common sense®

Assessing State Laws on Student Privacy in 2014 and Beyond:

A School Privacy Zone Update from Common Sense Kids Action

Assessing State Laws on Student Privacy in 2014 and Beyond

A School Privacy Zone Update from Common Sense Kids Action

www.commonsensemedia.org/kids-action

Table of Contents

Executive Summary

THE ISSUE: STUDENT PRIVACY IN A DIGITAL AGE

Schools and students are more connected than ever before, increasingly integrating laptops and tablets in the classroom and relying on cloud-computing services for a variety of academic and administrative functions. Online platforms and websites, mobile applications, digital courseware, and cloud-computing programs track students' attendance and grades, monitor students' physical activity and locations, manage school lunch programs, and offer individualized learning platforms. Schools and education technology ("ed tech") providers collect massive amounts of sensitive data about students, including contact information, performance records, online searches, family finances and backgrounds, health information, behavior and disciplinary records, meal selections, and locations.

Educational technology, used wisely, has the potential to enhance and personalize student learning and improve school operations and efficiency. To realize ed tech's promise, we must create trusted online environments that promote innovative learning while protecting students' privacy and the security of their personal data.

Students' sensitive information is at risk. Federal and state law has not kept pace with technology, and numerous contracted and uncontracted ed tech providers are generally free to sell or disclose student data or use it for marketing or profiling. Ed tech providers also do not always collect or keep data securely and may retain it indefinitely. The vast majority of adults polled by Common Sense in 2014 expressed concerns about noneducational interests accessing and monetizing students' data and creating student profiles. And nine in 10 supported tighter security standards.

ASSESSING THE 2014 LAWS

Twenty states enacted 26 laws addressing K–12 student privacy.

- More than half these states passed laws limiting the noneducational use of students' data, including its commercial use, primarily by educational agencies and contracted ed tech vendors.
- Almost half the states explicitly banned or restricted the commercialization of students' data, including its sale or use in marketing or advertising.
    - Most of these states regulated educational agencies or set forth contract provisions for certain third parties, though a few directly regulated ed tech providers.
    - California's Student Online Personal Information Protection Act (SOPIPA) is unique in that it applies to all K–12 ed tech services, whether they're cloud services, websites, or apps and whether or not a contract exists.
- Most states addressed data security, with some also directly addressing data breaches, data retention, and data destruction.
    - Laws usually required data-security plans or that data be kept securely by educational agencies or private (typically contracted) vendors.
- The majority of states moved to limit the collection of sensitive data, such as biometric data.
- States also passed laws regarding governance and transparency, often for educational agencies.

RECOMMENDATIONS FOR POLICY MAKERS

Legislators are giving student privacy more attention now than ever before. However, pitched battles between corporate interests and the public interest are playing out across the country.

Legislators should consider regulations that allow for innovation and prevent students' data from being misused or commercialized — including being sold or used in marketing, advertising, or other noneducational profiling. In crafting regulations that prevent certain uses of students' information, legislators should bear in mind that the school context is a unique one, in which schools and teachers make most of the ed tech choices, often leaving parents and students as a captive user audience with few choices. Given this reality, "consent" on the part of parents or students to additional data uses by ed tech providers may not be completely voluntary, meaningful, or informed. Parents may feel forced to consent so that their children can participate or may mistakenly assume a school has vetted an ed tech provider's practices. Thus, restrictions on the commercial, noneducational, and marketing use of data are best as flat bans, which set clear rules of the road for schools, industry, and families.

Laws also should establish robust security, retention, and disposal standards. Transparency and data minimization also are importance principles.

Additionally, legislators should be mindful of which entities their regulations cover. The vast majority of the student privacy laws in 2014 regulated schools and state and local education agencies, either by setting forth data-governance procedures (such as requiring chief privacy officers or transparency about what student data is collected) or by setting forth requirements for contracts with certain third-party vendors. These are good steps, yet they leave the ed tech providers uncovered. Legislators should consider directly regulating ed tech companies, as they — not overburdened schools — are often in the best position to ensure compliance with any new standards. Only a few states did this in 2014, directly regulating ed tech providers. And only California's SOPIPA directly regulated all ed tech providers: K–12 websites, online services, and mobile apps, whether or not a contract is involved. This is why Common Sense has been so supportive of SOPIPA and why SOPIPA has been hailed as a landmark law: It establishes clear privacy and data-security rules while permitting innovation, so students' personal information will be used to enhance their educations but won't be exploited for commercial purposes or fall into the wrong hands.

I. Introduction

In 2014, state legislators introduced over 100 bills addressing student privacy. Ultimately, 20 states enacted 26 laws addressing K–12 student privacy.[1] This report analyzes and assesses the legislative landscape and makes recommendations for policy makers.

