Alarms Sounded Over Student-Data Collection Services

By Emily Wilkins, CQ Roll Call

It was going to change the way education worked — individualized learning plans for students shaped by hundreds of pieces of data collected on each of them, analyzed and returned to teachers and parents by a program called inBloom. Now, two years after inBloom imploded, state and local education systems are utilizing similar methods, but with varying degrees of security and protocols.

To the technology community and educators struggling to make sense of large amounts of data, inBloom sounded like a solution. To some parents, it sounded dangerous. The information collected could range from test scores to behavior issues to whether students got free lunch. What if this information was hacked? What if it was sold? What if colleges used it to determine admissions?
“InBloom started a conversation,” says Amelia Vance, director of education data and technology with the National Association of State Boards of Education. “For the first time you suddenly had parents realizing that ... this is something that schools had always done, that schools collect a lot of data on students and most states did not have comprehensive law or policies to protect student privacy prior to 2014.”

In 2014, inBloom announced it would shut down and the nine states that initially partnered with the not-for-profit service had all backed away. CEO Iwan Streichenberger attributed the closure to “generalized public concerns about data misuse.”

That same year, lawmakers in 36 states introduced 110 bills related to student data privacy, and 27 of those bills passed in 20 states, according to statistics from the Data Quality Campaign and NASBE. In 2015, 47 states introduced 188 bills addressing student data privacy. As of May this year, the count of bills introduced is up to 111 bills in 36 states.

“A lot of these bills have been introduced over the last couple of years because of very legitimate concerns over how data is being used in education and how it’s being protected, but also by a number of concerns that have not yet come to fruition,” says Rachel Anderson, associate director of federal policy and advocacy with the Data Quality Campaign.

Of 20 school districts surveyed for a 2013 study by Fordham University’s Center on Law and Information Policy, 19 reported that they relied on cloud-based services for purposes that included managing data related to student performance, support for classroom activities and student guidance.

“The vast majority of schools, especially the small rural districts, don’t have the money or ability to hire someone who can put on all the security patches throughout the year,” Vance says. “[The third parties] are a lot more secure.”

For example, inBloom would have offered one place to store student names and addresses, test scores, learning disabilities, attendance, hobbies, after-school programs, career goals, family relationships and reasons for enrollment changes. Some of that information already was collected, but was stored on a number of different systems.
“Teachers would have to go into every type of software program they wanted to use for their class and manually enter every single kid,” says Tracy Weeks, the executive director of the State Educational Technology Directors Association. InBloom’s plan was to put all that data in one place.

On its now-defunct website, inBloom stated it would not “sell, assign, lease or commercially exploit confidential student data.” That pledge wasn’t enough for many parents, says Reg Leichty, a lobbyist for the Consortium for School Networking, an advocacy group for technology leaders.

“You see big data breaches in the retail industry, in the financial sectors, etc.,” he says. “That makes people nervous.”

Rachael Strickland is one of those people. A mother of two public school kids, Strickland cofounded the Parent Coalition for Student Privacy after her school district became a pilot district for inBloom. She said her interactions with the company left her feeling “marginalized” and “dismissed.”
About 60 percent of parents said they had heard little or nothing about schools letting private companies store students’ data, according to a 2014 survey by Common Sense Media, an independent organization focused on children’s use of media and technology. The Fordham University study of 20 school districts found only a quarter of those schools had informed parents they were using a cloud service to store student data.

Strickland envisioned a nightmare scenario where the information gathered on her children in elementary school plays a role not only in the academic world, like when they apply to college, but in matters like applying for a mortgage or health care.

“There’s not a lot of confidence that this information will be used to move policy in a positive way, much less help their individual child,” says Strickland. “As much as data could be and can be used for good purposes, it can be, maybe, used for not great purposes.”

One of the first student data privacy bills was passed in 2013 in Oklahoma that put the responsibility for protecting student data in the hands of teachers and education officials. But teachers and educators were overwhelmed when they tried to follow the new guidelines, says Ariel Fox Johnson, senior policy counsel with Common Sense Media.

Her organization, along with former California state Sen. Darrell Steinberg, a Democrat who takes office in December as Sacramento mayor, successfully pushed for passage of a law in California known as the Student Online Personal Information Protection Act in 2014, which put the burden of protecting data onto technology companies. The bill passed unanimously in both chambers before being signed into law. It has now been copied by 16 other states, each making their own adjustments.

Colorado, where Strickland lives, is one of those states. Colorado state Rep. Alec Garnett, a Democrat, heard similar concerns when he knocked on parents’ doors of parents to discuss issues. His bill passed into law this year.

“It was strongly bipartisan from the beginning,” he recalls. “I think folks have an expectation that protecting our kids is a high priority, and I think there was an assumption that this was already being done.”
The law is still being implemented, but Strickland isn’t cheering yet.

“When we feel like we’re being marginalized, it’s very difficult to have trust or faith in new legislation or technology that’s being introduced,” she says.

Weeks, a mother of two elementary-aged children herself, agrees that when it comes to introducing a new program for student data, parental involvement is vital.

“This is one of those places where communication is really key,” she says. “When schools and districts do a really good job of educating the parents and helping them understand how and why it’s being used, we see a better acceptance level from parents.”

While legislation has focused on privacy and safety, educators in Louisiana had different concerns after the state passed a student data law in 2014. The law was so strict that some teachers were concerned about being able to put together a yearbook, said Vance. The law was amended the next year.

“While privacy is important it’s also important that policy makers consider whether bills will inadvertently ban the use of technology that would help kids succeed and compete in today’s global economy,” Vance says. “We’ve seen some suffer from some of the fear driving these policies, which creates accidental policies down the road.”

When inBloom failed, then-SETDA executive director Doug Levin said in a statement the technology was “perhaps ahead of its time.” Two years later, his successor, Weeks, says she’s seen schools using new data systems that store information in the cloud, although most tend to be on a local level with greater restrictions on who can access the data.

“The industry has grown up around this, our policies have grown up around this,” she says.

“Most of what I see out there are ways to both have the data, and collect the data, and keep it secure and limited to only the people who need to see it,” Weeks says.