EdWeek Market Brief

Market Trends

Aug. 1, 2016

As States Toughen Data-Privacy Laws, Ed-Tech Providers Adjust

Policies Vary, But Vendors Could Face Decisions on Pricing, Marketing Strategy

Tam Harbert
Contributing Writer

The last three years have produced a tidal wave of state laws aimed at protecting student-data privacy, policies that lay out out how ed-tech vendors can, and cannot, use such data. Many providers are still gauging how those policies will affect their products and influence their strategies for working with schools.

Privacy advocates say the laws are almost certain to affect companies' pricing, product development, and contracts with districts. And ed-tech providers that adjust quickly to

the new landscape will likely have a competitive leg up.

But the full weight of the new laws on K-12 companies has yet to be felt, partly because implementation of the laws is playing out slowly in many states and districts.

Many vendors recognize that change is coming, though most are circumspect when asked if they have changed, or plan to change, their products and policies in response to the laws.

"I'm not certain that ed-tech vendors are fully aware of the impact," said Holly M. Hawkins, the chief safety and privacy officer at the Internet Keep Safe Coalition, or iKeepSafe.org. The nonprofit group, which advocates for data privacy and Internet safety, has launched a program that assesses vendors for compliance with state and federal privacy laws and regulations. *(See sidebar.)*

"The vendors I'm dealing with want to do the right thing," she said, "and the majority of them think they are in compliance. ... But I've not seen an ed-tech vendor yet that has truly been fully compliant."

Demands Vary by State

Since 2013, 34 states have approved new laws on student-data privacy, according to Rachel Anderson, the associate director of federal policy and advocacy at the Data Quality Campaign, a Washington-based group.

And overall interest in student-data privacy nationwide has mushroomed, with 47 states considering 186 different bills last year, and 34 states weighing 113 pieces of legislation this year.

The new laws place greater compliance responsibility on vendors, said Michael L. Whitener, a partner at VLP Law Group LLP, which has several ed-tech clients. Under the federal Family Educational Rights and Privacy Act, or FERPA, schools are primarily responsible for compliance. In cases where schools are not in tune with the law, the government can withhold or rescind funding, but it more commonly works with schools to bring them into compliance.

By contrast, many of the new state laws hold vendors responsible for compliance, and are enforceable by the attorneys general in different states.

"Now, for the first time ever, the attorney general can say to a company, 'We want to check your data-privacy practices,' " said Marsali Hancock, the president and CEO of iKeepsafe.org. "That never happened before."

Many of the laws require that vendors' privacy policies be included in their contracts, so a school district could take legal action if those policies were violated.

Most of the laws follow the model set by California's Student Online Personal Information Protection Act, or SOPIPA, which took effect at the start of this year. In general, SOPIPA prohibits vendors from knowingly engaging in targeted advertising to students or parents, creating a profile of a student based on data collected, selling student information, and disclosing certain student data, except under special circumstances.

Yet the states' laws also differ significantly. For example, SOPIPA applies to all vendors whether or not they have a contract with a school, but some state laws apply only to those with contracts, said Anderson. So the same vendor might fall under the law in one state but not in another.

What constitutes adequate security requirements can vary from one state to the next. SOPIPA requires vendors to

Tougher Privacy Laws to Spawn Compliance-Assessment Services?

As new laws on student-data privacy proliferate, third-party consultants could emerge to assess whether ed-tech products are meeting stricter state and local requirements.

One organization that is already taking on that work is the **Internet Keep Safe Coalition**, or **iKeepSafe.org**, a nonprofit based in San Jose, Calif.

The group offers three types of assessments: one for compliance with FERPA; one for the Children's Online Privacy Protection Act, or COPPA; and one that includes FERPA, COPPA and the California state law SOPIPA and related requirements – a tool it launched late last year.

The goal is to help both schools and vendors to meet the requirements of the new laws, said Holly M. Hawkins, the chief safety and privacy officer at iKeepSafe.org.

Schools typically don't have the resources to identify all the vendors and whether they meet the state laws. Under the iKeepSafe program, the vendor answers a series of questions about data-collection and -security procedures, privacy policies, and contracts. The organization then puts the product through its paces, probing for any discrepancies.

maintain reasonable security, but the Delaware law sets up specific, detailed security requirements, said Whitener. SOPIPA also includes a provision that allows ed-tech providers to include recommendation engines—a product feature that uses data on student performance to tailor lessons to their classroom needs. Other state laws do not allow those tools, according to Anderson.

One of the most recently enacted state laws, Colorado's Student Data Transparency and Security Act, is particularly strict. It stipulates that a vendor is responsible not only for protecting student data in its own product, but also when the data are used by third parties it does business with. And the law ensures that any vendor that violates its provisions will be publicly identified.

Under the Colorado law, schools are required to maintain and publish lists on their websites of all vendors that handle students' personally identifiable information, including a copy of each contract. A parent who has evidence that a vendor is not abiding by its privacy policies or is falling short of the law's requirements can trigger a public hearing by the school board, which could then result in cancellation of the contract.

"We look at whether the privacy policy actually reflects the way the product performs," said Hawkins. "Perhaps they overlooked something, and there was a function that performed just a little bit differently than what the text of the privacy policy said."

