Schools and Digital Education Technologies

by Khizar A. Sheikh and Kimberly Goldberg

The cloud, mobile apps, social media, SaaS—these are all digital technologies people knew nothing about until recently. Today, these and other digital technologies are being used by schools and their vendors to handle a growing number of functions.[1]

EdTech, as these digital technologies are known when related to education, holds promise for schools because of its potential to lower costs and help students learn more effectively. EdTech also, however, raises legal and regulatory questions. Schools are transferring sensitive student data to EdTech vendors, sometimes across state and international borders, without written agreements governing the transactions, and/or without parental knowledge or consent.[2] Parents are frustrated by a seeming lack of transparency about how their children's personal data are being used.[3]

While federal and state laws do exist to protect student data, both schools and vendors appear uncertain about the application of these laws to EdTech,[4] and some policymakers have argued that the current legal framework has not kept up with new technologies.[5]

This article focuses on a subset of the privacy challenges K-12 schools face, namely the privacy and data security compliance risks involved in the transfer and use of student data to EdTech vendors by schools and local school districts.[6]

The Federal and State Legal Framework

There are a number of federal and state laws that govern the collection, storage, and use of student data.

Family Education Rights and Privacy Act of 1974 (FERPA)[7]

FERPA applies to any school that receives federal funding, and imposes compliance requirements around a student's right to inspect, amend, and control disclosure of personally identifiable information (PII) from "education records."[8] Education records include information that is "directly related to the student" and maintained by a school or a party acting for the school, such as student files, grades, and disciplinary records.[9] Data from education records that have been completely de-identified is not considered PII.[10]

FERPA prohibits a school from disclosing PII[11] from an education record to anyone, including a vendor, without a parent's prior written consent. There are several exceptions, two of which are:[12]

- *The Directory Information Exception.* A school may disclose, without prior written consent, certain "directory information" to a vendor "that would not generally be considered harmful or an invasion of privacy if disclosed," so long as the school gives parents prior notice of the disclosure and a reasonable amount of time to opt out.[13] Directory information includes name, address, telephone number, date and place of birth, and in some cases a student ID.[14]
- *The School Official Exception.* A school may disclose PII without prior consent if a vendor performs a function that otherwise would be performed by a school employee, has a legitimate educational interest in that data, and the school directly controls the vendor's use and maintenance of the data.[15] Under this exception, the vendor can use the PII only for an authorized purpose and cannot re-disclose the data unless it has permission from the school and only in accordance with FERPA.[16]

Schools that fail to comply with FERPA may forfeit their federal funding.

Protection of Pupil Rights Amendment of 1978 (PPRA)[17]

FERPA deals with records maintained by a school. The PPRA governs the administration of surveys soliciting specific categories of information, and imposes certain requirements regarding the collection and use of student information for marketing purposes.[18]

The PPRA requires schools to notify, and provide an opt-

out opportunity to, parents when students are scheduled to participate in commercial activities involving the collection, disclosure, or use of student information for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes.[19] However, the PPRA does not apply when a vendor is using student data exclusively for the purposes of developing, evaluating, or providing educational products or services for students or a school.[20]

There is no private right of action under the PPRA, but school federal funding may be jeopardized.[21]

The Children's Online Privacy Protection Act (COPPA)[22]

COPPA requires commercial website operators (including EdTech vendors that may operate educational websites) to obtain "verifiable parental consent" before collecting PII from children under the age of 13.[23] Where a vendor has contracted with a school to collect PII from its students for the use and benefit of the school, and for no other commercial purpose, the website operator may rely on the school as an intermediary for obtaining parental consent.

Schools, however, must be careful regarding the student information that is subject to this law, which may be different than the information regulated by FERPA or the PPRA. COPPA was recently revised to expand the definition of PII to include geo-location information, photographs, videos and audio files, user names, and online 'cookies.'[24]

Operators who violate COPPA can be liable for civil penalties of up to $16,000 per violation. Recent Federal Trade Commission enforcement actions have resulted in fines from $50,000 to $3 million.

