



OLR BACKGROUNDER: USING EDUCATION TECHNOLOGY TO COLLECT AND ANALYZE STUDENT DATA

By: Marybeth Sullivan, Legislative Analyst II

BUZZWORDS

Personally identifiable information (PII) is unique to an individual, such as one's name, address, age, social security number, race, or date and place of birth.

Metadata provides context and insights about, or makes implicit connections to, other data. For example, metadata about a text document may include information about the document's length, author, and date of publication; it does not include the exact content of the text itself.

Data mining is the practice of combing through electronically collected data (PII or metadata) to look for patterns that can be used to generate revenue, cut costs, or tailor services.

ISSUES

This report describes:

1. the practice of data collection and analysis known as "data mining," as used by education technology companies;
2. debated issues surrounding the practice; and
3. state actions to strengthen student privacy protections.

SUMMARY

In the January 2014 issue of [*State Legislatures Magazine*](#), the National Conference of State Legislatures (NCSL) cited data mining as an emerging issue that state legislatures may address in 2014 and beyond. According to NCSL, public and private organizations engage in data mining when they comb through electronically collected data to look for patterns and relationships. Discovered patterns can be used to tailor services, reduce operating expenses, generate profit, or for other purposes besides the primary purpose for which the data was collected.

Education technology companies that provide services to school administrators, teachers, and student users have the ability to mine student data. These companies that create electronic devices, programs, or applications (i.e., apps) could use these technologies to identify the characteristics and habits of individual student users for various purposes without the users' knowledge or permission.

Such purposes include customizing educational products or generating additional profit by (1) selling the data to third parties or (2) using it for marketing purposes. The public debate about student data mining has focused on both its educational benefits and student privacy implications.

Although various federal laws contain provisions protecting students' personally identifiable information (PII) collected in schools and online, they have not been updated to incorporate changes in education technology such as data mining of metadata. The legislatures and governors of several states have addressed this gap by enacting laws and issuing executive orders to create student privacy protections beyond those in federal law.

DATA MINING BY EDUCATION TECHNOLOGY COMPANIES

There are two main types of education technology products: those that (1) organize student records on behalf of school administrators and teachers and (2) provide online academic lessons to students. Table 1 lists examples of these technology products that could be mined for student data.

Table 1: Education Technology Products Suitable for Data Mining

<i>Product Types</i>	<i>Product Services</i>
<i>Student Records Products for Staff Users</i>	
Online gradebooks	Organize teachers' student attendance notes, test scores, behavior notes
Attendance records software	Organize staff notes on student illnesses, medical appointments, or bereavement
Health records software	Store student behavioral and nutrition records or student fitness data generated by heart monitors worn in gym class
Data analytics programs	Help staff record and monitor progress as students work on digital materials (e.g., may track students' speed, accuracy, and persistence working through academic questions)
Biometric sensors (e.g., eye scanners, palm print readers)	Help staff track student movement and identity on school grounds
Radio frequency identification chips (usually embedded in student IDs)	Assist staff with tracking movements in school or on and off the bus or monitoring debit card purchases

Table 1: -Continued-

<i>Product Types</i>	<i>Product Services</i>
<i>Academic Products for Student Users</i>	
School-issued laptops and tablets	Store textbooks, run academic applications, access the Internet
Online academic games, videos, and applications (i.e., apps)	Present online lessons, games, and practice questions for students to answer
Digital textbooks	Replace traditional printed textbooks; can be accessed on a laptop or tablet
Web-based tutorial services and homework sites	Provide quizzes and tutorial help to students outside of classroom instruction
School-issued email accounts	Allow students to discuss classwork with teachers and classmates or submit completed assignments electronically

Sources: The Pew Charitable Trusts: [Stateline](#), "Protecting Student Privacy in the Data Age," December 17, 2013; [Politico](#), "Data Mining Your Children," May 15, 2014; [The Washington Post](#), "How much data is being 'mined' from our kids? More than you know." October 2, 2014

Education technology products designed for staff could be mined for student PII, while products for student users could be mined for metadata that reveals how students use the products. Consequently, these products allow technology companies to spot patterns and draw conclusions about individual students or groups of students. For example, metadata can help companies draw conclusions about students' academic progress, work habits, learning styles, personal interests, locations, and web-browsing habits, as [Politico](#) reports.

DEBATED ISSUES

Current issues in the education data mining debate center on whether (1) companies have exploited student PII or metadata for non-educational purposes and (2) data mining improves academic services or compromises student privacy. The Pew Charitable Trusts' [Stateline](#), [Politico](#), and [The Washington Post](#) have followed this debate, and their reports follow proponents' and critics' positions, which appear below.

Regarding the first issue, privacy experts claim it is nearly impossible to tell if student data has been used for non-educational purposes. Nonetheless, privacy advocates and parents have raised concerns about companies' possible misuse of student data by selling the data to a third party or storing it in a manner vulnerable to cyber-attacks.

Regarding the second issue, education technology companies and certain educators argue that they can achieve the following educational advances using mined student data:

- producing digital materials (e.g., textbooks, programs) that self-adjust and personalize instruction to suit each student's learning style,
- improving principals' access to the academic records of intra-district transfer students,
- aiding teacher lesson plans by measuring students' subconscious responses to lessons, and
- increasing student safety by electronically monitoring their whereabouts during school hours.

Furthermore, [Politico](#) reports that a 2013 report by McKinsey & Co. found that expanding the use of data in K-12 schools and colleges could improve overall education instruction and efficiency, contributing over \$300 billion per year to the U.S. economy.