Schools and students are more connected than ever before. Laptops and tablets are increasingly integrated in the classroom, and cloud-computing services perform a variety of academic and administrative functions. Schools and teachers are experimenting with digital learning platforms, fingerprint-purchased cafeteria meals, and digitized student records stored remotely "in the cloud." Educational technology ("ed tech"), used wisely, has the potential to positively transform America's schools; it can enhance and personalize student learning in previously unimaginable ways and vastly improve school communications, operations, and efficiency. To realize ed tech's potential, we must create trusted online environments for learning that protect students' privacy and the security of their personal data.

Through online platforms, mobile applications, digital courseware, and cloud computing, schools and education technology providers collect massive amounts of sensitive data about students, including contact information, click strokes, performance records, online activity, family background, health information, behavior and disciplinary records, eligibility for free or reduced-price lunch — even cafeteria selections and children's locations in real time as they ride the school bus home. Today's students leave digital footprints wherever they go, not only while sitting in the classroom but during their commutes and while doing their homework. The data collected from students can be very personal. And this personal student information is at risk.

At present, students' personal information may be used for a variety of purposes unanticipated by schools and unexpected by students and their parents. Many educators and educational institutions have not been trained to contend with today's rapidly advancing technology. Teachers may be enticed by "free" apps that turn out to be paid for by marketing students' data. For their part, ed tech vendors have a mixed record of protecting student data. Many indicate a desire to do the right thing, but many also have opaque privacy policies and unclear sharing practices. Students' sensitive information may be sold for profit, or it may be used to target ads and products to unsuspecting children and their families. It may be used to create rich profiles of children. Moreover, student data is vulnerable to security breaches and hacking, as it is not always maintained securely and may be stored for years or even decades.

This is a real concern. In a 2014 Common Sense survey, 90 percent of respondents expressed concern about how noneducational interests are able to access and use students' personal information.[2] The monetization of students' data is particularly problematic. Three-quarters of respondents supported making it illegal for schools and ed tech companies to sell students' private information to advertisers and restricting companies from using students' online habits and searches on school computers to target online advertisements to them. Additionally, 70 percent of respondents supported

[1] See Appendix 1. Common Sense is grateful to Data Quality Campaign for keeping track of the more than 100 bills pending in 2014.

[2] Common Sense Media press release, National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared: Americans Overwhelmingly Support Reforms to Protect Students, Including Increased Transparency, Tighter Security Standards, and More Restrictions on Companies and Cloud Services (Jan. 22, 2014) (available at http://www.commonsensemedia.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern.)

restricting cloud services from using students' emails, online searches, and Web histories to build a profile of personal data and demographics over time. And nine out of 10 respondents supported tighter security standards to protect students' private information in the cloud.

Unfortunately, currently companies are seemingly free to engage in many of these practices. Companies have built entire industries out of selling students' sensitive information — for example, under the guise of providing students with information about post-secondary, "enrichment," and scholarship opportunities. Regrettably, at present these companies can typically sell students' information not only to schools but also to data brokers, marketers, and other commercial interests. A Fordham Law School Center on Law and Information Policy study of contracts between schools and cloud-computing vendors found that fewer than 7 percent of contracts restricted the sale or marketing of student information by vendors.[3] On the security side, the Fordham study concluded that cloud-computing service contracts generally had inadequate data security measures and allowed vendors to retain student information in perpetuity.[4] And these vendor practices only took into account situations where the schools had contracts with the vendors. A number of apps, sites, and services are used without contracts and are simply downloaded or bookmarked by a teacher just before class or clicked-through by a student completing homework. It seems highly unlikely that when there's a lack of a contract, vendors will feel bound to keep students' data free from commercialization or secure.

Too many students have personal information transmitted and/or stored in unsecure environments. Software engineer and security researcher Tony Porterfield found that numerous K–12 educational services did not utilize basic encryption, stored passwords in plain text, or did not require user authentication.[5] In one case, the developers did not take additional security precautions even after serious flaws were brought to their attention.

Current federal laws have not kept pace with the development of education technology and do not fully address modern student privacy concerns. The Family Educational Rights and Privacy Act (FERPA) dates back more than 40 years to 1974, a time of paper records and punch cards, and has major gaps in coverage of sensitive information. The Protection of Pupil Rights Amendment (PPRA) is equally outdated, with limited requirements directed at school districts regarding surveys and notice about certain marketing activities. The Children's Online Privacy Protection Act (COPPA) and related rule recently revised by the Federal Trade Commission is not designed to address school use of online sites and services or students' educational data. Rather, its focus is on ensuring that parents provide informed consent before child-directed online companies collect personal information from their children under the age of 13.

