K-12 Student Data Privacy Law: Questions and Answers

August 2017

TENNESSEE COMPTROLLER OF THE TREASURY

Beth Swenson/Legislative Research Analyst
Elizabeth.Swenson@cot.tn.gov

Modern technology provides many methods of generating data about individual students. These technologies bring benefits, such as more targeted interventions designed to improve education outcomes, but they also increase opportunities for unauthorized releases of information about individual students. These two forces mean policymakers are often seeking the right balance between maintaining students' privacy and allowing access to student data to improve educational quality.

Federal and state laws are in place to protect K-12 students by regulating the creation of student data at school and how that data may be used and shared. This OREA Q&A will answer some basic questions about the existing legal framework in Tennessee for student data privacy in K-12 public schools.[1]

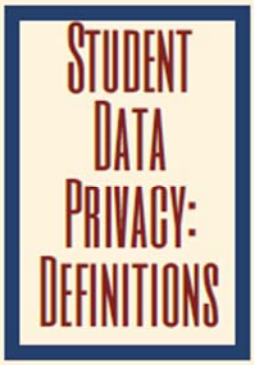
[1] There are privacy protections beyond those for grades K-12 as discussed in this Q&A. For example, privacy laws also apply to students in pre-kindergarten and Tennessee's Early Intervention System.

Q: What is "student data"?

Does a piece of information identify an individual student or use personal information about an individual student? If yes, then consider that information to be student data.

A: Academic records and health information are commonly recognized as types of student data, but the term "student data" is broad, encompassing almost anything that a student creates in school or that identifies an individual student. Student data is not limited to social security numbers or test scores; student data can encompass school work, class behavior, or even a student's location. For example, a teacher's decision to use a phone app to help her track individual student behavior creates student data. Responses to surveys administered to students during standardized testing is another source of student data. Creating a classroom blog with stories written by students generates student data, although the teacher might not consider such an effect; this is an important point: student data can be generated without the intent to create data.

An important question concerning student data is whether a piece of information identifies an individual student or uses personal information about an individual student. Identifying individual students may be done both directly or indirectly. For example, several pieces of seemingly unrelated data could combine to personally identify a student: if a source of information describes a student with certain characteristics and a specific grade point average (GPA) who attends a particular high school, and that school only has one such student, that information could be considered to personally identify the student, even without using his or her name.

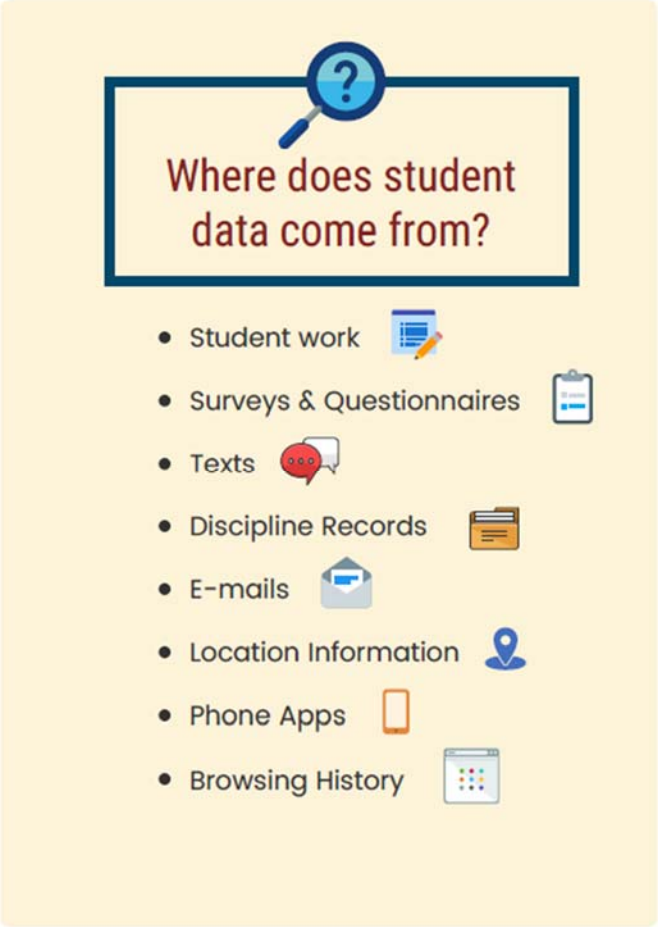


- Personally Identifying Information (PII) -- any information that can be used to identify individual students, such as name, address, social security number, etc.
- De-identified Data -- student level information that does not identify individual students, for example a data set that assigns random numbers to each student
- Breach -- unauthorized release of personally identifying student information for any reason; can be accidental or intentional

Q: Who creates student data?

