On the Block: Student Data and Privacy in the Digital Age

The Seventeenth Annual Report on Schoolhouse Commercializing Trends —2013-2014

Alex Molnar and Faith Boninger

University of Colorado Boulder
April 2015

National Education Policy Center

School of Education, University of Colorado Boulder
Boulder, CO 80309-0249
Telephone: (802) 383-0058

Email: NEPC@colorado.edu
http://nepc.colorado.edu

The annual report on Schoolhouse Commercialism trends
is made possible in part by funding from Consumers Union
and is produced by the Commercialism in Education Research Unit.

Briefs published by the National Education Policy Center (NEPC) are blind peer-reviewed by members of the Editorial Review Board. Visit http://nepc.colorado.edu to find all of these briefs. For information on the editorial board and its members, visit: http://nepc.colorado.edu/editorial-board.

Publishing Director: **Alex Molnar**

Suggested Citation:
Molnar, A. & Boninger, F. (2015). *On the Block: Student Data and Privacy in the Digital Age—The Seventheenth Annual Report on Schoolhouse Commercializing Trends, 2013-2014.* Boulder, CO: National Education Policy Center. Retrieved [date] from http://nepc.colorado.edu/publication/schoolhouse-commercialism-2014.

On the Block: Student Data and Privacy in the Digital Age

Seventeenth Annual Report On Schoolhouse Commercializing Trends, 2013-2014

Alex Molnar and Faith Boninger
University of Colorado Boulder

Executive Summary

Computer technology has made it possible to aggregate, collate, analyze, and store massive amounts of information about students. School districts and private companies that sell their services to the education market now regularly collect such information, raising significant issues about the privacy rights of students.

Most school districts lack the resources to manage all of the student data that federal and state laws now require that they collect and report. As a result, they are likely to hire private vendors to identify, collect, manage, and analyze student data. This has opened up opportunities for private vendors to access student information and to share it with others. Further, the computerization of student work offers opportunities for companies that provide education technology and educational applications to obtain and pass on to third parties information about students.

Which information may be appropriately collected, who has a right to see it, how long the information may be held, and how errors and inaccuracies are to be corrected have become critical policy issues. Important in this mix is that student information, even information in the form of "anonymized" meta-data (or massive amounts of data reported without linking specific information and individuals), is valuable to marketers interested in selling products and services to students and their families.

Because of these critical concerns, this year's report on school commercializing trends reviews the policy landscape related to student data and assesses the dangers associated with the dearth of policies to protect students and their families from third parties who wish to profit from access to information collected through schools.

As legislators develop statutory language and district leaders develop their contracting policies, we recommend that they review the comprehensive guidelines detailed in the Electronic Privacy Information Center's *Student Privacy Bill of Rights*. We also recommend that policymakers develop policies that encompass not only the privacy of student educational records but also the wide variety of student data (including anonymized data that may now be collected and shared). These policies should explicitly

address the potential commercial use of any data collected. Finally, we recommend that the burden of protecting student data be placed not only on schools and districts but also on any private vendors with access to student data. This would align the interests of all parties, public and private, in protecting student privacy.

On the Block:
Student Data and Privacy in the Digital Age
Seventeenth Annual Report on Schoolhouse Commercializing Trends, 2013-2014

Student data is now big business. Computer technology has made it possible to aggregate, collate, analyze, and store massive amounts of information about students—and it has concurrently created opportunities for private vendors to access and share such information. Most school districts, for example, don't have the resources to manage all of the student data that federal and state laws now require that they collect and report. As a result, private vendors are commonly hired to design and run systems to identify, collect, manage and analyze student data, raising significant issues about the privacy rights of students.

Which information may be appropriately collected, who has a right to see the information, how long the information may be held, and how errors and inaccuracies are to be corrected have become critical policy issues. Add to this mix of issues the reality that student information, even information in the form of "anonymized" meta-data, is valuable to marketers interested in selling products and services to students and their families. Whether vendors or schools themselves should be allowed to sell student information to third parties to use as they like is just one of several important questions that remain largely unaddressed by law or policy.

