New student data privacy laws: top points for school contractors and K-12 education sites, apps and online services

Data Protection, Privacy and Security Alert

6 JAN 2015
By: Jim Halpert

According to the Data Quality Campaign, 36 states considered 110 student data privacy bills this year, and 20 states enacted 28 such bills into law. **At least eight** of these new laws **may have significant implications for businesses that provide services involving student data** to schools, and **most** of these laws have **already taken effect**.

Some of the new laws regulate the use of student data. For example, a new law in Idaho (Idaho Code § 33-133) prohibits private vendors from using student data for any secondary purpose, such as sales, marketing or advertising. A new law in Kentucky (Ky. Rev. Stat. § 365.734) regulates cloud service providers, imposing on them a somewhat confusing prohibition against processing student data for any commercial purpose.

In addition to limitations on the *use* of student data, many states sought to include security provisions in contracts with service providers. New York (N.Y. Educ. Law § 2-D), enacted in response to parental concerns about inBloom, prohibits the use of student and teacher personally identifiable information for marketing purposes – and also contains very prescriptive requirements regarding security. Among other things, this law requires data systems monitoring, data encryption, incident response plans, limitations on access to personally identifiable information, safeguards to protect personally identifiable information transmitted over communication networks, and destruction of personally identifiable information when no longer needed. This includes a rigid requirement to encrypt student data in line with the encryption requirements of the federal Health Insurance Portability and Accountability Act (HIPAA) (N.Y. Educ. Law § 2-D(5)(f)(5)).

Other states also require security provisions in agreements between schools and vendors, but those states were generally less prescriptive. A new law in Colorado (Col. Rev. Stat. § 22-2-309) requires that contracts with private vendors (i) include express provisions that safeguard privacy and security; (ii) specify that personally identifiable data may only be used for the purpose specified in the contract; and (iii) prohibit further disclosure of such data for commercial purposes. A new Louisiana law (La. Rev. Stat. § 17:3913) will require contractors to agree to minimum security requirements, including privacy and security audits; information storage, retention and disposition policies; and breach planning, notification and remediation procedures. Finally, a new law in North Carolina (N.C. Gen. Stat. § 115C-402.5) requires that any contracts with private entities include express provisions that safeguard privacy and security and include penalties for noncompliance.

CALIFORNIA STUDENT DATA PRIVACY AND SECURITY LAWS

Two California bills signed into law in September impose privacy and security requirements. California S.B. 1177, known as the Student Online Personal Information Protection Act (SOPIPA), imposes rigorous rules on operators of websites or providers of Internet services or mobile applications with actual knowledge that the services are used primarily for "K-12 school purposes" and were designed and marketed for K–12 school purposes. Among other things, it prohibits the use of student data for targeted advertising on the website, service or app and the sale of student data. Operators of educational online services must also implement and maintain reasonable security procedures and practices, as well as protect that student data from unauthorized access, destruction, use, modification, or disclosure. "Operator" is broadly defined as any service provider whose services are *primarily* used for K-12 educational purposes and designed and marketed for K-12 school purposes. S.B. 1177 goes into effect on January 1, 2016.

California A.B. 1584 requires that contracts between a school district and third parties specify, among other things, that the student data remains the property of the educational agency; how students and parents may access their data; how the third party will ensure the confidentiality and security of student data; and how to notify students and parents in the event of a security breach. A.B. 1584 goes into effect on January 1, 2015.

IMPLICATIONS FOR VENDOR AGREEMENTS

Some of the new state student privacy laws specifically require that contracts with vendors include clauses that address the requirements of the new state law. The process of incorporating these privacy and security requirements into school district vendor agreements that come up for renewal is likely to be gradual.

However, in most cases, the new state law will be ***directly applicable to vendors*** whether or not the contract warns them of the new requirements. Service providers to state and local educational institutions should therefore be proactive and check to be sure that their data usage and security practices are in compliance with the newly enacted student data privacy laws in the states in which they operate.

Here are some steps that educational service providers who receive K-12 student data can take to anticipate contractual requirements:

- **Talk to your business and marketing teams** to understand how your organization uses K-12 student data that it receives by virtue of contracts with public schools and state and local education agencies as well as other entities with whom your organization shares or provides access to student, and to understand the purpose for doing so. Also discuss with your IT team how it secures student data.
- **Align your policies to the specific state requirements** for the states where you receive student data from K-12 schools, including typically restricting the use of student data for marketing or advertising purposes. Consider ways to enable different use restrictions for student data obtained from different states, while bearing in mind that regulation is likely to spread to other states.
- **Inventory existing agreements with your own service providers** who have received or have access to K-12 student data from your organization and **amend such agreements as practicable** and where required by applicable state laws to include provisions about security and privacy, data retention, data access and obligations regarding security incidents.

IMPLICATIONS FOR OPERATORS OF K-12 EDUCATIONAL WEBSITES, ONLINE SERVICES AND MOBILE APPS

In addition to being subject to the contractor requirements described above, K-12 educational websites, online services and apps **will be subject to further privacy requirements when SOPIPA takes effect in 2016**. These requirements include (i) not using K-12 student data for marketing, profiling, or targeted advertising purposes; (ii) providing parents with access to the student data, where practicable to do so; and (iii) securing student data. (In a drafting error, the law on its face also applies to information about school employees and administrators obtained by an operator from an employee or administrator.)

While SOPIPA's requirements are quite similar to those in state contractor K-12 student privacy laws, it is important to understand that (1) the requirements apply regardless of whether a K-12 site, online service or app has a contract with a school and in addition to the contractor requirements; (2) they apply in addition to federal Children's Online Privacy Protection Act (COPPA) requirements; and (3) unlike under COPPA, SOPIPA's requirements cannot

be avoided by targeting a school-age audience that is age 13 and older.

In anticipation of SOPIPA's taking effect at the start of 2016, sites, online services and apps that are directed at a K-12 school student audience should consider:

- Reviewing their data practices against the requirements and exceptions in S.B. 1177, particularly the prohibitions against use of data for marketing and profiling and the parental access requirement and

- Inventorying existing agreements with their own service providers who receive or have access to K-12 student data from the organization and amend these agreements as practicable to include provisions restricting use of the data by services providers and addressing security, data retention, data access, and obligations regarding security incidents.

LOOKING AHEAD: GET READY FOR EVEN MORE STATE-LEVEL LEGISLATION

The hectic trend of enacting student data privacy legislation at the state level is likely to continue throughout 2015. Organizations that provide educational services and thereby obtain student data should continue to monitor legislative developments – including implementing regulations – and prepare themselves for requirements in even more states.

To learn more about the implications of these rapid changes for your business, please contact the authors.

AUTHORS

Jim Halpert
Partner
Washington, DC | T: +1 202 799 4000
jim.halpert@dlapiper.com