States have begun to respond.[6] The 26 K–12 laws enacted in 2014 vary widely and reflect a range of concerns and issues, from collection of sensitive student and family information, to data sharing with companies and the federal government, to school access to students' social media profiles. Most of the laws regulate schools and state and local education agencies. For example, some set forth data-governance procedures and require chief privacy officers and the creation of more transparent data-collection systems. Some state laws address contracted third-party and commercial uses of data. And a few new state laws address ed tech providers directly.

[3] *Joel Reidenberg, Privacy and Cloud Computing in Public Schools 51 (Dec. 13, 2013) (available at http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip).*

[4] *Id. (executive summary).*

[5] *Natasha Singer, Uncovering Security Flaws in Digital Education Products for Schoolchildren, New York Times (Feb. 8, 2015) (available at http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html).*

[6] *Congress and the Obama Administration have also begun to address student privacy concerns, and bills are starting to appear at the federal level.*

II. Analysis

Common Sense Student Privacy Principles

Common Sense has long focused on protecting kids' and teens' online privacy as well as the smart use of technology in education. These issues naturally coalesced around student privacy. In 2013, Common Sense launched its School Privacy Zone campaign and introduced three fundamental principles that serve as guideposts for how educators and companies can wisely approach ed tech to enhance kids' education while protecting student privacy. The principles allow for technology to enrich student learning while ensuring that sensitive information about students is kept out of the hands of noneducational, commercial interests and other third parties.

These common-sense principles are visible in many of the laws that passed this year and serve as a useful framework for assessing the current landscape.

1. **Students' personal information shall be used solely for educational purposes;**
2. **Students' personal information or online activity shall not be used to target advertising to students or families; and**
3. **Schools and education technology providers shall adopt appropriate data security, retention, and destruction policies.**

More than half the states passed laws limiting the noneducational use of data, including its commercial use.

The very personalized nature of student data that enables individualized and customized learning also makes such data quite valuable commercially. One can easily imagine a student's online progress (or lack thereof) serving as the basis for companies to target advertisements directly to anxious parents who may feel pressured to buy whatever is offered. Alternatively, an enterprising but unscrupulous company might seek to buy high school students' math results, cull out the lesser-performing teens, and target them with unfavorable credit card offers upon graduation.

A. Almost half the states explicitly banned or restricted the commercialization of student data, including its sale or use in marketing or advertising.

Recognizing the perils of commercializing students' educational data and the need for regulation in this area, nine states explicitly limited the commercial use of data, prohibiting either the sale of data or its use in advertisements or marketing by schools, third parties, or both. In some instances, the laws are broad prohibitions. In others, there are exceptions, allowing certain commercial uses by certain parties or allowing for certain commercial use with parental consent.

Commercial Purposes

Using data for "commercial" purposes is a broad concept that can encompass multiple activities. There are a number of ways to profit from student data, such as:

- Using student data to send students or their families targeted advertisements or marketing;
- Allowing others to use student data to send such targeted advertisements or marketing;
- Selling student data; and
- Creating commercial profiles that can be sold or used for advertising, marketing, analytics, or other commercial purposes.

1) Most of these states regulated educational agencies or set forth required contract provisions for certain third parties.

Many states took the approach of regulating state and local educational agencies themselves. **Laws either prohibit schools and states from using data in certain ways or require them to put in place contractual restrictions regarding third parties' commercial use of data.** Such contracted third parties may be cloud-service providers, Web operators, or app or program developers who contract with schools and districts to provide their sites or services to schools and students.

Wyoming law, for example, prohibits Department of Education student data from being sold to private entities.

Missouri law requires the Department of Education to ensure that contracts involving student data include provisions prohibiting vendors from selling student data or using it in furtherance of advertising (there are exceptions for local vendors using directory information). Similarly, **California** law requires that local educational agencies prohibit contracted

California's SOPIPA: A Landmark Law

While most states focused their laws on educational institutions — putting in place new governance standards, data-collection rules, or contracting requirements — California regulated industry directly with the Student Online Personal Information Protection Act (SOPIPA). SOPIPA charges ed tech providers themselves with protecting student information while permitting innovation and customized and digital learning. It was passed unanimously by both chambers of the California legislature in 2014. It is model, comprehensive legislation that directly addresses the companies who are collecting massive amounts of student data and who may face few restrictions in their use (or misuse) of such data. These companies are often in the best position to make sure students' personal information is handled responsibly and securely.