This year's report on school commercializing trends reviews the policy landscape related to student data and assesses the dangers associated with the failure to enact policies to protect students and their families from third parties who wish to profit from their access to information collected through schools.

Digital Marketing to Children

The interactive nature of the Internet offers marketers many ways to reach children. Marketers create brand presence for children to interact with in the virtual worlds, social networks, and instant messaging environments in which they live. As early as 2001, *Business Week* reported that 98% of children's websites permitted advertising, and that more than two-thirds of websites designed for children relied on advertising as their primary revenue source.[1] In 2009, the digital measurement company comScore Inc. reported that U.S. Internet users of all ages viewed a total of 4.5 trillion display ads during 2008, with the average person viewing more than 2,000 ads per month.[2]

Marketers attract children to branded entertainment sites, to watch and pass on "viral" commercial videos made for viewer dissemination. Children are also invited to become

brand advocates by engaging in buzz marketing and by creating their own advertisements for products.[3]

Schools as Digital Marketing Venues

Children encounter digital marketing when they use technology on their own during "private" time, but they also increasingly encounter it as part of their schooling. To some extent students themselves drive this development; for example, it only makes sense for high school sports teams to communicate via social media, where teens communicate anyway. Teachers and schools, however, don't just go where the students already are; they also encourage students to spend more time immersed in virtual environments. It is, therefore, important to consider whether schools' efforts to promote student use of the Internet is being done in a responsible way and for age-appropriate, educationally valid reasons.

Schools now routinely incorporate digital technology in the form of educational software, educational websites, and 1:1 programs that provide laptops or tablets to each student, allowing and encouraging teachers to incorporate technology into their lessons.[4] A 2014 study released by the Sesame Workshop reported that 74% of K-8 teachers use digital games for instructional purposes, with 55% of teachers reporting that they assign digital game playing to their students at least weekly.[5] Whereas 80% of teachers reported that their students primarily play games specifically created for an educational audience, 13% reported their students playing commercial games or commercial games that have been adapted for educational use.[6]

In addition, expansion of technology in schools is being constantly promoted in a wide variety of venues and by a wide variety of players—via webinars for educational professionals, articles addressed to both professionals and parents, professional organizations such as edWeb.net, non-profits such as Common Sense Media, and professional publications such as *Education Week*.[7] With so many advocates, yet more technology in school activities—creating still more opportunity for marketing to children—appears inevitable.

Schools as Portals to the Internet

As children move around the Internet, using educational sites and jumping off from them to surf other sites, their activity is constantly tracked and recorded for future use.[8] A 2014 *Politico* article pointed out that students are tracked by education technology companies as they play online games, watch videos, read books, take quizzes, and work on assignments from home.[9] The data recorded may include information about their locations, homework schedules, Internet browsing habits, and academic progress.[10] Students also create marketable profiles when they take surveys in school and when they take standardized tests.[11] Because these data are not part of the "educational record" protected under the Family Educational Rights and Privacy Act of 1974 (FERPA), they may be used to target marketing to children and their families, or to build profiles on them that

would be of interest to such potential purchasers as colleges, universities and businesses that seek to market products to students, as well as to potential employers or military recruiters.[12]

The Nature of the Internet as a Marketing Environment

When schools direct children to the Internet, even for educational purposes, they put them in an environment full of marketing. Children are likely to wander off of education sites to other sites to play (and be marketed to), but even if they don't wander and do stay focused on their work, many sites that claim to be educational or that children use for educational purposes (such as search engines, educational game sites, or research help sites) serve them ads while they work.[13] Some of these ads are for things that look like fun for children, and many children will, not surprisingly, click through to have a look.

For example, we spent a little time playing on www.funbrain.com, a site that offers games to help make learning to standards more fun for children.[14] When we played Math Baseball (at a level that an elementary school student might play), among the ads we were served were some for products related to www.Poptropica.com, Funbrain's parent site. The ad for "the ultimate Poptropica sticker collection" led to an opportunity to buy the stickers along with an assortment of games and books. The ad for Popotropica music led to an opportunity to purchase it from Amazon or iTunes.

