Re: Student Privacy and Ed Tech and P175412

November 17, 2017

Comment by:

Douglas Levin, President
EdTech Strategies, LLC
5507 24th St North
Arlington, VA 22205
dlevin@edtechstrategies.com
www.edtechstrategies.com

Emerging Data and Issues Related to the Security of Student Data

As the announcement of the joint FTC-ED workshop acknowledges, the embrace of technology by U.S. elementary and secondary schools has been near universal and continues to evolve rapidly. While these technologies have tremendous potential, it is appropriate to revisit how the Rule implementing the Children's Online Privacy Protection Act ("COPPA Rule") applies in the school context, and how it intersects with the Family Educational Rights and Privacy Act ("FERPA"). While there are many important issues at the intersection of the COPPA Rule and FERPA, I would like to focus on the narrow, but critically important issue of student data security. These issues relate to one specific question to be addressed at the workshop ("How should requirements concerning notice, deletion, and retention of records be handled and by whom and when?"), although their implications are potentially much broader.

First, there is an emerging knowledge base on cybersecurity incidents involving schools and student data that should be used to guide decisionmaking. In March 2017, EdTech Strategies launched the K-12 Cyber Incident Map (https://www.edtechstrategies.com/map) in an effort to address an information gap in the knowledge base about the sufficiency of school (and, by extension, school vendor) cybersecurity policies and practices.[1] It remains the only freely available, up-to-date source of data on the prevalence and nature of school cyber incidents, including of breaches and exfiltrations of student data. With data covering incidents from January 2016 to present, it has cataloged 237 incidents

1 See "Introducing the K-12 Cyber Incident Map" (published March 30, 2017) online at: https://www.edtechstrategies.com/blog/introducing-the-k-12-cyber-incident-map/; Chang, Richard. "EdTech Strategies Publishes K–12 Cyber Incident Map." *THE Journal*. 31 March, 2017. Available online at: https://thejournal.com/articles/2017/03/31/ed-tech-strategies-publishes-k12-cyber-incident-map.aspx

to date (which corresponds to more than 2 incidents per week on average). While not every incident on the Map represents a student data breach, taken together they suggest pervasive weaknesses in school and school vendor information security practices.

Since January 2016, the K-12 Cyber Incident Map has documented student data breaches, unauthorized disclosures of student data, and cyberattacks resulting in the exfiltration of student data in dozens of public schools and districts, including:

- Nazareth Area School District (PA)
- Poway Unified School District (CA)
- Lewis-Palmer School District 38 (CO)
- Northside Independent School District (TX)
- Ruben S. Ayala High School (CA)
- Hilliard Bradley High School (OH)
- Detroit Edison Public School Academy (MI)
- Frederick County Public Schools (MD)
- Robbinsdale Area Schools (MN)
- South Washington County Schools (MN) (*2 incidents*)
- Chicago Public Schools (IL) (*2 incidents*)
- Hanks High School (TX)
- Corpus Christi Independent School District (TX)
- Katy Independent School District (TX)
- Upper Arlington Schools (OH)
- Abingdon-Avon CUSD #276 (IL)
- West Bloomfield School District (MI)
- Montgomery County Public Schools (MD)
- Lovejoy Elementary School (IA)
- District of Columbia Public Schools (DC)
- Troy City School District (NY)
- New Dorp High School (NY)
- Spring Branch Independent School District (TX)
- Palo Alto Unifed School District (CA)
- Confluence Charter Schools (MO)
- Munday Consolidated Independent School District (TX)
- Hamilton Central School (NY)
- Spencerport Central School District (NY)
- Williamson County Schools (TN)
- Mt. Diablo Unified School District (CA)
- Fairfield Public Schools (CT)
- Niskayuna Central School District (NY)
- Mammoth High School (CA)
- Tryon Elementary School (NC)
- Miami-Dade County Public Schools (FL)
- American Senior High School (FL)
- Seminole High School (FL)
- Columbia Falls Schools District (MT)
- Splendora Independent School District (TX)
- Johnston Community School District (IA)
- Palo Alto High School (CA)

These incidents – surely an undercount given variable breach notification requirements across states – have involved the unauthorized disclosure of tens of thousands of student records, sometimes including highly sensitive personal information. In a few cases, the same school district has been responsible for a student data breach more than one time since 2016 alone. And, some of the most high profile breaches of student data have garnered national news coverage in outlets such as the Wall Street

Journal, NBC Nightly News, and National Public Radio.[2] (Of note, there also have been data breaches of millions of student records by school vendors Edmodo[3] and Schoolzilla[4] over this same time period.)