SOPIPA has been hailed as "a landmark law" by President Obama[7] and *Ed Week*[8]. The *New York Times* refers to SOPIPA as "the most wide-ranging" of state student privacy laws, calling California "the first state to comprehensively restrict how [student] information is exploited by the growing education technology industry."[9]

- SOPIPA sets forth requirements for websites, online services, and mobile apps that are designed, marketed, and used primarily for K–12 school purposes. The law **prohibits**:
    - **Targeted advertising** to students or families based on students' personal information;
    - **Profiling** based on students' personal information (except for school purposes);
    - **Selling** students' personal information; and
    - **Disclosing** students' personal information (with limited exceptions to permit site functionality or as required by law).
- SOPIPA also protects the security of students' data and **requires**:
    - **Reasonable data security** for student information; and
    - **Deletion** of student information upon the school's request.
- SOPIPA enables innovation without encroaching on student privacy, because it allows companies to use **de-identified** K–12 student information internally to improve educational products/services and allows sharing of **aggregated de-identified** student data for development of educational sites, services, and apps.
- SOPIPA covers a broad range of K–12 online companies, including websites, services, and apps that may be used with or without a contract.
- SOPIPA is enforceable directly against companies. This can make it a more effective tool in protecting student privacy than FERPA and laws only enforceable against schools.

Schools and teachers support SOPIPA because it relieves some of the burdens of monitoring for them by establishing a clear baseline and rules of the road for companies. And, because SOPIPA enables innovation, members of the ed tech community have publicly supported it as well.[10] SOPIPA ultimately passed unanimously with no opposition.

[7] *President Barack Obama, Remarks at the Federal Trade Commission (Jan. 12, 2015) (transcript available at http://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission).*

[8] *Benjamin Herold, Student Data Privacy in 2014: Revelations, Legislation, Controversy, Ed Week (Dec. 26, 2014) (available at http://blogs.edweek.org/edweek/DigitalEducation/2014/12/student_data_privacy_year_in_review.html?cmp=SOC-SHR-TW).*

[9] *Natasha Singer, With Tech Taking Over in Schools, Worries Rise, New York Times (Sep. 14, 2014) (available at http://www.nytimes.com/2014/09/15/technology/with-tech-taking-over-in-schools-worries-rise.html?_r=1).*

[10] *Mike Lawrence, CEO of CUE, said that SOPIPA was "successful in putting in language that protects student privacy from advertising without limiting the innovation … " (See Tanya Roscorla, California Protects Student Data Privacy with Two Bills, Center for Digital Education (Sep. 4, 2014).) Mark Schneiderman of SIIA said that SOPIPA "seems to strike generally the right balance." Justin Hamilton, a spokesman for Amplify, said that "[SOPIPA's rules] are the standards and commitments that we already live up to and that we think every company working with school districts should live up to." (See Benjamin Herold, "Landmark" Student-Data-Privacy Law Enacted in California, Ed Week (Sep. 30, 2014) (available at http://blogs.edweek.org/edweek/DigitalEducation/2014/09/_landmark_student-data-privacy.html).)*

vendors from using student personally identifiable information for targeted advertising.[11] And in **Idaho**, the state board must ensure that contracts involving individual student data either prohibit sales, marketing, or advertising use of such data or specifically disclose in detail such uses of data and obtain express parental consent.

In **New York**, the law prohibits educational agencies and third-party contractors from selling personally identifiable information or using it for marketing purposes. In addition, the law includes a parents' bill of rights, which is to be included in all contracts and which reiterates that a student's personally identifiable information cannot be sold or released for commercial purposes. In **Colorado**, education department contracts involving personally identifiable data must prohibit outside vendors from using such data for commercial purposes. In addition, the department itself may not sell or monetize student data for commercial use.

2) Some laws contain consent exceptions and loopholes.

A few states restrict the commercial use of student data but contain potentially large exceptions that permit such use, such as when parents consent or when contracts stipulate otherwise. As noted above, **Idaho** allows contracted third-party vendors to use student data for sales, marketing, or advertising if they disclose in detail such uses and obtain express parental consent. **Louisiana** law, which on first blush offers a very broad prohibition on commercial use of data, has an escape clause: It prohibits any school system or government agency or public or private entity from selling, transferring, sharing, or processing student data for use in commercial advertising, marketing, or any other commercial purpose — unless otherwise stipulated in a contract for services.

Though at first it may sound appealing to allow parents, students, or schools to "consent" to commercial use of students' personal educational data, on closer inspection this idea is deeply problematic. The school context is a very unique one. With schools making many of the ed tech choices, parents and students are a captive user audience. Schools may feel pressured by operators to give or get consent to receive free or discounted products. Parents may easily feel pressured by schools to "consent" so their children can participate, or they may assume that the school has fully vetted the vendor and its privacy and security practices. Professor Joel Reidenberg of Fordham has called consent in this context "forced consent,"[12] and rightly so. And most K–12 students are not of appropriate age or level of understanding to give meaningful consent. In the school/educational context, it is better for students and parents if the law bars commercial use of student data outright, without creating loopholes for companies.