The ability to track visitors makes the Internet a different kind of advertising environment than, for example, a baseball stadium filled with ads directed at baseball-lovers, or even than a school littered with advertising directed specifically toward children. When marketers track a child's activity on her computer, they can specifically direct ads to that child based on her activity. For the purpose of serving ads to this child, her name and other identifying information do not really matter; the behavior that indicates her likes and dislikes is much more important.[15]

Behavioral tracking is part of a "360-degree" marketing strategy that targets children wherever they may be and engages with them in as many environments as possible (including television, off-line, and online).[16] Whereas marketers cannot monitor children's television viewing and other off-line activities, they can and do monitor children's online behavior and record the data for the purpose of subsequently targeting marketing to them.[17]

Websites' privacy policies are often long, complex documents and few people read them before clicking "accept." Nevertheless, they can be revealing to anyone who takes the time to consider what is being asked of them. Funbrain's privacy policy, for example, explains that it collects "personal" and anonymized information. Its parent company, Family Education Network (FEN—a subsidiary of Pearson Education, Inc.) "collects IP addresses for system administration, to report aggregate information to our advertisers, sponsors, and partners, and to audit the use of our site."[18]

FEN does not "knowingly collect, use, or distribute personal information from children under the age of 13 without prior verifiable consent from a parent or guardian." When we played math baseball, however, we were not asked to report our ages. FEN does not take responsibility for the activity of other sites to which users may connect via its site—for example, Amazon or iTunes, where we could have purchased stickers, books, or music, and other sites we could have explored from there.[19]

Privacy policies need not be complex. For example, the policy could be as simple as "We will not knowingly share any information with anyone for any purpose and we will not market to you." Commonly, however, privacy policies are very complex documents that appear designed to obscure and protect advertising and other potential revenue-generating opportunities.

When children enter the Internet environment, even if they enter from a responsible site with a transparent privacy policy, they are quickly exposed to other commercial sites that may be less concerned about their privacy. For parents and educators the hard truth is this: When schools send children into the open online environment, they are in reality often offering up these children to be tracked for the purpose of serving them ads for products that algorithms predict what they will want to buy.

Tracking software also records adult behavior on the Internet, of course, although many adults may be unaware of it. Since educators are, however, responsible for the children entrusted to their care, they cannot afford to be uninformed about potential threats to student privacy. Educators are obliged not only to learn how student data may be gathered and exploited but also to develop privacy policies that protect their students from such exploitation.

Concerns about the Collection and Tracking of Student Data

Trends in parent activism and legislative activity suggest that stakeholders primarily worry that companies will collect, sell, and use for advertising purposes information that personally identifies children, such as their names, Social Security numbers, addresses, and telephone numbers.[20] They also worry that companies will hold and sell students' data, allowing colleges, employers, medical insurance providers, and other future decision-makers to make consequential decisions about them.[21] Privacy policies, contracts, or laws that prohibit collection of personally identifiable data, can address this concern.

There is also much concern about the possibility of data security breaches[22]—and for good reason. When tech-savvy parents examined the security provided by software used in their children's classes, they found weaknesses that could have allowed unauthorized users to access children's private information.[23] One of these parents, Tony Porterfield, continued his investigation to examine nearly 20 products used by schools and districts, including school-district-wide social networks, classroom assessment programs, and learning applications. He told the *New York Times* that he found several potential security risks, only some of which were addressed when he alerted the companies responsible.[24]

Parents and legislators seem to worry much less about companies collecting behavioral tracking data that does not personally identify children than they do about the collection of unique personal information. Although these data are anonymized (the marketer doesn't really care who they are in this instance), they can be used to target children with ads matched to their particular interests. And even without a child's name or Social Security number, a company with enough other details about that child can trace her back and identify her.[25] Privacy policies, contracts, or laws that prohibit collection of personally identifiable data do not address this issue.

