“FTC Would Get New Enforcement Powers Over Ed Tech in Data-Privacy Bill”

By Sean Cavanagh
Education Week
April 29, 2015

After an extended delay prompted by sharp criticism from privacy advocates, new federal legislation aimed at better protecting students' sensitive information is likely to be introduced in the U.S. House this week.

The bill, sponsored by Rep. Jared Polis, D-Colo., and Rep. Luke Messer, R-Ind., and developed with involvement from the White House, would prohibit ed-tech vendors from selling student data or using that information to target students with advertisements. The bill would also require vendors to meet new requirements related to data security, breach notification, and contracts with third parties. Perhaps most significantly, the Federal Trade Commission would be granted enforcement and regulatory authority over the burgeoning ed-tech industry, including the right to impose penalties on bad actors.

The revamped "Student Digital Privacy and Parental Rights Act of 2015," a near-final copy of which was obtained by Education Week, would also take steps to close perceived loopholes in an earlier draft that had been set for formal introduction in March.

"My sense is this new version has important improvements," said Joel Reidenberg, a Fordham University law professor and privacy expert. "The strides are in expanding the scope of children's information that is covered, more clearly articulating permissible uses of [such] information, and adding important security requirements and transparency features."

All told, the bill, if enacted, would significantly expand the federal government's role in efforts to protect students' sensitive information. Over the past 18 months, the issue has emerged as a legislative priority in statehouses and now Congress, largely due to the rapid expansion of the $8 billion-per-year ed-tech industry and corresponding concerns among parents and privacy watchdogs.

A bipartisan overhaul of the country's primary current student-privacy law, the Family Educational Rights and Privacy Act, is also under consideration. A discussion draft that would dramatically rewrite FERPA is being circulated for feedback, although there is no timetable for a final version of that bill to be introduced in Congress.

Closing loopholes

The politics surrounding the federal government's involvement in student-data-privacy issues have proven tricky.

Last month, a version of the Student Digital Privacy and Parental Rights Act was supposed to be introduced in the U.S. House, but critical media reports ignited concerns from parents, educators, and advocates who blasted the bill as too industry-friendly.

Reps. Polis and Messer delayed the bill's introduction in order to solicit more input from privacy advocates and the education community.
Those efforts seem to have resulted in meaningful changes.

Gone from the previous draft of the bill are provisions that many feared would make it too easy for vendors to sell student information to post-secondary institutions and employers and obtain consent to violate their own privacy policies. Also eliminated is a provision—considered to be overly broad by many in the privacy community—that would have allowed teachers and school officials (a technical term that often includes vendors) to identify for themselves what constitutes a legitimate educational use of a student’s information.

Added into the revised bill is language that would expand the definition of "covered information" to be protected by law to include the metadata and other information that students generate when using vendors’ products. Also new are requirements that vendors publicly identify any third parties to whom they disclose student information and delete student information within one year of ceasing to provide services to the student or his or her educational institution. The revised bill would also require vendors to take "reasonable steps" to ensure that anonymous and aggregated student information they disclose cannot be linked back to individual students.

"We're really encouraged to see the congressmen and their staffs working hard to try to get this right," said Joni Lupovitz, the vice president for policy at Common Sense Media, a San Francisco-based nonprofit that has been actively pushing for strong student-data-privacy legislation at both the state and federal levels.

**A new federal approach**

While there has been much haggling over key legislative details, the broad principles of the Student Digital Privacy and Parental Rights Act remain consistent.

In the biggest shift from current practice, the new federal bill would specifically address educational technology vendors, rather than schools, districts, and states.

Targeted advertising to students by ed-tech operators would be prohibited, as would collecting, generating, or disclosing student information for such purposes. Vendors would be prohibited from using "covered information"—including personally identifiable data such as name, address, online contact information, biometric record, social security number, and "persistent identifiers" that recognize individual users across different web sites—to build a profile of students for non-educational purposes.

Vendors would also be subject to a host of new federal requirements.

For one, they would be required to "establish, implement, and maintain reasonable security procedures" needed to protect any covered student information they may hold.

If they were to disclose such information to a third party (say, a subcontractor), vendors would also be required to get that third party to agree in writing to not use the information for any new purposes, to not disclose the information to anyone else, and to maintain reasonable security procedures.

In the event of a data breach, ed-tech vendors would also be bound to notify, at a minimum, the FTC.
They would also be required to delete most of a student's covered information within 45 days of receiving a request from an educational institution or a parent, and within one year of ceasing to provide its services to the educational institution or student in question.

And vendors would also be required to "disclose publicly...in a manner that is clear and easy to understand, the types of covered information collected or generated" by their service or product, as well as "the purposes for which the covered information is used or disclosed to third parties" and "the identity of any such party."

**Not trumping the states**

The Student Digital Privacy and Parental Rights Act is intended as a floor, establishing a minimum level of protection for student data that is uniform across the nation.

States would still be free to enact and enforce laws that offer stronger protections. Student-data-privacy has remained a hot legislative issue at that level, with almost 200 bills being introduced so far this year, according to the Data Quality Campaign, a Washington-based nonprofit.

The likelihood of the new federal bill's passage is difficult to ascertain until it is formally introduced.

That could happen as early as Wednesday, although the sensitivity of the bill—and its sponsors' difficult recent experience—could conceivably lead to further delays.