A: Student data is either created *by the student* or an entity other than the student creates the data *about the student*. For example, the classroom teacher who takes daily attendance is creating data about her students. Parents who request and receive an IEP[2] for their child set in motion the creation of a large amount of data about their child.

Conversely, students themselves can generate their own data. This can take many forms, from standardized test performance (e.g., a student's score on his or her test) to Internet browsing history (e.g., a student using the Internet on a school computer to conduct research for a school project generates a browsing history) to student work (e.g., an essay a student writes for a homework assignment).



Q: What is "student data privacy"?

Student data privacy refers to efforts to maintain the confidentiality of information that identifies individual students.

A: In general, student data privacy refers to efforts to maintain the confidentiality of information that identifies individual students. Student data is often specifically defined within the law or regulation that governs its collection and/or disclosure. However, student data can take the form of any personally identifying information about students, such as demographic information, grades and test scores, and attendance or behavior records.

Thinking about student data privacy may also include considerations about what student data *should not* be collected. There is no privacy interest to protect if there is no student data collected.

[2] IEP stands for Individualized Education Program, which is a written statement that ensures a student with a disability has access to the general education curriculum and is provided the appropriate learning opportunities, accommodations, adaptations, specialized services, and supports.

Q: What is a data breach?

A: A breach occurs when unauthorized persons have access to data on individual students. A breach may be accidental, such as a school official giving the wrong folder (containing another student's private data) to a parent, or intentional, such as the deliberate theft of student data.

Remember to consider what student data should not be collected. There is no privacy interest to protect if there is no data collected.

How to prevent data breaches, and how to deal with them should they occur, are elements of student data privacy. Current laws focus on regulating the behavior *of the party collecting or generating the student data*; thus, the responsibility for preventing breaches of privacy lies with the party collecting the information. Student data privacy policies generally require some corrective action following a breach, including notification to affected individuals.

Q: How does Tennessee law protect student data privacy?

A: Tennessee has multiple laws that address, either directly or indirectly, the use and disclosure of data about Tennessee students.

Regulating student data privacy involves targeting the behavior of a specified entity. Laws protect student data privacy by governing the actions of either a school employee, a member of the public, or a third-party vendor or technology operator. School districts may take steps to protect student data privacy beyond what the laws require. However, those additional protections are likely to cost more in time or money.

Q: What are Tennessee's current student data privacy laws?

Tennessee's Open Records law

2014 Data Accessibility, Transparency and Accountability Act

2016 Student Online Personal Protection Act

A: Tennessee's **Open Records** law,[3] which governs access to and disclosure of certain records to members of the public, specifies that "the records of students in public educational institutions" are to be "treated as confidential" and, therefore, not subject to a public records request. However, information relating only to an individual student's name, age, address, dates of attendance, grade levels completed, class placement and academic degrees awarded may be disclosed.[4]

In 2014, the General Assembly passed the **Data Accessibility, Transparency and Accountability Act,**[5] which gives the state more control and oversight regarding Tennessee public school employees' collection of student data, and strengthens parental rights with respect to student data privacy. This law requires the Tennessee Department of Education to develop a model policy for school districts related to student records and data privacy; school districts must either adopt the model policy or develop their own policy subject to the approval of the Department of Education. The law also includes requirements for notifying parents of their rights (such as the right for parents to request student data specific to their children's educational record or the right to inspect and review their children's education records maintained by the school), as well as prohibiting school employees from collecting certain types of data (such as voting history and firearms ownership) and requiring parental consent prior to collecting certain types of biometric data (such as pulse, blood volume, posture, eye-tracking).

Public records are "all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings, or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency." Tennessee Code Annotated 10-7-503(a)(1)(A)(i). Any citizen of Tennessee has the right to personally inspect a public record unless there is a state law that restricts or prohibits inspection. Tennessee Code Annotated 10-7- 503(a)(2)(A).