The Rise and Fall of inBloom

To help streamline the use of data collected about students, the Bill & Melinda Gates Foundation and the Carnegie Corporation of New York funded a non-profit organization, called inBloom, to provide a "vendor-neutral data service." The idea of the service was, purportedly, to serve as a repository for all the information collected about students, "to make it easier for teachers, parents and students to get a coherent picture of student progress, give them more options to be involved and informed, and make learning more engaging for students."[26]

Several states and districts, including Colorado, Delaware, Georgia, Illinois, Kentucky, North Carolina, Massachusetts, Louisiana, and New York, initially signed up to participate in inBloom's data collection effort, and in March 2013, the *Atlanta Business Chronicle* reported that 21 education technology companies had already announced plans to develop applications to work with inBloom.[27] By the end of the 2013-2014 school year, however, the tide had turned: every one of the participating states and districts had pulled out. What happened?

Advocacy groups such as Campaign for Commercial-Free Childhood, Class Size Matters, NYC Public School Parents, and a band of progressive education bloggers (including Carol Burris, Jason France, Susan Ohanian, and Diane Ravitch) opposed the mass adoption of inBloom[28] and helped rally opposition to the program.

Critics questioned inBloom's commitment to and ability to protect student privacy. In particular, they challenged the motives of its funders and partners, particularly Rupert Murdoch's News Corp, whose subsidiary, Wireless Generation, built part of the inBloom software infrastructure. They also questioned the security of the system and the potential violations of privacy associated with the massive collection and maintenance over time of personally identifiable student data.[29]

inBloom's responses to these concerns did not reassure its critics. It claimed that neither funders nor partners would have access to student data and that vendors would be allowed to access student records through inBloom only if the relevant state or district allowed it.[30] With respect to data storage and disclosure, it asserted that its Data Store provided "the privacy and security functionality required by" the Family Educational Rights and Privacy Act (FERPA)[31]; that each state and district was responsible for the security of its own

students' data; and that according to FERPA, districts may disclose personally identifiable student information if they want to.[32]

Also, inBloom did not provide an option to "opt out." Parents who wanted to opt out were referred back to their school district.[33] Significantly, decisions about whether to sign on with inBloom, along with the policy that would encourage districts to use its services, were made at the state level. Once a state opted in, it became extremely difficult for school districts to opt out.[34]

The development and initial adoption of inBloom illustrates the intersection of corporate-friendly education reform and commercializing activities in schools.[35] Districts need the technology offered by additional vendors to comply with the testing requirements of the Common Core State Standards and of legislation that requires them to offer online learning and testing. They also need the technology to inform their own decision-making. But to the extent that private vendors are collecting or storing the data, its collection for purposes of school district decision-making is linked to potential commercial use. Unless specifically prohibited from doing so contractually or by law, a private vendor who is contracted to collect or hold data for purposes of legitimate district decision-making may also use those data for its own commercial purposes or share it with third parties who do.

Therefore, while inBloom may have been abandoned, the need to protect student data remains an issue for advocacy and policy.[36] The trend of collecting and using student data shows no sign of slowing. The threats posed by districts contracting with a variety of vendors remain.[37] Without expertise or legal protection to help them navigate the contracts presented to them, districts may sign off on contract language that does not adequately protect student privacy.[38]

Opportunity for a "California Effect"

A December 2013 report released by the Center on Law and Information Policy at Fordham Law School examined district contracts with third-party data-cloud-providing services and found that 95% of districts now rely on cloud-services providers for a wide variety of services, such as data mining for student performance, support for classroom activities, student guidance, and data hosting.[39] However, fewer than 25% of the agreements specify the permitted purposes for disclosures of student information, fewer than 7% of the contracts restrict the sale or marketing of student information by vendors, and many agreements allow vendors to unilaterally change the terms. Many also allow vendors to retain student data into perpetuity.[40]

Joel Reidenberg, the lead author of the Fordham report, warned that districts do not have the expertise to ensure that the contracts they sign with vendors adequately protect student privacy. Moreover, in the absence of formal policy, conditions (such as whether to include a field for Social Security number, for instance) are dictated by the technological choices made by private companies, companies whose interests are first and foremost to promote profits and avoid liability, not to protect student privacy.[41]

In September 2014, California enacted three laws that address some of the concerns raised by the Fordham report and also regulate data that are not typically categorized as part of the educational record.

