Senate Bill 29

Derek L. Towster, Esq.

Scott Scriven LLP

Senate Bill 29

Big Picture

Scott Scriven LLP

Big Picture

- Senate Bill 29: The "Education Record and Student Privacy Bill"
- Enacted over the summer, and it will go into effect on October 24, 2024.
- The Bill slightly modifies Ohio Revised Code Sections 149.43 and 3319.31 as they relate to student records.
- The Bill creates three new Ohio Revised Code Sections: 3319.325, 3319.326, and 3319.327.

Big Picture

- The Bill affects two primary areas of public school districts' operations:
  1. The Bill establishes safeguards and required contractual provisions for contracts between public school districts and technology vendors.
  2. The Bill prohibits public school districts from accessing or monitoring various types of data collected by its technology – except in specific circumstances.
- Additionally, the Bill saddles public school districts with three new notice obligations to parents. Below, please find a more comprehensive summary of the Bill as well as our advice for how you should proceed under these new laws.

Senate Bill 29

Contracts with Technology Vendors

Scott Scriven LLP

Definitions

- "Technology provider" is defined as "a person who contracts with a school district to provide a school-issued device for student use and creates, receives, or maintains educational records pursuant or incidental to its contract with the district."
  - *See* R.C. 3319.325(E)
  - This definition includes ITCs, private technology vendors, software providers, app creators, etc.
- "School-issued device" is defined as "hardware, software, devices, and accounts that a school district, acting independently or with a technology provider, provides to an individual student for that student's dedicated use."
  - *See* R.C. 3319.325(C)
  - This definition is incredibly broad – e.g., chromebooks, emails accounts, monitoring software installed on specific devices, etc.
  - The only aspect of the definition with some wiggle room is the phrase "dedicated use."

Contracts with Technology Vendors

- The Bill codified a lot of education records obligations that already existed in FERPA.
  - *See* R.C. 3319.326(A), (C), (D), and (E)
- If there is a data breach containing student records maintained by a "technology provider" (e.g., Schoology, InfiniteCampus, etc.), then that technology vendor is now legally responsible for responding to the breach as required by R.C. 1347.12.
  - *See* R.C. 3319.326(B)
- When contracting with a "technology provider" (the definition for which is found at R.C. 3319.325(E)), the Bill requires the contract to contain a provision prohibiting the technology provider's employees from accessing education records unless doing so is necessary to fulfill the obligations of the contract.
  - *See* R.C. 3319.326(F)
- The Bill created an obligation for public schools to provide students and parents written notice by August 1st of each year identifying certain technology provider contracts. The below paragraph discusses this obligation in much more detail.
  - *See* R.C. 3319.326(G)

Notice Obligations – Technology Contracts

- New Notice Requirement: By August 1st of each school year, public school districts are now required to send a written list to all parents and students identifying every "curriculum, testing, or assessment technology provider contract affecting a student's educational records."
  - Since the Bill does not go into effect until October 24, 2024, school districts will not need to send out their first notice until the start of the 2025-26 school year.

According to the new law, the school district's written notice must:

1) "identify each curriculum, testing, or assessment technology provider with access to educational records;"
2) "identify the educational records affected by the curriculum, testing, or assessment technology provider contract;"
3) "include information about the contract inspection and provide contact information for a school department to which a parent or student may direct questions or concerns;" and
4) "provide parents and students an opportunity to inspect a complete copy of any contract with a technology provider."

Notice Obligations – Technology Contracts

- It is important to remember that the technology contract notice obligation only pertains to technology contracts that allow the technology vendor to access educational records and that also provide a "curriculum, testing, or assessment" service.
- If the District has a contract with a technology provider that does not meet both of those criteria, then the contract does not need to be included in the annual notice.

Senate Bill 29

Prohibitions on Accessing or Monitoring Data

Scott Scriven LLP

Monitoring & Accessing Student Data

Prohibitions:

A school district and its technology providers are prohibited from electronically accessing or monitoring any of the following:

1) "Location-tracking features of a school-issued device;"
2) "Audio or visual receiving, transmitting, or recording features of a school-issued device;" and
3) "Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity;"
    - *See* R.C. 3319.327(A)

- The legislature's vague use of the word "interactions" in the third prohibition leaves a lot to be desired.
- The two examples make it clear that accessing or monitoring keystrokes and web-browsing activity is prohibited, but what about the monitoring of student emails?
- Is that an "interaction" with an "account"?

Monitoring & Accessing Student Data

Exceptions:

The above prohibitions do not apply in the following circumstances:

1) "The activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by school district employees, student teachers, staff contracted by a district, a vendor, or the department of education, and notice is provided in advance."
2) "The activity is permitted under a judicial warrant."
3) "The school district or technology provider is notified or becomes aware that the device is missing or stolen."
4) "The activity is necessary to prevent or respond to a threat to life or safety, and the access is limited to that purpose."
5) "The activity is necessary to comply with federal or state law."
6) "The activity is necessary to participate in federal or state funding programs."
    - *See* R.C. 3319.327(B)

Monitoring & Accessing Student Data

New Notice Requirements:

1) "In any year that a school district or technology provider elects to generally monitor a school-issued device for any of the circumstances described [under prohibitions], the school district shall provide written notice of that monitoring to the parents of its enrolled students."

2) "In the event that one of the circumstances described [under exceptions] is triggered, the school district shall, within seventy-two hours of the access, notify the student's parent and provide a written description of the triggering circumstance, including which features of the device were accessed and a description of the threat, if any. This notice is not required at any time when the notice itself would pose a threat to life or safety, but must instead be given within seventy-two hours after that threat has ceased."
   - *See* R.C. 3319.327(C)

Monitoring & Accessing Student Data

New Notice Requirements:

- The first notice requirement applies to any school district that is "generally monitor[ing]" the protected data on a school-issued device. The timeline for issuing this notice is not precisely identified, but it must happen each school year. As such, for the 2024-2025 school year, we recommend that each school district provide this notice on or before October 24, 2024 – the effective date of this new legislation.

- The second notice requirement only applies when a school district "access[es]" the protected data on a school-issued device. The notice must be sent to the student's parents within seventy-two (72) hours following the access of the data.

Enforcement

- No enforcement mechanism is built into the new law.
- As such, individuals wishing to enforce the new law have very limited options.

1. A mandamus action against a non-complying school district. This type of legal action asks a judge to order the school district to comply with its legal obligation.
2. There are a few different statutes in Ohio law that generally permit ODEW to remove funding from a school district that is not complying with all of its legal obligations; however, since ODEW has not used this authority in the past to force compliance with other statutes, it seems unlikely that ODEW will take that position with these new laws.
3. The last (and most likely) way someone could enforce this new law is through a disciplinary appeal. In other words, a parent or student could use the suspension/expulsion appeal process already set forth in a school district's policies to challenge certain evidence of wrongdoing (e.g., browser history) when the evidence was monitored and/or accessed in violation of these new laws. Practically, a parent, student, or their attorney could argue that a school district cannot consider such ill-begotten evidence when making disciplinary decisions. We believe that this is the most common way in which these new laws will see true enforcement.