Current rules and guidelines relating to schools' care of digital student records are insufficient. Actors, both internal and external to schools, are routinely demonstrating through breaches and hacks that school information security practices are lacking.

Second, parents and taxpayers should expect uniformity in student data breach reporting and remedies across schools, states, and technology providers. The K-12 Cyber Incident Map assembles data on school incidents primarily via news reports, which are supplemented by data published by others (including DataBreaches.net, The Privacy Rights Clearinghouse, and The Identity Theft Resource Center). Nonetheless, the dataset underlying the Map is undeniably incomplete and may contain errors. Neither school districts nor their vendors are compelled to make public disclosures of every potentially significant incident (if required at all by state data breach notification laws[5]), and media reports can be short and ambiguous.

Students and/or their parents, as appropriate, deserve to be informed in a timely manner of unauthorized disclosures of students' personal information (no matter the source or reason), of the nature of those disclosures, of how the responsible parties are remediating any deficiencies that led to the unauthorized disclosure, and of the remedies available to them (including of credit monitoring). Minimum standards for disclosures and remedies – such as the length of free credit monitoring – should be established via federal regulation (ensuring that the federal government does not preempt any state or local law or policy that may be more stringent).

A secondary benefit that such a uniform reporting requirement could spur is increased information sharing within and across states and school vendors of cybersecurity vulnerabilities facing schools. Absent a reliable and up-to-date data source on demonstrated threats to student data security, it is difficult to prioritize scarce public resources toward effective deterrents. Data from the K-12 Cyber Incident Map also clearly shows that cyberattacks against schools are often repeated on target after target. By promptly sharing information on student data security vulnerabilities in school or school

2 See, e.g., Gosk, Stephanie, Melnick, Michelle, and Newcomb, Alyssa. "Criminals make student data public in escalating demands for ransom." *NBC News*. 15 November 2017. Available online at: https://www.nbcnews.com/tech/security/criminals-make-student-data-public-escalating-demands-ransom-n821066; Hobbs, Tawnell D. "Hackers Target Nation's Schools." *Wall Street Journal*. 23 October 2017. Available online at: https://www.wsj.com/articles/hackers-target-nations-schools-1508751002; WNYC. "Hackers Target Student Data as Schools Report Increasing Cyberattacks." *The Takeaway*. 24 October 2017. Available online at: https://www.wnyc.org/story/hackers-target-student-data-schools-report-increasing-cyberattacks/

3 See, e.g., Cox, Joseph. "Hacker Steals Millions of User Account Details from Education Platform Edmodo." *Motherboard*. 11 May 2017. Available online at: https://motherboard.vice.com/en_us/article/ezjbwe/hacker-steals-millions-of-user-account-details-from-education-platform-edmodo

4 See, e.g., Cameron, Dell. "1.3 million K-12 students exposed by now-secured data breach." *The Daily Dot*. April 20, 2017. Available online at: https://www.dailydot.com/layer8/1-3-million-american-students-exposed-data-breach-now-secured/

5 A compilation of information about state data breach laws can be found at: https://www.databreaches.net/state-breach-notification-laws/

vendor IT systems, school district technology leaders can take prompt action to reduce the effectiveness of copycat attacks.

Third, liability and penalties for negligent student data security practices must be assignable and enforceable. The ability to appropriately and accurately assign responsibility for student data breaches is fundamental to any enforcement actions. Such actions should carry liability and penalties sufficient to encouraging schools and school vendors to take student data security more seriously. While penalties may involve monetary fines, they also could include mandatory training (or re-training), third-party audits of the sufficiency of cybersecurity practices, and public disclosures of sanctions.