California Education Code §49073.6 regulates contracts for services that gather information about students from social media.[42] It explicitly forbids companies that provide a social media service from sharing the information collected, from selling the information, and from using the information for any purpose other than the contracted purpose, which may be school or student safety only. It requires educational agencies to inform parents and provide for public comment before contracting for service. Finally, it requires the service provider to offer students and their parents means to see, correct, or delete the information gathered about them, to delete individual student data when students turn 18 or disenroll, and to delete all student data completely upon completion of the contract.

California Education Code §49073.1 addresses the ownership of "pupil-generated content" (such as "essays, research reports, portfolios, creative writing, music or other audio files, photographs, and account information").[43] It requires that when an educational agency contracts with a provider to store or manage pupil-generated content, the contract must specify how students may retain ownership and control of it, and it must prohibit the service provider from using the content in any way other than specifically contracted for—including using personally identifiable information to target advertising.

When schools send children into the open online environment, they are in reality often offering up these children to be tracked for the purpose of serving them ads for products that algorithms predict what they will want to buy.

This law also requires contracts to include statements that specify that the educational agency—not the service provider—owns and control its students' records, to describe the precautions the service provider will take to ensure the security and confidentiality of student records, and to describe how the agency and the service provider will jointly ensure compliance with the FERPA.

California Business and Professions Code §§22584-22585 regulates Internet sites, online services, online applications, and mobile applications designed and marketed for K–12 school purposes.[44] It prohibits operators of such services from engaging in targeted advertising, from collecting information to create profiles of K–12 students (except as needed to meet the education purposes for which it was contracted), and from selling or disclosing students' information. This legislative enactment was described by the *San Jose Mercury News* as the "stiffest U.S. bill to protect K-12 students' online data."[45]

A week after California's governor signed these three laws, a group of 14 education technology companies spearheaded a voluntary pledge to protect student privacy, beginning January 2015.[46]

The companies promised to refrain from collecting, maintaining, using or sharing student personal information beyond that immediately needed for the contracted educational purposes, from selling student information, from using or disclosing student information for the purpose of developing behavioral targeting for advertisements to students, from knowingly retaining student personal information beyond the time period necessary to complete their contract, and from changing without notice their privacy policies or other policies regarding the use of student personal information.[47] The companies also promised to limit data collection to that needed for their contracted purpose, to disclose clearly in an easy-to-understand manner the nature of data collected about students and why it may be shared with third parties, to support parent access to and correction of student personally identifiable information, to protect the security of the data collected, and to make sure, in the event of an acquisition of the company, that its successor commits to the same safeguards.[48]

The industry's voluntary pledge and the new California student privacy laws are steps forward; however, key privacy issues remain unresolved. Microsoft and other "big players" in education technology immediately signed onto the pledge and 130 companies are currently signatories—Pearson has not yet signed on.[49]

In January 2015, President Obama announced a bipartisan effort to create a "Student Digital Privacy Act," presumably modeled on California's Student Online Personal Information Protection Act.[50] Although the text of this federal bill has not yet been made public, its stated intention is to limit use of data collected about students to "educational and legitimate research purposes."[51]

This type of action on the part of legislators and private companies aligns with public opinion. A January 2014 survey found that 86 percent of adult respondents agreed that "…oversight is necessary to ensure [children's] private information is not exploited for commercial purposes and stays out of the hands of the wrong people."[52]

Student Privacy Bill of Rights

Another step forward has been the *Student Privacy Bill of Rights*, produced by the non-profit Electronic Privacy Information Center (EPIC). It calls for greater rights for students (or their parents, if students are under the age of 18) over information about them that is collected, stored, and used by others in and around the educational system.[53] These rights make requirements on both companies and schools: to make transparent their data collection, security, and privacy policies; to specify in advance the purpose for which they collect any information and to refrain from reusing that information for any other purpose; to provide students the opportunity to see and correct any information collected about them; to secure any information collected; and to be held accountable by students for maintaining their rights.[54]

As reasonable as these proposed rights are, current federal and state privacy laws tend to fall short on one or more of them. The discussion that follows below reveals how.

