EdWeek Market Brief

Analyst's View

March 16, 2018

Learning From the 'Accidental Consequences' of Student-Data-Privacy Laws

Experts Trying to Help Ed-Tech Companies Navigate the Twists and Turns of State Measures

Michele Molnar
Associate Editor

Forty states have passed 124 laws since 2013 to protect the privacy of students' data, and more than 600 bills have been introduced.

How can ed-tech companies avoid becoming collateral damage in the unintended consequences of these laws?

Amelia Vance, policy counsel at the Future of Privacy Forum, led a panel discussion on the accidental consequences of privacy laws at the SXSWedu conference in Austin recently and weighed in on the topic herself.

EdWeek Market Brief Associate Editor Michele Molnar attended the session in Austin and interviewed Vance afterward to learn what general advice she has for ed-tech companies trying to address the difficult challenges of data privacy. The following draws information from both the public event and that conversation. It has been edited for brevity and clarity.

About This Analyst

Amelia Vance is the director of the Education Privacy Project and a policy counsel at the Future of Privacy Forum. She leads the organization's work to ensure the responsible use of student data and education technology in schools, convening school districts, state and federal policymakers, companies, and privacy advocates to develop and share best practices and resources. Prior to FPF, Vance was the director of the Education Data & Technology Project at the National Association of State Boards of Education. Vance is a member of the International Association of Privacy Professionals and the Virginia State Bar.

How is it that 40 states could pass 124 laws on student data privacy? That averages three laws per state.

We've seen a lot of states go back and usually expand upon—but also, occasionally fix—their laws. New Hampshire had an unintended consequence around video recordings in the classroom. Their original law required school board, student, parent and teacher sign-off before any video could be recorded of a student in the classroom. The problem was that the law was very vague, and it restricted the ability of New Hampshire teachers to be certified—which is based on videos of them teaching in the classroom. The law also did not make exceptions for students with IEPs (Individualized Education Programs) that required video recordings of their classes. [Legislators] went back and fixed the IEP part of the law the next year. But not the teacher certification issue.

What states should companies look to for "best practices" around privacy governance?

Resources for Ed-Tech Providers

Georgia and Louisiana are two that we mentioned in our session. Some states have learned from, and built upon, the successes of their neighbors. We started out with California's SOPIPA. [The Student Online Personal Information Protection Act applies to websites, applications and online services that provide programs or services for K-12 students.]

That law was pretty good, but it didn't have a definition of what targeted advertising is. Subsequent versions [in other states] did. We have SOPIPA 2.0 in Texas and Illinois, which passed a law last year. I think we're up to around 20 states. SOPIPA is most useful for companies. [The Future Privacy Forum has created a 38-page SOPIPA guide for K-12 administrators and ed-tech vendors.] This convergence can help companies.

California still hasn't defined "targeted advertising." How do you see that playing out?

We're a little worried. The AG's [Attorney General's] office did put out best practices guidance but did not address targeted advertising. The legislature did not give them the regulatory authority to interpret the law. They just have enforcement power. Either the legislature will have to clarify this, or at some point, the AG's office will bring a case against a company and that definition will be decided by a judge.

The Future of Privacy Forum maintains the FerpaSherpa website, an education privacy resource center named after the Family Educational Rights and Privacy Act, the core federal law governing education privacy.

Beyond that, the following data privacy resources for companies selling products into the K-12 market can be useful:

- StudentPrivacy.ed.gov has model terms of service and runs a hotline where "a person will pick up the phone and talk to you," said Amelia Vance, the director of the Education Privacy Project and a policy counsel at the Future of Privacy Forum. It is operated by the U.S. Department of Education's Privacy Technical Assistance Center and the Family Policy Compliance Office.
- Polisis is a new, free tool, powered by machine learning, that automatically produces charts to help a users understand where the data for any online service ends up. Privacy policies from some ed-tech companies are in its database, and any company's URL can be uploaded to it.
- The National Conference of State Legislatures surveyed the student data landscape in 2017, and raised policy questions for states to consider.
- Louisiana's Data Governance and Student Privacy Guidebook is, Vance said, one of the best in the country.

As of today, 330 companies have signed the Student Privacy Pledge, which is a list of 12 commitments school service providers make to keep K-12 student information private and secure. FPF oversees it. How many applications do you have from companies interested in taking the pledge?

As of December 1, we have 51 applicants. Any company can apply to be part of the pledge. We will look at their privacy policy for free to make sure they're in compliance. The vast majority do go back and forth with us. It's not necessarily because they're doing anything problematic, but because we have a lot of smaller and new companies. Their lawyers have copied and pasted their privacy policies from somewhere that doesn't necessarily match their business model.

> Sometimes we deal with clauses that are just vague. When the privacy policy has to also serve as a way to build trust with your clients, being vague does not serve your company.

Where do companies typically go wrong in their contract language?

A lot of it is just that this is a hard area to write for. Lawyers who aren't familiar with it sometimes use cookie-cutter policies. The aim of their policies is to cover their liability as much as possible and allow them to do things in the future that they [the companies] don't know yet that they want to do. That's problematic when it comes to the pledge, which requires data only be used for educational purposes. A privacy policy is not just a legal document for ed-tech companies. It's also where districts, educators, and parents will go to learn more about the company and see whether they're able to trust them.

What can make an educator, a district, or a parent mistrust a privacy policy?

Sometimes we deal with clauses that are just vague. When the privacy policy has to also serve as a way to build trust with your clients, being vague does not serve your

company. Not stating things specifically can be an issue. The pledge requires that, before any material changes are made to the privacy policy, you have to offer notice… so schools can choose to remove data if they want. Being specific in how they [companies] do that is important. It's important to look at it through a community lens, as well as a legal liability lens

Another panelist talked about developing "whitelists" of companies that meet student data privacy criteria. Is that a trend in districts and states?

It's certainly something we've started to see, and something I continually hear the state educational agencies I've worked with asking about. People are wary of it because products could change at any time. They'd have to stay on top of re-evaluating new versions—and their privacy policies. I think more people are going toward a contractual model where they have a company bound to a certain set of privacy terms, whether the product changes or not.

Follow EdWeek Market Brief on Twitter @EdMarketBrief or connect with us on LinkedIn.

See also:

- Privacy Advocates Brace for Shakeup at U.S. Education Department
- How Companies Can Fix Ambiguous Privacy Policies
- 'Unified Contract' Designed to Help Districts, Companies Comply With California Law
- As States Toughen Data-Privacy Laws, Ed-Tech Providers Adjust
- Student-Data Privacy: How Parents' Views Can Shape K-12 Companies' Work
- Provider of 'Connected Toys' Vtech Settles Federal Privacy Complaint
- New Data-Privacy Realities Forcing Companies to Adjust
- State Lawmakers Balance Concerns On Student-Data Privacy

Image by Getty

Tags: Data Privacy, Federal/State Policy, Future of Privacy Forum

Michele Molnar
Associate Editor

Michele Molnar is associate editor of *EdWeek Market Brief*. She is also a reporter who covers industry and innovation for *Education Week*. Michele began working as a contributing writer for *Education Week* in 2012, covering parents' influence on education. She joined the staff in 2013 to write about the intersection of education and business in the pre-K-12 marketplace.

mmolnar@epe.org @EdWeekMMolnar LinkedIn