3) A few states passed laws directly addressing third-party service providers.

A few states recognized that not all ed tech falls under a contract. Sometimes, an individual teacher or student may simply download an app or visit a website. These states also understood that, in many instances, it may be better to directly regulate companies, because they can effectively manage their own policies and practices, rather than burden overstretched schools with additional oversight duties.

i. Two states addressed cloud-computing services.

Rhode Island and **Kentucky** passed laws **restricting data use by cloud-computing services.** Cloud-computing services under these laws provide educational institutions with account-based access to online-computing resources, such as email, document storage, and document editing. Rhode Island and Kentucky's laws prohibit "account-based" cloud-computing services from using educational data for commercial purposes, including advertising. Kentucky's law

[11] California was one of a handful of states to pass multiple student privacy laws. In California, two laws — SOPIPA and a complementary bill, AB 1584, which governs school contracts with vendors — work together to provide students using education technology strong privacy coverage. A third bill, AB 1442, requires that schools give notice before collecting students' social media information and puts limits on collection and retention of such information by schools or contracted third parties.

[12] Professor Joel Reidenberg, Testimony Before Committee on Education and the Workforce Subcommittee on Early Childhood, Elementary, and Secondary Education Hearing on "How Emerging Technology Affects Student Privacy" (Feb. 12, 2015) (video archive available at https://www.youtube.com/watch?v=zWgfszB03V0).

also prohibits cloud-computing services from selling student data or creating individual or household profiles for any advertising purposes. Both state laws also require contracted cloud-computing services to certify their statutory compliance in writing.

ii. California addressed all K–12 ed tech services.

California law goes beyond account-based cloud-computing services, prohibiting all K–12 websites, online services, and applications from selling student data or using students' personal information or persistent unique identifiers for targeted advertising. The Student Online Personal Information Protection Act (SOPIPA) **restricts data use by all eligible K–12 third parties, whether they're cloud services, websites students use for homework, or apps a teacher has downloaded before class.** Under California law, all personal student information, no matter where it is held, is to be used only for educational purposes. See California's SOPIPA, A Landmark Law (p. 7) for more details.

B. A few states did not directly address the commercial use of student data but nonetheless required that certain data be kept private or used only for educational purposes.

Some states focused less on the commercial use of data and instead addressed fears of data sharing primarily by and among states, districts, schools, and the federal government. In many instances, this reflects fears that students' standardized testing data will be used for far broader purposes than scoring the tests at hand. For example, **Tennessee** and **Ohio** both require that data collected during student testing shall be used only for tracking the progress and needs of students as well as, in Ohio's case, improving their academic progress. **New Hampshire** broadly prohibits the state from sharing personal student information, except with parents or students or in limited measures to testing entities. The testing entities may not use personal student information for test-data analysis and must destroy such information after verifying test takers.

C. Some states mandated further reports and studies on the commercial use of student data.

In addition, two states did not pass laws regarding the commercial use of data but, nevertheless, noting concerns, **created procedures for further study and consideration of the commercialization of student personal information.** **Maine** law requires a study and report on privacy concerns related to students' social media accounts, email, and the cloud. **Florida** law requires schools to consider commercial implications when designating information as "directory information." Directory information may be more widely shared, so long as parents and eligible students have been given notice and an opportunity to opt out.

Directory Information

Under FERPA, schools may disclose certain types of information, known as "directory information," without prior parental consent (so long as there was initial notice and an opportunity to opt out).[13] Directory information is described by the Department of Education as "information that is generally not considered harmful or an invasion of privacy if released"[14] and includes data such as names, addresses, telephone numbers, dates and places of birth, and school activities or honors. This exception allows schools and others to publish student information in publications such as yearbooks, drama programs, honor rolls, and news stories. It also can allow companies to compile, use, share, and sell student information to prospective schools, employers, and far less scrupulous actors, such as data brokers, marketers, and scam scholarship purveyors.

[13] *34 C.F.R. §§ 99.3 and 99.37.*

[14] *U.S. Department of Education, "Family Educational Rights and Privacy Act (FERPA) Model Notice for Directory Information" (available at https://www2.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html).*

Most new student privacy laws addressed data security, and some specifically considered data breaches, retention, and destruction.

In today's world of frequently publicized data breaches and hacker scares, keeping students' sensitive information safe and secure is one goal almost everyone can agree on.

A. Sixteen states addressed data security in 2014, typically mandating that a data security plan be developed or that data be kept securely by educational agencies or private (usually contracted) vendors.