The Legislative Landscape: Federal Law Regarding Student Privacy

Federal law protects student privacy via Section 1232h of the Education Code and the Family Educational Rights and Privacy Act of 1974 (FERPA). [55] Following are details on each.

Protection of Pupil Rights (20 U.S. Code § 1232h)

20 U.S. Code § 1232h addresses the collection, disclosure, or use of personal information collected from students for marketing purposes or for sale of the information. Local education agencies must notify parents of any activities involving collection, disclosure, or use of personal information obtained from students for marketing purposes and allow parents both the opportunity to inspect any data collection instruments and to opt their children out of any survey of protected information.[56] That is: districts and schools are still allowed to engage in gathering student information for marketing purposes—but they have to tell parents they are doing it and allow parents who are aware of privacy concerns to remove their children's information from the school's reach.

Family Educational Rights and Privacy Act (FERPA)

FERPA applies to any public or private elementary, secondary, or post-secondary school and any state or Local Education Agency (LEA) that receives federal funds, which in effect includes almost all public and private schools. It works by denying funding to any agency or institution that violates its regulations. FERPA's scope is limited to "educational records." That is, it excludes such items as data collected by education technology websites and applications and the "pupil-generated content" (essays and so on) now protected by California law. However, if such excluded materials contain Personally Identifying Information from education records, then they, too, are included in the law's protection.[57]

FERPA gives parents the right to obtain a copy of their institution's policy concerning access to educational records, to halt the release of personally identifiable information, and to review their children's education records and request corrections, if necessary.[58] Parents can also choose to opt out of its policy of allowing schools to release "directory information," which includes students' names and addresses, to the public. Originally, it also prohibited educational institutions from disclosing "personally identifiable information in education records" without parental consent.[59]

However, several FERPA exceptions allow for disclosure of student records to certain parties or under certain conditions without parental consent. For the purposes of our discussion, the most significant exception is that records may be released without consent to *school officials* with a legitimate educational interest and to organizations conducting

studies for or on behalf of a school, and also to *authorized representatives* of the U.S. Comptroller General, U.S. Education Secretary, or state educational authorities.[60]

Changes to FERPA in 2008 and 2011 expanded the definitions of both school officials and authorized representatives. The Department of Education now considers "school officials" to include "contractors, consultants, volunteers, and other parties to whom an educational agency or institution has outsourced institutional services or functions it would otherwise use employees to perform."[61] The Department also considers "authorized representatives" to be any individuals or entities that local or state educational authorities, U.S. Secretary of Education, or U.S. Comptroller General select as an authorized representative.[62] In other words, the law has been weakened in recent years to allow schools to provide data to private companies without parental consent.[63]

The Department of Education's guidelines of "best practices" for schools and districts recommends case-by-case evaluation of any online educational services to determine if FERPA-protected information is implicated; if so, of course, the school or district must ensure that FERPA requirements are met.[64] The guidelines also recommend that schools and districts maintain written contracts for any use of online educational services, and that these contracts contain provisions for: which data will be collected; with whom they may be shared; how they will be stored; how they will be secured; how they may be accessed by students, parents, and the school; when they will be destroyed; and whether the school or district may be indemnified for a vendor's failure to comply with relevant laws.[65] These guidelines, which do not hold the force of law, may help the schools and districts held responsible under FERPA to define their contract terms.

