UT LAW CLE | THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

34th Annual School Law Conference

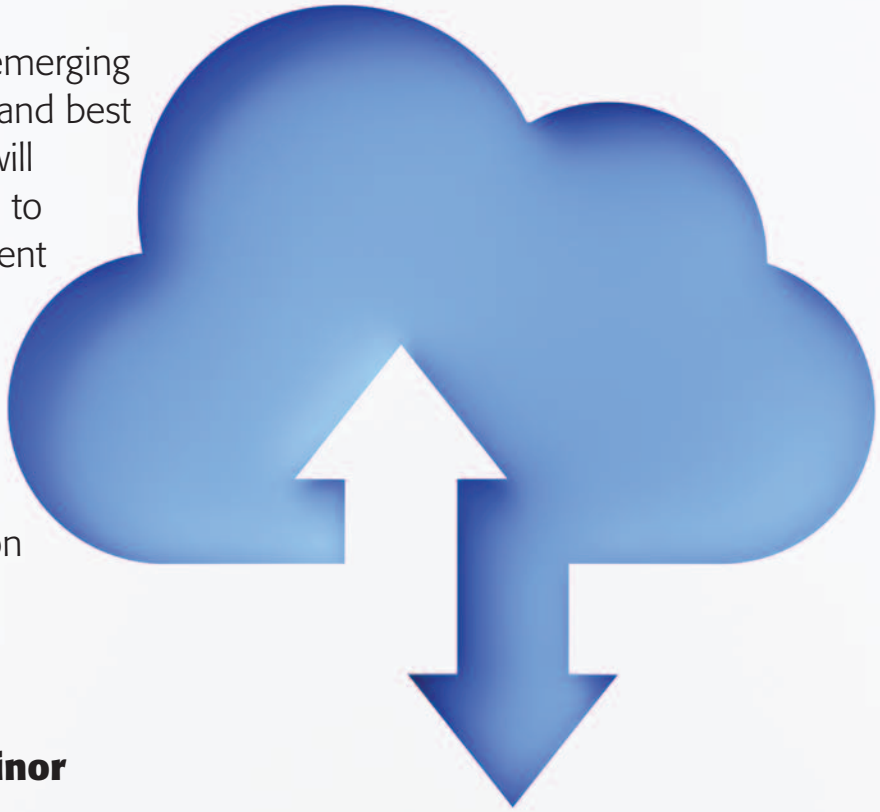
February 25-26, 2016
Austin, Texas

Student Data Privacy: The National Conversation

Sonja Trainor

Student data privacy is cloudy today, clearer tomorrow

Consensus is emerging over concepts and best practices that will enable schools to safeguard student privacy while continuing to use powerful, third-party computing for better education outcomes.



By Sonja Trainor

THE EDUCATION COMMUNITY operates in the "big data" world that promises big advantages, including individualized learning and the ability to track and document the needs, progress, and successes of individuals and groups. Most schools and districts rely on outside parties to process and store the data due to the prohibitive costs involved in developing their own platforms. Similarly, in health care, banking, consumer transactions and many public services, we hand over vast amounts of our personal information to online service providers for the convenience, speed, and even security they offer.

But seemingly frequent and certainly publicized data breaches and the federal government's own online surveillance apparatus have given rise to increasing concerns over privacy. These days we want our information stored and processed for our own purposes; we do not want vendors to push ads to us without our permission nor to pass along our personal data to others.

For years, privacy advocates have articulated anxieties felt by the public and pushed back against intrusions on data privacy. Following Edward Snowden's revelations regarding the scope of NSA surveillance practices in May 2013, privacy concerns played out in national media, and certain sectors of the public seemed more receptive to them. Policy discussions among education, privacy, government, and vendor groups at the na-

SONJA TRAINOR (strainor@nsba.org) is director of the National School Boards Association Council of School Attorneys, Alexandria, Va.

✱ Deepen your understanding of this article with questions and activities in this month's *Kappan* Professional Development Discussion Guide by Lois Brown Easton. Download a PDF of the guide at **kappanmagazine.org**.

Illustration: Thinkstock/iStock

tional level became more urgent and frequent. From these discussions, bright-line rules began to emerge — new norms of student data privacy on which nearly all interested groups could agree.

Data privacy backlash chronology

2011 inBloom's predecessor, Shared Learning Cooperative, launches with $87.3 million from the Bill & Melinda Gates Foundation and $3 million from Carnegie Corp. to provide a data warehouse in the cloud for many kinds of student data and to link that data through the Common Core to digital educational content.

MAY 2013 Edward Snowden leaks NSA vast surveillance practices.

2013 Privacy groups' concerns about student data protection in education garner national media attention.

2014 More than 100 bills are introduced in state legislatures addressing student data privacy.

April 2014 inBloom announces that it will wind down. CEO cites "missed opportunity for teachers and school districts to improve student learning."

MAY 2014 Google says its Apps for Education suite will no longer collect data for advertising purposes. It also eliminates scanning functions that could have been used for ads.

MAY 2014 The White House report on big data recommends measures to ensure that student data is used only for educational purposes and that investment and innovation in education technology continue to flourish.

MAY 2014 Federal Trade Commission identifies "best practices" and recommends that Congress require the data broker industry to become more transparent and give consumers greater control over their personal information.

— Sonja Trainor

At the same time, legislation was introduced in most states addressing student data privacy. By May 2014, after the collapse of education data platform inBloom, nearly 100 bills addressing student data privacy were pending in state legislatures, and that number continues to grow.

To a large extent, the state-level bills attempt to codify some of the bright-line rules filtering out of the policy discussions at the national level, although there is disagreement about whether and how those rules should be reflected in law. As a general matter, the evolving law seeks to protect student privacy by giving parents more rights in the form of consent or notice regarding disclosure and/or use of their children's data, and to rein in practices — real or perceived — of vendors seeking to use student data for purposes unrelated to learning. Future legal frameworks are likely to impose more requirements on schools and vendors.

Educators who know the key issues regarding student data privacy in education will be more able to be part of the conversation.

Student records became student data

Before 2000, student data was still kept largely in paper records stored in file cabinets. Then No Child Left Behind introduced widespread accountability requirements, prompting the federal government to begin awarding grants for the creation of statewide longitudinal data systems. The explosion began. Companies developed a flurry of applications allowing schools to store and process information in a variety of ways, many allowing data to be stored on remote servers.

Emerging concepts

In Washington and across the country, organizations representing educational, privacy, vendor, and data interests have been holding symposia, summits, conferences, and white paper-review panels. These conversations have centered on simple yet stubborn questions: How do we as an education community protect student and family privacy while still using the extraordinary potential of student data to facilitate learning and operate a school district? Is parent consent the answer? Or will transparency in school district data practices provide sufficient notice and protections to families? Does the current legal framework sufficiently address the needs of schools,

Also available as part of the eCourse
[The Intersection of School Law and Technology: Privacy Issues and Responsibilities beyond the Brick and Mortar]

First appeared as part of the conference materials for the
31st Annual School Law Conference session
"Student Data Privacy: The National Conversation"