In some instances, the states addressed concerns about security of student data in the cloud or maintained by private companies. This was an approach taken in **California**. Other states, such as **Indiana**, addressed concerns about the security of new statewide longitudinal data systems (SLDS). A number of states, including **New York** and **West Virginia**, now require schools and states to keep data securely as well as to insert contractual requirements mandating that contracted third-party vendors do the same.

The following states addressed data security in 2014.

- **California**
- **Colorado**
- **Idaho**
- **Indiana**
- **Kansas**
- **Kentucky**
- **Louisiana**
- **Missouri**
- **New York**
- **North Carolina**
- **Ohio**
- **South Carolina**
- **South Dakota**
- **Tennessee**
- **West Virginia**
- **Wyoming**

In addition, at least a handful of state laws require third parties to provide notification when data breaches occur. For example, **New York** and **Kentucky** require third-party contractors to provide notice in the event of a data breach. **California** requires that third-party contracts explain notice procedures in the event of a breach. And **Kansas** requires any entity (government or third party) holding student data or personally identifiable information to provide notice in the event of a security breach.

B. Numerous states passed data retention and disposal provisions.

One way to improve the security of students' personal information is to make sure it is destroyed — by educational agencies, schools, or third parties — when it's no longer needed, such as when a contract ends, a student has graduated, or a school requests deletion.

The following states are among those that passed laws in 2014 **requiring the destruction or disposal of data or plans for appropriate destruction and disposal**. In many instances, to the extent third parties must dispose of or destroy data, it is by contract. Thus, again, schools and education agencies often are the ones who must ensure compliance.

- **California**
- **Colorado**
- **Idaho**
- **Indiana**
- **Kansas**
- **Louisiana**
- **New Hampshire**
- **New York**

C. The majority of states moved to limit sensitive data collection.

A number of states moved to limit collection of particularly sensitive information. An additional way to secure and protect sensitive student information is not to collect it in the first place, particularly if its educational value is questionable, debated, or limited. The concept of data minimization, which has been endorsed repeatedly by the Federal Trade Commission and privacy experts, involves collecting only data that is needed, as well as disposing of it when it's no longer useful.[15] A number of states made the determination that it was unnecessary for educational purposes to collect certain particularly sensitive data about students and their families.

[15] *The Future of Privacy Forum and Software & Information Industry Association's Student Privacy Pledge of 2014, which has over 100 signatories, incorporates data-minimization principles. Pledge signers commit, among other things, not to collect or retain students' personal information beyond what is needed for authorized educational/school purposes. See http://studentprivacypledge.org/?page_id=45.*

Biometric Data

Biometric data is data regarding the measurement of physical attributes. Laws targeting biometric data collection are typically concerned with the collection of unique biometric data that would identify an individual, such as fingerprints, palm prints, iris and retina scans, voiceprints, DNA sequences, and facial features. Some states also include handwriting or signature characteristics.

Schools may use biometric information for a number of purposes, including taking attendance, verifying identities, and allowing students to make lunch purchases.

One type of sensitive data gained a lot of attention: biometric data. States vary in their precise definitions of biometric data, and some do not clearly define it. Particularly for the states that have flat prohibitions, there may be some unintended consequences. For example, if a law prohibits collecting biometric data and biometric data includes handwriting, that would seem to encompass a lot of traditionally collected student work. In addition, a law prohibiting the collection of voice data could have unintended consequences for students with special needs.

The following twelve states **prohibit or restrict the collection or retention of biometric data**.[16]

- **Colorado**
- **Florida**
- **Idaho**
- **Kansas**
- **Louisiana**
- **Missouri**
- **New Hampshire**
- **New York**
- **North Carolina**
- **Ohio**
- **Tennessee**
- **West Virginia**

Five states **prohibit collection of information about family ownership of guns or firearms: Idaho, Louisiana, South Dakota, Tennessee, and West Virginia**.

States also moved to restrict collection of other data. For example, **California**, **Rhode Island**, and **Louisiana** passed laws that **restrict or prohibit the collection of social media password or profile information**. **Kansas** law **prohibits tests or surveys about sex, family life, or morality**. And **Ohio** law **prohibits the collection of political or religious information during state testing**.

States passed laws regarding governance and transparency.

States also passed laws in 2014 that sought to improve data-governance procedures and practices.

A number of state laws took a "governance" approach, seeking to improve accountability and data-management practices among schools and districts and to increase access and transparency for parents.[17] **Colorado**, **Missouri**, **North Carolina**, and **West Virginia**, for example, incorporated this approach, requiring state boards of education, schools, and districts to publish data inventories, develop procedures for research requests, and ensure ongoing compliance with existing federal privacy laws such as FERPA. **Louisiana** passed a law requiring state and local education agencies to publicly post what student information they transfer. Many of these laws also typically require that contracted parties handle data securely.