In 2016, the General Assembly passed the **Student Online Personal Protection Act,**[6] which primarily addresses the actions of third parties outside of Tennessee schools and districts. This law regulates the actions of vendors/contractors or other third parties operating online services used by students, while still allowing personalized learning and development of new educational technologies.

[3] *Tennessee Code Annotated 10-7-504(a)(4)(A).*
[4] *Tennessee Code Annotated 10-7-504(a)(4)(A).*
[5] *Tennessee Code Annotated 49-1-701.*
[6] *Tennessee Code Annotated 49-1-708.*

The act prohibits the operator of a website, online service, online application, or mobile application used primarily for K-12 students from doing any of the following:

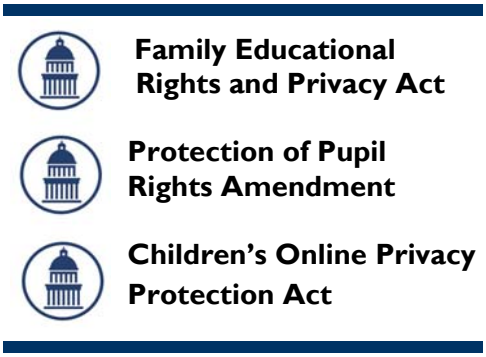
- Using targeted advertising based on student data collected by the operator,
- Creating profiles of student users except for K-12 school purposes, and
- Selling or renting a student's information.

Student information protected by the act, known as “covered information,” is defined as personally identifiable information or material in any media or format that is not publicly available and is:

- Student generated (or generated by the parent or guardian),
- Employee generated, or
- Operator generated.

The Student Online Personal Protection Act prohibits an operator from disclosing covered information to outside parties unless an exception applies. The statute also requires an operator to implement security procedures and delete student data.

Q: How does federal law protect student data privacy?



A: There are three primary federal statutes that currently govern student data privacy: FERPA, PPRA, and COPPA. FERPA is the **Family Educational Rights and Privacy Act,**[7] which protects the privacy of student education records and applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent in order to release any information from a student's education record. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.

[7] *Family Educational Rights and Privacy Act, U.S. Code 20 (1974) § 1232g.*

PPRA is the **Protection of Pupil Rights Amendment,**[8] which governs any entity (school or otherwise) that administers a student survey, analysis, or evaluation to students. It lists eight categories of survey content that are limited by the act:

(1) political affiliations or beliefs of the student or the student's parent;

(2) mental or psychological problems of the student or the student's family;

(3) sex behavior or attitudes;

(4) illegal, anti-social, self-incriminating, or demeaning behavior;

(5) critical appraisals of other individuals with whom respondents have close family relationships;

(6) legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;

(7) religious practices, affiliations, or beliefs of the student or student's parent; or

(8) income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).[9]

FERPA is a complex law with many provisions. For more information, see Comptroller of the Treasury, Office of Research and Education Accountability, Defining Tennessee Education: A Glossary of Education Terms, http://comptroller.tn.gov/OREA/Glossary.

This law requires schools to obtain prior consent of the parent before administering a survey, analysis, or evaluation if it gathers any data within these protected categories. There are also provisions in the law addressing parental rights of access to and notification of the survey.

COPPA is the **Children's Online Privacy Protection Act**,[10] which governs the operators of websites and online services (including mobile apps) and regulates what information may be collected from any child younger than 13 on the Internet. The law does not apply strictly to students and is not limited to educational data. COPPA requires parental consent to the operator's collection and use of a child's information, but schools may also provide consent as the parent's agent for educational purposes.

---

[8] *Protection of Pupil Rights Act, U.S. Code 20 (1974), § 1232h.*
[9] *Protection of Pupil Rights Act, U.S. Code 20 (1974), § 1232h(b).*
[10] *Children's Online Privacy Protection Rule, Federal Trade Commission, Title 16 Code of Federal Regulations §312.1 et. seq.*

Contact Information

Justin P. Wilson
Comptroller of the Treasury

Jason Mumpower
Chief of Staff

Comptroller of the Treasury
State Capitol
Nashville, Tennessee 37243
(615) 741-2501
www.comptroller.tn.gov

To report fraud, waste, or abuse of government funds and property, contact the Comptroller's toll-free hotline at 1-800-232-5454 or ***www.comptroller.tn.gov/hotline*****.**