students are immersed in technology too. Many students have their own cell phones or, at least, access to a home or public computer. They text each other, post to their Instagram accounts, or tag along in popular online games, such as Fortnite or Minecraft to pass the time.

With every keystroke done in school devices or through platforms monitored by them, children provide their schools, and other organizations with data that may or may not be protected by federal and state laws. Consequently, all data a student generates is bound to be at risk, from their behavior on a school's online platform that might be inadvertently tracked by the vendor, to their educational records.

What Laws Protect These Students' Data?

In the United States, three laws have been enacted to uphold student privacy and data security: the Family Education Rights & Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Children's Internet Protection Act (CIPA). Each is administered by different branches of the federal government, and each seeks to police possible cyber dangers to minors. There are also many state-level laws, but for now, we'll focus on the big three.

FERPA: Family Educational Rights and Privacy Act

Administered by the Department of Education, [The Family Educational Rights and Privacy Act \(FERPA\)](#) was enacted in 1974 specifically to protect the privacy of education records. It gives parents rights to those records but transfers those rights to the student when he or she reaches 18 years of age.

The Department of Education maintains a site, "[Protecting Student Privacy](#)," with information that explains what best practices every educational stakeholder — from students, to parents, to teachers, vendors, and researchers — must adopt in order to manage student data while still maintaining student privacy.

The Dept. of Education's FERPA Video "[Student Privacy 101](#)" is a good place to find out more about this law.

COPPA: Children's Online Privacy Protection Act

The [Children's Online Privacy Protection Act \(COPPA\)](#) of 1998 falls under the jurisdiction of the Federal Trade Commission. Unlike FERPA, which focuses on

student rights, COPPA regulates how website operators or online services can collect personal information from children under 13 years of age.

The FTC's COPPA Rule includes a "safe harbor" provision designed to encourage increased industry self-regulation in this area. Under this provision, industry groups and others may ask the Commission to approve self-regulatory guidelines that implement the protections of the Rule. Companies that comply with the FTC-approved guidelines receive safe harbor from agency enforcement action under the Rule.

Congress has updated COPPA many times since it was implemented in 1998. Most recently, the FTC sought and won permission to modify the law's self-regulating program for the video game industry.

To learn more, take a look at the FTC summary pdf [Protecting Children's Privacy Under COPPA](#).

CIPA: Children's Internet Protection Act

The third big federal law protecting children is the [Children's Internet Protection Act \(CIPA\)](#) of 2000, which is concerned with children's access to the obscene or harmful Internet. This law requires schools and libraries participating in the E-rate discount program CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the FCC's E-rate program.

A promotional graphic for the Prey application. The background is dark blue. On the left, white and light blue text reads: "Stay on top of you 1:1 program like a pro". Below this, in smaller white text: "Streamline your school's device management and automate security." At the bottom left is a white button with the text "TRY IT FOR FREE" and the Prey logo, which consists of a stylized bird icon and the word "PREY". On the right side, there is a stylized illustration of a person in a dark shirt and light blue pants, holding a laptop and reaching up to place a large white arrow pointing upwards, which has the number "1" inside it. The entire graphic is set against a dark blue background with some light blue cloud-like shapes.

With CIPA, schools and libraries must be able to prove that they have an Internet safety policy in order to obtain E-rate discounts. These protections must include either blocking or filtering online content that is either obscene, child pornography, or harmful to minors. In order to demonstrate compliance, these schools and libraries must publicize their compliance policies and hold at least one public meeting.

In addition, schools must also have a provision to monitor online activities of minors and, per the 2012 Protecting Children in the 21st Century Act, must educate these same minors on how to act online. Their education curriculum must encompass appropriate online interactions on social networking, in chat rooms, as well as cyberbullying and response.

You can find out more about CIPA or apply for E-rate funding by contacting the Universal Service Administrative Company's (USAC) Schools and Libraries Division (SLD)

Or, you can print out read this PDF: [Children's Internet Protection Act \(CIPA\)](#)

Takeaways

This patchwork of three laws administered respectively by the Department of Education, the Federal Communications Commission and the Federal Trade Commission, seeks to monitor and protect students in schools and in the commercial marketplace.

All educational shareholders, from the institution's management stakeholders to the students and their parents would do well to familiarize themselves with these laws and make sure that they, or their schools, are in compliance.

[CIPA] [COPPA] [FERPA] [PRIVACY] [STUDENT PRIVACY]

NICOLAS POGGI



Nicolas Poggi is the head of mobile research at Prey, Inc., provider of the open source Prey Anti-Theft software protecting eight million mobile devices. Nic's work explores technology innovations within the mobile marketplace, and their impact upon security. Nic also serves as Prey's communications manager, overseeing the company's brand and content creation. Nic is a technology and contemporary culture journalist and author, and before joining Prey held positions as head of indie coverage at TheGameFanatics, and as FM radio host and interviewer at IndieAir.



Previous Post

4 Ways to Protect Your Phone's Data From Unwanted Tracking

[Next Post](#)[Data Encryption 101: A Guide to Data Security Best Practices](#)

RELATED POSTS



The Student Awareness Kit: Making Students More Security Savvy

BY NICOLAS POGGI JULY 9, 2019 0



Data Encryption 101: A Guide to Data Security Best Practices

BY HUGH TAYLOR JULY 1, 2019



a blog by Prey inc. [back to top](#) ^

[Home](#) [Get Prey](#) [Features](#) [Business](#) [Personal](#) [Privacy Policies](#) [Terms & Conditions](#)