These are laudable steps and help to address concerns of parents who have no idea what information is being collected from their children or how it is being handled — or by whom. Publishing data inventories increases transparency for families and may cause schools to consider more closely whether all the information they collect is truly needed, thereby limiting data collection. Having procedures in place before data is given to researchers or third-party contractors helps to increase accountability and may ultimately improve trust in the system.

These practices can be complementary to other privacy protections and restrictions on data use discussed above. But unfortunately, given today's ed tech landscape, governance, accountability, and transparency procedures for educational institutions alone do not go far enough.

[16] *Oklahoma also passed a broader Parent's Bill of Rights (HB 1384), which — among many other things — addresses parents' rights with respect to biometric-data collection.*

[17] *Some of these bills appear modeled after the Student Data Accessibility, Transparency, and Accountability Act put forth by the American Legislative Executive Council and modeled after an Oklahoma 2013 law (model bill available at http://www.alec.org/model-legislation/student-data-accessibility-transparency-accountability-act/).*

III. Looking Ahead

States continue to move forward with new bills to address K–12 student privacy. By the beginning of March 2015, more states had introduced more bills than in the entirety of 2014.[18]

A number of states are considering or have already acted upon new student privacy legislation in 2015. Even the United States Congress has student privacy legislation under consideration. Several of the 2015 bills look more directly to ed tech providers than did the laws in 2014, which Common Sense supports as a good step. A number also are attempting to improve transparency and governance procedures. All reflect the growing importance of this issue for parents, educators, and policy makers across the nation. However, pitched battles between corporate interests and the public interest are playing out across the country.

While the legislative landscape is still in flux, Common Sense is hopeful that legislators around the country will continue to give this important issue deep consideration and develop laws that protect one of our nation's most valuable resources: our students. In crafting laws that will protect our nation's students while allowing them and their schools to benefit from ed tech, legislators should consider regulations that allow for innovation in education and at the same time prevent students' data from being misused or commercialized. Students' personal information can and should be used to enhance learning and further educational purposes. But it should only further educational purposes, not corporate interests. And, given the uniqueness of the school context, bans on commercial use of students' personal information should be firm — not subject to parental or student consent. Robust security, retention, and disposal standards also are vital in creating trusted online learning environments. And legislators can support transparency and data-minimization principles in data collection, both on the part of the schools and education agencies and on the part of ed tech providers. In crafting bills, legislators should recognize that, in many instances, ed tech companies themselves are in the best position to ensure that they comply with any new standards. And ed tech companies benefit from having clear rules of the road, which legislation can provide.

Common Sense is actively working in states across the country for strong student privacy legislation. For a look at current state action and Common Sense activity, please visit us at www.commonsensemedia.org/kids-action/issues

[18] *See Data Quality Campaign, Ed Data Update 3/6/2015, at http://dataqualitycampaign.org/blog/2015/3/eddata-privacy-update-3-6-2015, noting that 128 bills had been introduced in 39 states as of March 6, 2015.*

Appendix 1: 2014 State Statutes

California (AB 1442–Cal. Educ. Code §49073.6)

California (AB 1584–Cal. Educ. Code §49073.1)

California (SB 1177–Cal. Bus. & Prof. Code §22584)

Colorado (HB 14-1294–Colo. Rev. Stat. §22-2-309)

Florida (HB 195, SB 188–Fla. Stat. §1002.222)

Idaho (SB 1372–Idaho Code Ann. §33-133)

Indiana (HB 1003–Ind. Code. §22-4.5-10, sections amended by Public Law 167)

Kansas (SB 367–Kan. Stat. Ann. §72-6215, et seq.)

Kentucky (HB 5–Ky. Rev. Stat. Ann. §61.931, et seq.)

Kentucky (HB 232–Ky. Rev. Stat. Ann. §365.720, et seq.)

Louisiana (HB 340–La. Rev. Stat. Ann. §51:1951, et seq.)

Louisiana (HB 946/1076–La. Rev. Stat. Ann. §17:3914)

Louisiana (HB 1283–La. Rev. Stat. Ann. §17:3913)

Maine (LD 1194–126th Session Me. Laws, Resolve, Chapter 112)

Missouri (HB 1490–Mo. Rev. Stat. §160, sections amended by HB 1490)

New Hampshire (HB 312–N.H. Rev. Stat. Ann. §359-N)

New Hampshire (HB 1587–N.H. Rev. Stat. Ann. §189:65, et seq., §193-E:5)

New York (AB 8556, SB 6356–N.Y. Educ. Law, §2-C, §2-D)

North Carolina (SB 815–N.C. Gen. Stat. §115C 402.5, §115C 402.15)

Ohio (HB 487–Ohio Rev. Code §3301.0714 (as amended by HB 487), §3301.947)

Rhode Island (SB 2095, HB 7124–R.I. Gen. Laws §16-103-1, et seq., §16-104-1)

South Carolina (H. 3893–S.C. Code Ann §59-1-490)

South Dakota (SB 63–S.D. Codified Laws §13-3-51 et seq.)