IKeepSafe.org works with ed-tech providers under nondisclosure agreements, so any problems with a product's safeguards on data privacy are kept under wraps. If a vendor does not meet all requirements, iKeepSafe works with it to bring it into compliance, said Hawkins.

Upon successful completion, the vendor receives a product profile with all the data and can display a California Student Privacy Badge. The product profile answers all the questions that most schools will ask about privacy and security, thus saving time for both vendors and schools.

As of July, five vendors had successfully completed the SOPIPA assessment, said Hawkins. Although compliance with SOPIPA likely means vendors will be in compliance with laws in many other states, iKeepSafe.org is in the process of identifying differences in state laws and may broaden its assessment to include them, said Hawkins.

Colorado schools also must publish lists of vendors they have dropped, along with the reasons for doing so and the vendors' written responses.

“To my knowledge, this is the first time that’s been done, the first time there is a public acknowledgment that a school has stopped using the vendor for a negative reason,” said Hawkins of iKeepSafe.org.

A number of ed-tech providers, in response to questions from *EdWeek Market Brief*, were vague in describing how new state laws would shape their business practices.

Knewton, which sells adaptive learning technology, said in a statement that students remain anonymous in its system, and that it doesn’t collect any personally identifiable information about them. The company also said that its partners “market, sell, and deploy [adaptive learning products] into the classroom. As part of that engagement process, our partners ensure compliance with all applicable laws.”

Trickle-Down Changes

Brendan Desetti, the director of education policy at the Software and Information Industry Association, said he hasn’t seen vendors change their products in reaction to the new state laws. They are, however, reviewing their privacy policies to make sure they’re clear and specific about what information they collect, why they collect it, and whom they share it with and why, he said.

He pointed out that more than 270 companies have signed on to the Student Privacy Pledge, which the SIIA and the Future of Privacy Forum launched in 2014. The forum is a think tank that says it advocates responsible data-privacy practices and seeks to bring together industry officials, advocates, regulators, and others on privacy issues.

One of the signatories to the pledge is Texthelp. The company has taken several steps in the past two years to ensure it is in compliance with not only state laws, but also individual data-security agreements that school districts often require, said Martin McKay, the founder and CTO.

Texthelp does not store any personally identifiable information, and what information it does store is both encrypted and de-identified, he said. In 2014, in response to increasing concern in states and districts over student-data privacy, the company put in place policies on data security and privacy that include regular security audits and training to make sure developers used security best practices when writing software.

One reason vendors haven't felt the full impact of the new laws may be that the provisions haven't trickled down to affect industry practices yet. Many of the laws will affect schools and districts first. Some laws, such as Colorado's, require school boards to develop detailed data-governance policies, privacy protocols, and security audits, for example. Colorado's law also requires schools to know what products are being used—information they may not know without conducting extensive research.

"Currently, if you ask districts about all the tech products that have access to student data, they can't tell you," Hancock said. "They haven't had a culture where they've had to keep track."

Colorado districts are now working to identify and list all the vendors they use, said Andrew Moore, the CIO of the Boulder Valley school system.

"When school starts, we'll survey the teachers about the apps they are using in classrooms," he said. "I anticipate a significant amount of work through the first school year, and then the law said we have to update that twice a year, because the terms change."

Once schools have catalogued products and put security procedures in place, they will be able to hold vendors accountable, Hancock said.

With Privacy Changes, Pricing Changes?

Texthelp is already complying with the requirements of individual school districts, which can vary significantly and can be stricter than state law, said McKay, the company's founder.

"These individual agreements are increasing in number and becoming more and more onerous," he said.

The new laws, and perhaps the individual agreements between vendors and districts, could shape ed-tech companies' pricing to K-12 clients. If companies are depending on revenue from selling student data or using the information for marketing, that revenue could evaporate, Whitener of the VLP Law Group said.

The state laws "are much more restrictive in what [vendors] can do, even with de-identified or anonymized data," he said.

Other vendors, meanwhile, could raise prices because of the added costs, such as having to hire consultants to conduct security audits of software or hire lawyers to review privacy policies.

In other cases, new laws also could force "freemium" vendors to charge for a subscription or leave the education market if they depend on advertising for their revenue, Whitener said.

Yet there's a potential bright side for vendors. Those that meet tougher state and local standards may have a competitive advantage. In fact, the best approach for vendors may be to meet the requirements of the most-restrictive state laws, so they cover all their bases.

Andy Bloom, the chief privacy office for McGraw-Hill Education, said his company is poised to hit the mark.

"We build our privacy program based on a standard that meets all the state requirements, rather than trying to address each independently," Bloom said in a statement. "While we certainly verify that our policies comply with applicable laws, we do not operate to any one particular law."

See also:

- Data-Privacy Expectations Likely to Influence District Purchasing
- ESSA's "Innovative Assessment Pilot": What K-12 Businesses Should Expect
- Nation's 6th-Largest District Leapfrogs RFP Process for LMS Purchase
- Rising K-12 Interest in Software-as-a-Service Brings Changes to Market

---

Tags: Ed-tech, student data privacy

Tam Harbert
Contributing Writer

Tam Harbert is a contributing writer for *EdWeek Market Brief*.

tam@tamharbert.com @tamharbert LinkedIn

6935 Arlington Road, Bethesda MD 20814 - 1-800-346-1834