States backtrack on student tracking technology

By **Jeffrey Stinson, Stateline.org**

Nov. 13, 2014 2:00 AM

Dawn and Mike Cantrall's daughter, a seventh-grader at Brittan Elementary School, at her Sutter, California, home, wearing the radio frequency identification tag that the school asked her to wear, Feb. 8, 2005. The Cantralls filed a formal complaint against the school board, protesting the tag.

WASHINGTON—Do you know where your student is? At school? On the bus? Paying for lunch in the cafeteria?

Principals in thousands of the nation's schools know the answer because radio frequency chips are embedded in students' ID cards, or their schools are equipped with biometric scanners that can identify portions of a student's fingerprint, the iris of an eye or a vein in a palm.

Such technologies have become increasingly common in schools, which use them to take attendance, alert parents where their children get off the school bus or speed up lunch lines.

But those tools, which are supposed to make schools safer and more efficient, have become a flash point. Several states are now banning or restricting the use of the technology in schools, as worries over student privacy have risen amid breaches of government and commercial computer databases.

This year, Florida became the first state to ban the use of biometric identification in its schools. Kansas said biometric data cannot be collected without student or parental consent. New Hampshire, Colorado and North Carolina said the state education departments cannot collect and store

biometric data as part of student records.

New Hampshire and Missouri lawmakers said schools can't require students to use ID cards equipped with radio frequency identification (RFID) technology that can track them. The new laws are similar to one Oregon passed last year and what Rhode Island lawmakers passed in 2009.

The laws reflect a growing sense of unease among parents and lawmakers about new technology, how it's being used, what student data is being collected and stored and what security protects the information.

In all, 36 states considered 110 bills this year on the collection and security of student data, according to the nonpartisan, nonprofit Data Quality Campaign, which advocates the effective use of data in education. At least 39 bills addressed biometric data, according to the campaign's tracking, including 14 that passed.

"Technology is moving so fast," said Paige Kowalski, director of state policy and advocacy for the campaign. "I think that's why you're seeing these new laws. I think people are nervous about it. It's new. It's different from when we were kids."

She said, "I think there's a desire to use (technology), and a desire to slow down. We want to know exactly how it's being used . . . so we don't sacrifice too much privacy."

Nobody knows exactly how many of the nation's school districts use biometric or RFID technology, but many schools have been using them for a decade or longer.

Jay Fry, CEO of the biometric-in-schools company identiMetrics, said biometric identification is used in more than 1,000 school districts in 40 states from Alaska to Long Island, New York. West Virginia uses the technology in 70 percent of its 57 school districts, he said.

In cafeterias, for example, schools can replace traditional student ID cards with machines that can read small, identifiable portions of an index-fingerprint. The machine cannot capture a child's entire fingerprint or personal identity, Fry said. The data is tied to a multi-digit number that's tied to a student's identification in the school's computer database for billing.

"It's more secure from a privacy standpoint than a student ID, which has a name, picture and school on it—when lost, can be picked up by someone," said Fry, an educator for 25 years.

He said he devised the idea in 2002 when he was a middle school principal in Illinois because students too often lost their lunch money, their IDs or pin numbers during lunchtime and too many were left without enough time to get and eat their lunches. "You can't lose your finger," he said.

The system, he said, also allows for easy auditing and billing, including reimbursement to schools in the federal government's subsidized meals programs that fed students breakfast in 89,000 schools

and lunch in 100,000 in the federal fiscal year of 2012.

Other schools are embracing RFID systems. Students are issued badges or tags with embedded chips that either broadcast a radio signal, (battery-powered active systems) or are read when they are near a radio-frequency reader (passive systems). Such tags are widely used by government and the private sector for building security and for tracking packages.

Elizabeth Hunger, government relations manager for the Security Industry Association, said passive RFID technology is more common in schools, where students' RFID badges are read at school doors, on buses or at school events so educators know who's where. The technology also allows school doors to be locked and allow entry to only those with RFID badges.

Hunger said RFID readers pick up a number of a student's badge that can be correlated to a student's identification in a school's central computer. If a badge is lost, she said, "no one else can read it; they'd only get a number if they did."

Hunger said the industry recommends RFID technology as part of a "holistic approach" to school security, along with video cameras and trained personnel, especially after such incidents as the Sandy Hook Elementary School shooting in December 2012 in Connecticut, in which 20 students and six adults were killed.

But some lawmakers question whether schools really need such tools and worry that it is yet another example of government surveillance.

"There's a Big Brother' quality to this," said Missouri State Senator Ed Emery, who sponsored a law, which took effect this month, that restricts how school districts can adopt RFID technology and allows parents to opt out in districts that do employ it.

No Missouri school district had employed RFID before the legislature overrode Democratic Governor Jay Nixon's veto of Emery's legislation in September to make it law. But, Emery said, he wanted the law in place before any district spent $500,000 to $1 million to adopt it.

"This is a technology that is very difficult to limit and to secure," Emery, a Republican, said. "If a private company wants to do it, fine. But it's not something you should mandate on children."

Florida State Senator Dorothy Hukill stepped in when she got wind that the Polk County school system last year began a pilot program without parental permission to scan the retinas of students' eyes to keep track of them on school buses.

Calling it "an overreach," Hukill, a Republican, sponsored legislation signed by Republican Governor Rick Scott in May to ban the use of biometric identification in Florida schools.

"You don't need to collect biometric information to buy a hot dog in the school cafeteria or check

out a library book," she said.

Hukill, who's on the Florida Senate's commerce and government oversight committees, said she's not opposed to technology, but she is concerned about the hacking of data held by governments and businesses. "And once you collect the information," she said, "there is no rolling back."

The issue has caught fire in other states, such as Texas, where State Representative Lois Kolkhorst has pushed RFID legislation similar to Missouri's in recent years.

"The question is: Should the government be able to force a parent to have their children tracked in the same exact way that warehouse pallets, prisoners and migratory animals are monitored," said Kolkhorst, a Republican.

State legislators have continued to propose restrictions on the technology, despite repeated assurances from the companies that supply it that student information is secure. Fry said parents should be aware and consent to its use before it's deployed. And those who do not want their children using it should be able to opt out, he said.

Rather than prohibit use of the technology, Kowalski of the Data Quality Campaign suggested lawmakers focus on transparency so parents know how the technology is being used, what data is collected and what safeguards are in place to protect students' privacy.

"Were you as a lawmaker to prohibit it, you may be taking something useful away," she said.