State Law

Several states have passed their own FERPA-type statutes,[25] and several states are considering measures to address transparency about data collection, anonymization, and restrictions around commercial use.[26]

A number of states have laws that mirror or extend the survey provisions of the PPRA, including Arizona, Arkansas, Colorado, New Mexico, and New Jersey.[27]

At least two state attorneys general (including New Jersey's) have used their enforcement powers to sue companies for COPPA violations.[28] California recently passed its own version of COPPA, which requires a mechanism for minors under 18 to "erase" their public social media posts.[29]

Future Legislation

There has been recent federal activity regarding student data privacy, including the issue of private companies managing student data. In Jan. 2014, Senator Ed Markey (D-Mass.) announced plans to introduce legislation regarding student data privacy, with requirements that include prohibitions on student data ever being used for commercial purposes.[30]

Practical Steps for Schools to be in Compliance

The above laws were enacted because of concerns over the collection and use of sensitive information about students by private parties. As education data is digitized, the need to exercise care in the handling of personal information has intensified. When outsourcing school functions, schools must ensure that vendors and service providers are properly protecting student information.

In order to comply with federal and state laws in this area, schools, at a minimum, should adhere to the following privacy, security, and transparency best practices:

1. Be aware of the EdTech vendors being used in the school district.
2. Determine whether the information provided to EdTech vendors is protected by federal, state, or local law.
3. Have the right policies and procedures to evaluate and approve vendors.
4. Determine the legal requirements regarding information disclosure. For example, if a school seeks to disclose student information under FERPA's directory exception, it must publish a public notice indicating the specific elements or categories of directory information it intends to disclose, and also honor and maintain student opt-outs. If a school seeks to disclose information under FERPA's school official exception, it must determine whether an EdTech vendor meets the criteria for being a school official with a "legitimate educational interest," and must restrict the EdTech vendor from using the PII for unauthorized purposes.[31]
5. When disclosing student information, be mindful of access rights. A school must log all requests for access to and all disclosures of education records, and must retain the ability to respond to parent requests for access within 45 days.[32] This means a vendor must provide the school with a mechanism for providing parents either direct or indirect access to a student's records maintained by the vendor.[33]
6. Enter into a written agreement with the vendor that specifies the data to be accessed; memorializes the vendor's assurance regarding security and data stewardship, collection, data use, retention, disclosure, destruction, data access, modification, duration, termination, limitations of liability, indemnification for third-party claims, and warranties; verifies the vendor's training and discipline procedures for compliance violations; and grants the school

audit rights over the vendor's privacy, data security, and compliance practices.[34]

7. Endeavor to collect and use the least amount of data necessary and anonymize data when practicable.
8. Be transparent with parents, teachers and the public about their policies and relationships with vendors.

Conclusion

Regulatory or civil actions undoubtedly would cause distraction and disruption to already over-burdened and under-resourced school institutions. Furthermore, with federal and state lawmakers and the public focusing on student data privacy, new laws with more onerous penalties may be on the horizon.

In this rapidly evolving environment, EdTech vendors must meet schools halfway by offering compliant products and entering into the appropriate contracts. Ultimately, however, schools are the stewards of student data, and can no longer blindly adopt EdTech offerings without understanding the implications for student data privacy. Institutions that are able to implement best practices will not only be in compliance with existing law, but will have defensible contracts and procedures in place to weather the increasing scrutiny from both legislators and the public.