The Protecting Student Privacy Act of 2014: An Unsuccessful Attempt to Strengthen FERPA

In the summer of 2014, Senators Edward J. Markey and Orrin Hatch introduced the Protecting Student Privacy Act of 2014 to strengthen parent and student rights under FERPA. This bill would have prohibited agencies from entering into contracts with vendors ("outside parties") that do not secure sensitive student data or who use students' personally identifiable information to advertise or market to them. It would have required agencies to minimize the data provided to outside parties when possible and to maintain records of which outside parties had been given access to information. It would also have required outside parties to maintain lists of others to whom they had granted access and to destroy records after they had served their specified purpose. Finally, it would have provided parents the rights to know which outside parties might access their child's information and to review and amend the personal information held by outside parties.[66]

Had it passed, the Markey/Hatch bill would have increased protections to student privacy; however, it also fell short in important ways. The bill applied only to the official "education record" and left out data collected about students as they use education technology. Moreover, instead of putting an affirmative burden of compliance on outside parties with

access to student data, it placed oversight and enforcement with agencies that lack the resources and expertise to do so successfully.

The Legislative Landscape: State Laws Passed 2011-2014

We used the Open States and National Conference of State Legislatures databases to gather information about state legislative activity related to K-12 student privacy.[67,68] We found thirty-four bills related to student privacy that were signed into law between 2011 and 2014. The Appendix provides a list of these bills along with our analysis of their major provisions and gaps in protection, exclusions and omissions).[69] The number of privacy-related bills passed increased over time: 3 laws passed in 2011, 2 in 2012, 8 in 2013, and 21 in 2014.

Overview of Questions for Analysis of State Laws

We examined the 34 state bills to assess which data the laws address, the methods by which they protect those data, and—our primary interest—whether they insulate students from having information collected about them that may be used to market to them. In each area, we asked a variety of sub-questions.

First, we identified which data each law includes. More specifically, we asked whether the law addresses:

- data that is part of the educational record,
- data collected by education technology companies as part of their contracted work with a school or district,
- data collected by Internet websites and applications used by students for educational purposes, or
- data of some other kind.

Although protecting information in the educational record is a good start, as we have discussed, much data can be and is collected from students' use of educational technology and also from their use of computers in school.

Second, we assessed children's and their parents' rights regarding collected data. Here we asked whether parents (and children when they turn 18) have the right to see the information collected, to challenge it, or to opt out of its collection, storage, or use.[70] As things now stand, in many instances incorrect information can be spread about students without them or their parents having the right to see or correct it.

Third, we considered whether and how the laws protect students from unwarranted secondary use of their information. Here we asked whether state laws prohibit companies from using the data they collect or store for advertising and marketing purposes; we also

asked whether they must delete data after it has served its specified purpose. If data collection has a specific, declared educational purpose, and if it must be deleted after that purpose has been met, then students and parents can better trust that the information will not subsequently be used for other, unapproved purposes.

Finally, we asked whether and how the laws address the security of the information collected. Our first question in this area was whether the law requires that procedures for keeping data secure be specified. If so, then we asked who is to be held accountable for compliance: the school or district (Local Education Agency, or LEA), vendors, a state agency, or some combination of these. To the extent that any of these parties is held responsible for breaches of security or appropriate use of the data collected, they have a stake in ensuring that breaches do not occur.[71]

Findings: To Which Data Do State Laws Apply?

Twenty-nine of the student privacy-related laws passed by state legislatures in 2011-2014 address data collected and saved as part of students' individual educational records. Some state laws address narrowly defined educational data. Montana's 20-1-213 MCA, for example, addresses only basic school attendance data transferred from schools to the Montana Youth Challenge Program.[72] Other states, such as Oklahoma, enacted comprehensive legislation.[73]

Oklahoma's Student Data Accessibility, Transparency, and Accountability Act of 2013 covers: state and national assessment results; course taking and completion, credits earned, and other transcript information, including course grades and GPA; date of birth, grade level and expected graduation date/graduation cohort; degree, diploma, credential attainment, and other school exit information such as General Educational Development and drop-out data; attendance and mobility; data required to calculate the federal four-year adjusted cohort graduation rate, including exit and drop-out information; discipline reports limited to objective information needed to produce the federal Title IV Annual Incident Report; remediation; special education data; and demographic data and program participation information.[74]