Tennessee (HB 1549, SB 1835–Tenn. Code Ann. §49-1-309, §49-1-701, et seq.)

West Virginia (HB 4316–W. Va. Code §18-2-5h)

Wyoming (SB 79–Wyo. Stat. Ann. §21-2-202)

Appendix 2: 2014 State Law Privacy Matrix

State	CA*	CO	FL	ID	IN	KS	KY*	LA*	ME	MO	NH*	NY	NC	OH	RI	SC	SD	TN	WV	WY
Expressly prohibits ed tech providers from non-educational profiling	Y	N	N	N	N	N	Y [2]	N	N	N	N	N	N	N	N	N	N	N	N	N
Prohibits ed tech providers from advertising/marketing with student data	Y	N	N	N	N	N	Y [2]	Y [3]	N	N	N	N	N	N	Y [2]	N	N	N	N	N
Prohibits ed tech providers from selling student data	Y	N	N	N	N	N	Y [2]	Y [3]	N	N	N	N	N	N	N	N	N	N	N	N
Requires data security and/or breach planning by ed tech providers	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N
Requires contracts to expressly prohibit vendors from non-educational profiling	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Requires contracts to prohibit vendors from advertising/marketing with student data	Y	Y	N	Y [1]	N	N	N	N [3]	N	Y [4]	N [5]	Y	N	N	N	N	N	N	N	N
Requires contracts to prohibit vendors from selling student data	Y	N	N	Y [1]	N	N	N	N [3]	N	Y [4]	N [5]	Y	N	N	N	N	N	N	N	N
Requires ed tech vendor contracts to include data security and/or breach planning	Y	Y	N	Y	N	Y	Y	Y	N	Y	N	Y	Y	N	N	N	N	Y	Y	N
Expressly prohibits educational agency/ state from non-educational profiling	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Prohibits educational agency/state from advertising/marketing with student data	N	Y	N	N	N	N	N	Y [3]	N	N	N [5]	Y	N	Y [6]	N	N	N	Y [6]	N	N
Prohibits educational agency/state from selling student data	N	Y	N	N	N	N	N	Y [3]	N	N	N [5]	Y	N	Y [6]	N	N	N	Y [6]	N	Y
Requires data security and/or breach planning by educational agency or state	N	Y	N	Y	Y	Y	Y	N	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y

* Multiple statutes - (CA: AB 1442, AB 1584, SB 1177; KY: HB 5, HB 232; LA: HB 340, HB 946/1076, HB 1283; NH: HB 312, HB 1587)

1. Prohibited unless fully discloses secondary uses to state board and obtains prior express parental consent
2. Applies to cloud computing services only
3. Contract can specifically allow for commercial use
4. With exceptions for local service providers who only have directory information
5. The state shall not provide student personal information for any purpose, except to testing entities
6. Applies to testing data only

Assessing State Laws on Student Privacy in 2014 and Beyond

A School Privacy Zone Update from Common Sense Kids Action

www.commonsensemedia.org/kids-action

Credits

Authors: **Ariel Fox Johnson, Joni Lupovitz**
Research Support: **Harrison Stark**
Copy Editing: **Jenny Pritchett**
Design: **Dan Ramsey**

About Common Sense Kids Action

Common Sense Kids Action is an independent, non-partisan and powerful voice whose mission is to make kids and education America's top priority. We work with national and state leaders to advance policies that help ensure every child has the opportunity to succeed. Kids Action is committed to advancing a 21st Century Kids and Education agenda—an agenda that includes ensuring that all children 0-5 have access to vital health and education resources, advancing 21st Century learning, reducing child poverty, and protecting children's online privacy. Learn more at **www.commonsensemedia.org/kids-action**.

For inquiries, contact **kidsaction@commonsense.org**.

About Common Sense

Common Sense is a nonprofit, nonpartisan organization dedicated to improving the lives of kids, families, and educators by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology.

OUR OFFICES

SAN FRANCISCO	650 Townsend Street, Suite 435, San Francisco, CA 94103	(415) 863-0600
NEW YORK	1230 Avenue of the Americas, 3rd Floor, New York, NY 10020	(212) 315-2675
WASHINGTON, D.C.	2200 Pennsylvania Avenue, NW, 4th Floor East, Washington, DC 20037	(202) 350-9992
LOS ANGELES	1100 Glendon Avenue, 17th Floor, Los Angeles, CA 90024	(310) 689-7535

common sense®