Endnotes

1. These functions include replacing onsite servers with cloud-based information systems; storing student and school data such as personal information, student grades, teacher feedback, attendance, health and immunization information, and state-mandated reporting requirements; collaborating/emailing between teachers and students; planning lessons; creating online courses; networking on social media; assessing student and teacher performance; and even planning bus routes. For a recent paper that tries to inventory the state of current cloud-based EdTech, *see* Isaac Meister, *et al.*, K-12EdTech Cloud Service Inventory, Jan. 15, 2014, viewed at cyber.law.harvard.edu/node/8717.
2. According to a recent study by the Center for Law and Information Policy at Fordham Law School, 95 percent of school districts surveyed are using cloud-based services, but many have either no, or inadequate, documentation. *See* Joel Reidenberg, *et al.*, Privacy and Cloud Computing in Public Schools, viewed at ir.lawnet.fordham.edu/clip/2.
3. Deciding Who Sees Student Data, Oct. 5, 2013, *New York Times*, viewed at nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html.
4. Reidenberg, *supra* note 2.
5. *See, e.g.*, letter from Senator Edward Markey to U.S. Secretary of Education Arne Duncan, dated Oct. 2, 2013, viewed at markey.senate.gov/documents/2013-10-22_FERPA.pdf.
6. The transfer and use of student data by federal or state education agencies and their representatives is treated differently under current law, and is outside the scope of this article. In addition, schools face other compliance challenges around student searches, speech/conduct regulation, and anti-bullying, to name a few.
7. *See* 20 U.S.C. § 1232g; 34 C.F.R. Part 99.
8. Until the student is 18, the FERPA grants these rights to the parent.
9. *See* 34 C.F.R. § 99.3. *See Owasso Independent School Dist. v. Falvo*, 534 U.S. 426, 434-436 (2002) (holding that a peer-graded test is not an education record because it was not maintained by the school).
10. *See* Privacy Technical Assistance Center of the U.S. Department of Education, Protecting Student Privacy while Using Online Education Services: Requirements and Best Practices (PTAC Guidance), available at ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services; Reidenberg, *supra* note 2, p. 6.
11. The FERPA defines PII as any (i) direct identifiers such as name, address, date of birth, social security number; (ii) indirect identifiers such as a parent name, mother's maiden name, Social Security number; and (iii) any other information that could reasonably identify a student when used alone or in combination with other information. *See* 34 C.F.R. § 99.3.
12. *See* 12 U.S.C. 1232g. Other exceptions include the audit and evaluation exception and the studies exception, both of which have different requirements and would apply to data analytics functions performed by school boards and state education authorities. *See* 20 U.S.C. §§ 1232g(b)(1)(C), (b)(3), (b)(5) and (F), and 34 C.F.R. §§ 99.31(a)(3), (6) and 99.35.
13. *See* 20 U.S.C. 1232g(b)(5)(A); 34 C.F.R. § 99.37.
14. *See* 34 C.F.R. § 99.3.
15. *See* 20 U.S.C. § 1232g(b); 34 C.F.R. § 99.31(a)(1).
16. *See* 34 C.F.R. § 99.31(a)(1). For example, upon a school's request a vendor may use student data it has already collected to create a new product for that school, but the vendor would not be allowed to use the data to directly market products to students or to develop a new product without the school's authorization.
17. *See* 20 U.S.C. § 1232h; 34 C.F.R. Part 98.
18. For a detailed discussion of com-

mercial activity in schools, *see* GAO Report on Commercial Activities in Schools, p. 5 (Aug. 2004), viewed at gao.gov/assets/250/243777.pdf.

19. *See* 20 U.S.C. § 1232h(b), (c).
20. *See* 20 U.S.C. § 1232(c)(4).
21. *See* 20 U.S.C. § 1232h(e).
22. *See* 15 U.S.C. §§ 6501-06; 16 C.F.R. Part 312.
23. *See* 15 U.S.C. §§ 6501-02.
24. *See* 16 C.F.R. § 312.2 (revised Dec. 19, 2012, effective July 1, 2013).
25. *See, e.g.,* Oklahoma Student Data Accessibility, Transparency and Accountability Act, House Bill 1989; Nebraska LB 262; Arizona SB 1450.
26. *See, e.g.,* California's proposed Student Online Personal Information Protection Act, S.B. No. 1177; *see also* Scrutiny in California for Software in Schools, Feb. 14, 2014, *New York Times*, viewed at nytimes.com /2014/02/20/technology/scrutiny-in-california-for-software-in-schools.html; Adrienne Liu, Dec. 17, 2013.
27. *See* N.J.S.A. 18A:36-34. *See also* GAO Report on Commercial Activities in Schools, *supra* note 18.
28. *See* New Jersey Attorney General Press Release, June 6, 2012, available at nj.gov/oag/newsreleases12/pr20120606a.html; Texas Attorney General Press Release, 12/5/07, available at oag.state.tx.us/oagnews/release.php?id=2288.
29. Privacy Rights for California Minors in the Digital World, Calif. S.B. 568.
30. Senator Edward Markey Press Release, Jan. 14, 2014, available at markey.senate.gov/news/press-releases/markey-to-introduce-legislation-to-protect-student-privacy.
31. *See* 34 C.F.R. § 99.31.
32. *See* 34 C.F.R. § 99.32.
33. *See* PTAC Guidance, *supra* note 10.
34. *See* PTAC Guidance, *supra* note 10; 34 C.F.R. § 99.31(a)(1)(ii).

Khizar A. Sheikh *is a partner at Mandelbaum Salsburg, and chair of the firm's privacy and information management practice group.* ***Kimberly Goldberg*** *is the founder and principal of the Goldberg Law Firm and is a certified privacy professional.*