Data mining critics are concerned that education technology companies could use mined student data in ways that compromise student privacy, including:

- targeting commercial advertisements to the needs of individual students and their parents;
- allowing teachers to easily view students' academic histories and develop negative preconceptions about their capability;
- building student profiles that could be sold to employers, military recruiters, or college admissions officers;
- tracking students' physical locations outside of school hours or off-campus; and
- exposing personal student information stored on vulnerable company databases to cyber-attacks.

FEDERAL LAW AND STATE ACTION

Several federal laws include provisions safeguarding student data, but they were adopted before data mining practices evolved. Table 2 summarizes these protections.

Table 2: Federal Laws Protecting Student Information

<i>Federal Law</i>	<i>Scope of Protection</i>
Family Educational Rights and Privacy Act (FERPA) of 1974	<ul style="list-style-type: none"> • Requires schools, school districts, state education agencies, and federally-funded institutions to keep confidential PII in student records • Provides several exceptions to the confidentiality rule, including occasions when (1) parents or students over age 18 consent to disclosure or (2) organizations are conducting studies for educational agencies to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction
Protection of Pupil Rights Amendment (PPRA) of 1978	<ul style="list-style-type: none"> • Affords parents rights regarding U.S. Department of Education-administered student surveys, collection and use of student information for marketing purposes, and certain physical exams • Requires parental consent for student participation in surveys concerning political affiliation, psychological issues, sexual behavior, illegal behavior, family relationships, privileged relationships, religious beliefs, or income
Children's Online Privacy Protection Act (COPPA) of 1998	<ul style="list-style-type: none"> • Regulates the online collection of PII from children under age 13 by commercial websites or online services directed at children, which need not be education-related • Requires parental consent for websites to collect PII from children, with the exception of contests, newsletters, and homework help, among other things

Politico reports that U.S. Department of Education chief privacy officer Kathleen Styles has acknowledged that student metadata could be mined using education technology and is likely not protected by FERPA. In many states, legislation or executive orders have addressed this problem, using efforts ranging from imposing data-sharing restrictions on school districts to forbidding education technology companies from using student data for non-educational, commercial purposes. Table 3 provides a sample of recent state efforts.

Table 3: Sample of State Student Data Privacy Protection Initiatives

State	Initiative(s)	Scope of Protection
California	SB 1177 (enacted September 2014)	Prohibits operators of K-12 online sites or mobile apps from using student information obtained from technology to: <ol style="list-style-type: none"> engage in targeted advertising, create a profile about a student (unless for school purposes), sell the information for profit, and disclose a student's PII (unless responding to the judicial process or other special circumstances) Requires these operators to: <ol style="list-style-type: none"> use reasonable security procedures to protect student information and delete a student's PII upon school or school district request
	AB 1584 (enacted September 2014)	Allows school districts to enter into contracts with third party vendors to provide online pupil records management services, but requires these contracts to contain certain privacy protection provisions to be valid
Georgia	Executive order (May 2013)	Prohibits the collection of student data for the development of commercial products or services
New York	Common Core Implementation Reform Act, S6356D , Subpart L (Part AA) (enacted March 2014)	Requires appointment of a State Education Department Chief Privacy Officer to develop data security standards and privacy policies Calls for immediate development of the Parents' Bill of Rights, to be posted on all public and charter school websites, to inform parents of legal requirements regarding privacy, security, and use of student data Prohibits the sale or release of a student's PII for any commercial or marketing purposes Restricts a school's authority to collect and release PII

Sources: [The National Law Review](#), "California Strengthens Student Privacy Protections," October 6, 2014; [The National Law Review](#), "New York State Requires Parents' Bill of Rights for Data Privacy and Security," September 5, 2014; The Pew Charitable Trusts, [Stateline](#), "Protecting Student Privacy in the Data Age," December 17, 2013

HYPERLINKS

State Legislatures Magazine, "Hot on the Horizon,"

<http://www.ncsl.org/bookstore/state-legislatures-magazine/hot-on-the-horizon.aspx>, last accessed November 20, 2014.

The Pew Charitable Trusts, *Stateline*, "Protecting Student Privacy in the Data Age,"

<http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2013/12/17/protecting-student-privacy-in-the-data-age>, last accessed November 20, 2014.

Politico, "Data Mining Your Children," May 15, 2014,

<http://www.politico.com/story/2014/05/data-mining-your-children-106676.html>, last accessed November 20, 2014.

The Washington Post, "How much data is being 'mined' from our kids? More than you know," October 2, 2014, <http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/10/02/how-much-data-is-being-mined-from-our-kids-more-than-you-know/>, last accessed November 20, 2014.

The National Law Review, "California Strengthens Student Privacy Protections," October 6, 2014, <http://www.natlawreview.com/article/california-strengthens-student-privacy-protections>, last accessed November 20, 2014.

The National Law Review, "New York State Requires Parents' Bill of Rights for Data Privacy and Security," September 5, 2014, <http://www.natlawreview.com/article/new-york-state-requires-parents-bill-rights-data-privacy-and-security>, last accessed November 20, 2014.

California Legislative Information, SB 1177, http://leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_bill_20140929_chaptered.pdf, last accessed November 20, 2014.

California Legislative Information, AB 1584, http://leginfo.ca.gov/pub/13-14/bill/asm/ab_1551-1600/ab_1584_bill_20140929_chaptered.pdf, last accessed November 20, 2014.

The State of Georgia, Executive Order, http://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/document/05.15.13.01.pdf, last accessed November 20, 2014.

LegiScan, New York Senate Bill 6356D, <http://legiscan.com/NY/text/S06356/2013>, last accessed November 20, 2014.

MBS: ts/tjo