Creating and promulgating minimum and uniform standards of 'reasonableness' of cybersecurity standards for the handling of student data would also be most useful. While cyberthreats facing schools will continue to evolve, it should not be insurmountable to come to agreement on common sense IT security practices, such as for user authentication/password management, user training, encryption of student data in transit and at rest, data minimization and deletion, and software patching/updates. Based on available information, it seems likely that many – if not most – of the incidents reported on the K-12 Cyber Incident Map could have been avoided if such standards were in place and (even modestly) enforced.

Fourth, school administrators lack guidance, resources, and the capacity to assess the reasonableness of their own and third-party data security practices. Both FERPA and the COPPA Rule presume that schools have the resources and knowledge to assess their own data security practices, to say nothing of that of their vendors. Emerging evidence suggests that this presumption should be challenged and that – at a minimum – such expertise and capacity is unevenly distributed across the thousands of public school districts, charter schools, and other public schools serving U.S. PreK-12 students.

While evidence from the K-12 Cyber Incident Map is certainly suggestive of this fact, recent audits of school district cybersecurity practices in Wyoming and Missouri offer more evidence of a systematic lack of capacity.

In Wyoming, school districts were found by the Wyoming Department of Audit[6] to have generally weak physical and logical security for student data systems. 'Physical' security refers to access to the actual equipment – servers, computers, routers, switches, etc. – that host and share student data. 'Logical' security refers to who can access data systems and with what authentication (which includes but is not limited to password policies). Most Wyoming school districts (42 of 48 examined) had some degree of findings related to weaknesses in security of student data systems (e.g., unencrypted connections, weak password, no audit trail, etc.). The auditors attributed the lack of attention to security of student data systems to school districts being unaware of security issues due to a lack of expertise, as well as privileging convenience over good security practices. Further, the auditors noted that most school

6 To read a summary of the Wyoming Department of Audit report to the members of the Wyoming Task Force on Digital Information Privacy (June 10, 2015), please see: https://www.edtechstrategies.com/blog/student-data-security-practices/

districts in Wyoming did not have comprehensive IT policies and procedures in place to address the identified concerns.

In Missouri, the Missouri State Auditor implemented a 'Cyber Aware School Audits Initiative,' which involved in-depth audits of five school districts' student data privacy and security policies and practices. The summary report[7] detailed numerous deficiencies in school district data security practices, including with respect to:

- **data governance**;
- **controls for creating and maintaining user accounts for accessing system resources**, including for terminated users, new authorized users, inactive users, and shared accounts;
- **security controls**, such as by designating a security administrator/lead, implementing strong password and access controls, maintaining security logs, ensuring the physical security of systems, and documenting security controls;
- **incident response and continuity planning**, including by creating and documenting polices and procedures for responding to data security incidents and for data breaches, as well as for continuity planning in cases where access to critical systems and data are interrupted;
- **security awareness and training programs**; and,
- **vendor controls**, including vendor monitoring and vendor contracts.

Any review of the COPPA Rule and FERPA with respect to the management of digital student records must consider and address these school capacity issues in ways that are responsive to the demonstrated need. Certainly, evidence suggests that if and until there is an actionable, evidence-based strategy to improving school student data security policies and practices, the underlying assumptions about the safety of the collection and use of student data in digital formats should be revisited.

In sum, in the enthusiasm to embrace innovative learning technologies to improve student outcomes, we may have unwittingly overlooked data security issues and introduced new threats to student safety and security. Now is the time to shore up student data security practices, and I urge the FTC and ED to take affirmative action in any revised regulatory guidance or policy that may emerge from this workshop and associated efforts.

7 Office of Missouri State Auditor. "Summary of Audit Findings – Cyber Aware School Audits (Report No. 2016-112)." October 2016. Available online at: https://app.auditor.mo.gov/Repository/Press/2016112401006.pdf