March 27, 2015

Student privacy has become a focal point in the education sector. While media attention has largely focused on activities in Washington, we believe it is also critical for schools and Ed Tech companies to pay closer attention to privacy and security actions at the state level.

Recap of recent federal student privacy initiatives

Earlier this week, Representatives Luke Messer (R-IN) and Jared Polis (D-CO) unveiled legislation focused on student data privacy. The bill, developed in coordination with the White House and some industry stakeholders, has been in the works for many months. The bill, which is based on Student Online Personal Information Protection Act ("SOPIPA"), a California law enacted last year, would apply to third parties that "operate" websites, online services, or mobile applications designed or marketed for K-12 school purposes and would limit the ability of those entities to use, disclose or sell the information they collect for targeted advertising or other commercial purposes.

The Messer/Polis bill would provide more flexibility for online service providers than does SOPIPA. Most notably, the bill would permit disclosures "pursuant to a request" by a student or parent if the disclosure is "in furtherance of postsecondary education or employment opportunities." This bill, like the White House's draft Consumer Privacy Bill of Rights Act that was released in February, has received a lot of attention (and criticism); but, as with the Consumer Privacy Bill of Rights Act, the legislative path forward for Messer/Polis remains uncertain and we believe it likely represents more of a "marker" in the ongoing student privacy debate than a viable new law.

While the Messer/Polis bill deals only with K-12 concerns, we expect congressional activity around the student privacy issue will pick up in the higher education sector as well. Congress must reauthorize the Higher Education Act ("HEA"), which is overdue for renewal , and the House and the Senate may also look to amend the Family Educational Rights and Privacy Act ("FERPA"), a nearly 40-year-old law that governs student (or parent) access to information and the disclosure of student personally identifiable information to third parties. While the likelihood of passing comprehensive legislation in the current DC climate seems small, there is the prospect of at least some bipartisan agreement on certain aspects of student data privacy over the next year, particularly in the context of larger debates about federal education policy.

On the regulatory side, a potentially impactful privacy action may have occurred last month, without much fanfare, when the Department of Education released a "Model Terms of Service" that provides a list of "best practices" language (as well as language to avoid) for agreements between schools and online service providers. The Model Terms of Service is only guidance and does not change the legal requirements under FERPA or other federal laws. However, while some of the recommended terms align with FERPA, others go beyond the legal requirements. While the Model Terms of Service are nominally geared toward K-12 schools, most of the focal points are also applicable to higher education institutions. The guidance provides a useful tool for addressing key privacy issues in contracts and terms of service, but schools and providers should both carefully consider what terms will best suit their goals and needs in any individual agreement.

Meanwhile, states governments are not waiting for Washington

While gridlock may continue to be the story in Washington, this is not the case in state legislatures. In 2014, 110 student privacy

bills were introduced in 36 states and 21 states enacted student data privacy laws. In just three months, 2015 has seen more privacy bills introduced than all of 2014. Already 138 bills have been introduced in 39 states. Some laws, including the landmark California law, SOPPIPA, discussed in more detail below, apply only to those in the K-12 space while other laws also apply to entities in the postsecondary space. The laws that have been enacted have their unique aspects; however, a few general themes have appeared. The laws tend to break down into three categories: (1) Security; (2) Transparency; and (3) Use.

Security laws focus on how student data is stored, retained, accessed, and destroyed or returned. Common provisions require the establishment of minimum data security standards, policies on the retention or destruction of information, and monitoring and notification of security breaches. While many such laws are technology-neutral, some are more prescriptive.

Transparency laws focus on how schools and Ed Tech companies notify students or parents regarding how they may collect, use, disclose, or sell student data (and with whom). They often deal with such questions as "How are the disclosures made?" and "Are terms of service or policies subject to amendment without a school's prior consent?"

Use laws focus on limiting or prohibiting schools or companies from collecting, using, disclosing, and/or selling student data (possibly regardless of transparency or parental/student consent). These limits could restrict disclosure to certain entities or for certain purposes. The California law – SOPIPA – is the prime example of this type of law and strictly limits commercial use of student data. Another area of debate focuses on the use of "de-identified" data. At what point is data reasonably considered de-identified? If it is de-identified, are additional uses permissible?

SOPIPA – A model for other states?

While SOPIPA was far from the only privacy law enacted last year, it was probably the most significant. What is most notable about SOPIPA is that it broadly applies to websites, online services providers, mobile application providers, and other third parties that provide services focused on K-12 students. These entities have direct liability under the law (unlike FERPA where the liability is generally indirect). And SOPIPA applies to such entities even if they are not based in California as long as their services are used in California. Another interesting aspect is that SOPIPA does not provide any consent mechanism whereby students or parents can "opt-in" to certain uses or disclosures of their information.

With its broad application – to any service known to be used for K-12 purposes in California (the most populous state in the country and one of the ten largest economies in the world) –SOPIPA may soon establish a "de facto" national standard, just as California Senate Bill 1386 did for data breach notification when it went into effect in 2003. Additionally, California is unlikely to be alone for long. Already in 2015, legislatures in at least ten states have introduced, or will soon introduce, bills that are similar to or nearly identical to SOPIPA.

SOPIPA shows why state actions are likely more relevant to student privacy law at this point. In fact, Messer/Polis specifically does not preempt state law. California's law (and any similar state laws) would be more restrictive than the current federal proposal. And, of course, the federal proposal faces long odds of ever becoming law.

This means that, at least in the near term, student data privacy requirements will vary by state and may sometimes be contradictory. Any entity seeking to operate across state lines will need to have the administrative systems in place to comply with multiple sets of standards that are rapidly changing.

Conclusions

While the debate in Congress will continue to play a significant role in the national dialogue on student data privacy, the more concrete impact in the near term is likely to be at the state level. The laws in this area are changing rapidly and staying on top of the requirements will be critical to long term success in the educational space. Our Education practice group works closely with our

Privacy & Data Protection practice group to closely track these developments. Please contact any members of our team to find out more.

NOTES

1. The HEA was last reauthorized in 2008 through the Higher Education Opportunity Act. It was set to expire in 2013 and has continued via temporary extensions since that time.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090