October 1, 2015

While Congress continues to consider (but not act on) nationwide student data privacy initiatives, the states continued to lead the charge in 2015. Earlier this year, **we reported** that, in 2014, 36 states introduced 110 student data privacy bills and 21 states passed new student data privacy laws. The final numbers for 2015 are now in, and the pace is largely unchanged. In fact, according to numerous reports, legislatures in 46 states (all but Nebraska, Pennsylvania, Vermont, and Wisconsin) considered student data privacy bills this year (182 bills in total).

Nearly half of the legislatures considered bills based, at least in part, on the California Student Online Personal Information Protection Act ("SOPIPA") which essentially established a national student data privacy standard for ed tech companies operating in the K-12 space when it was passed last fall. SOPIPA becomes effective in January 2016 and our detailed analysis of SOPIPA is **here**.

Fifteen states passed student data privacy bills and quite a few (including Georgia, Maryland, Oregon, and Washington) passed comprehensive bills based on the California law. Notably, however, it appears that legislatures are listening to the concerns of the ed tech industry that were raised in the wake of SOPIPA. The laws that were passed in 2015 tended to address some of the major concerns companies have had about the workability of SOPIPA. For example, SOPIPA was unclear or ambiguous about many critical issues such as what services are covered, obtaining parent consent, and how the law will be enforced. While some advocacy groups have been critical of what they see as a watering down of SOPIPA, many of the laws passed this year provide more certainty and clarity for the companies subject to them (for example, limiting the covered entities to those with contracts with a school or district, as the Maryland law does). This debate will continue as more states consider these bills. Provisions that create certainty for an ed tech company can also be seen as creating a loophole in the view of a parent or advocacy group (as well as schools).

Another interesting development was in Nevada where a new student data privacy law requires school districts to develop policies regarding the use of ed tech products by individual teachers. Such policies could restrict or limit the ability of teachers to use products that do not meet certain data privacy standards as well as the use of "freemium" products (those that are free for basic services, but charge for premium services) under certain conditions. District initiatives to establish internal policies regarding the use of third party technologies in the classroom are becoming increasingly common.

The pace of these changes—and the intricacies of the differences between various state requirements—requires both schools and ed tech companies to reconsider student data privacy as a priority.

Practice tips

For ed tech companies

- Ensure that your product and practices conform to the student data privacy laws of the states where you operate and continue to monitor the changing landscape. This is critical when companies are first starting out. Few things are as damaging as finding out down the road that schools in California (or any state) are prohibited from using your product or service.
- Keep your privacy policy and terms of service updated to match your current practice. These documents form the agreement between you and your client (including on issues such as liability and dispute resolution). Don't limit your ability to enforce those

policies.

- Consider your contractual and marketing practices in light of the importance schools (and parents) are placing on student data privacy.

For schools (K-12 and postsecondary)

- Establish an internal student data privacy policy and procedure that is aligned with the relevant state laws.
- Develop a procedure for assessing (and keeping track of) the technologies and products that are being used in your classrooms and have a process for ensuring compliance with your internal policy.
- Review your contractual arrangements with third parties for compliance with federal and state student privacy laws.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. This content may be considered **Attorney Advertising** and is subject to our **legal notices**.

Key Contacts

Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.