Oklahoma also restricts the information that can be included as part of a student's educational record, specifically excluding the following from a student's educational record: juvenile delinquency records; criminal records; medical and health records; student Social Security number; and student biometric information.[75]

Some comprehensive state privacy laws exclude fewer items from potential data stores. North Carolina, for example, excludes only biometric information, political affiliation, religion, and voting history.[76] Other states exclude more. For example, New Hampshire's list of exclusions totals 22 items applying to students and their families, such as health insurance information, electronic addresses, and mental or psychological problems.[77]

Several states (Florida, Louisiana, Kansas, New Hampshire, New York, North Carolina, Ohio, and Oklahoma) explicitly forbid or limit the collection and use of "biometric"

information.[78] The definition of "biometric" in the New Hampshire statute is typical: "a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting."[79]

Overall, however, few states have addressed forms of data other than students' educational records. As discussed above, California regulates "pupil-generated content," social media services, and Internet sites, online services, online applications, and mobile applications designed and marketed for K–12 school purposes.[80] Other states that have taken a step beyond educational records include Colorado, which addresses online education services, including websites and applications, [81] and Rhode Island, which covers pupil-generated content and any data processed by cloud providers. [82]

In addition, both Louisiana and New Hampshire prohibit schools from demanding students' personal electronic account information. New Hampshire forbids electronic surveillance of students (to identify them, transmit information about them, or monitor or track them), without a public hearing leading to school board approval and parental consent.[83]

Findings: What Are Students' and Parents' Rights?

As noted above, FERPA gives parents the right to see their children's data. If they object to some aspect of the data stored, parents can submit a claim to the Education Department's Family Policy Compliance Office (FPCO) to "investigate, process, and review complaints and violations."[84] As federal law, FERPA is valid in all states. Although many of the state bills require schools and districts (LEAs) to annually alert parents of their rights under FERPA, only California and New York explicitly provide parents the right to correct their children's data.

California's Education Code §49073.1 requires contracts with vendors to include a description of the procedures by which a parent, legal guardian, or eligible student may review personally identifiable information in the student's records and correct erroneous information.[85] New York's Education Law §2-d calls for the creation of a parents' bill of rights that, according to the New York State Education Department, does the same thing; that is, it requires all contracts to contain information about how parents can challenge the accuracy of any data that is collected. However, it also explicitly denies parents the "private right of action," which would allow them to directly sue the Education Department or an educational agency.[86]

Some states allow parents to opt in or out of data collection, sharing, or both. Requiring parents to "opt in" is the stronger protection. New York requires parental opt-in for a company to release information[87]; Idaho requires it for secondary uses of the data[88]; Louisiana and Montana require it for release of personally identifying data[89]; and Kansas and Oklahoma require it for biometric data.[90] Oklahoma law allows parents to opt out for data other than information it considers necessary in the educational record.[91, 92]

Findings: How is Student Data Protected?

State laws may require that security measures be taken without specifying the nature of those measures. Alternatively, they may require such specific security measures as de-identification (via aggregation, encryption, or the assignment of unidentifiable codes), or the destruction of the data. Fourteen states require some kind of security measure. Only California, Kansas, New York, Rhode Island, and Oklahoma laws hold private companies responsible for security breaches; Texas holds researchers who obtain data responsible.[93]

Eight states require specification of how data will be used, or at least imply that requirement in their language (California, Colorado, Kansas, Idaho, New York, North Carolina, Oklahoma, and Wyoming).[94] Eight states require destruction of the data collected (California, Colorado, Kansas, Idaho, New York, Louisiana, North Carolina, and Wyoming).[95]

Of the 34 laws we examined, only eight (California, Colorado, Idaho, Montana, New York, Rhode island, and Wyoming) explicitly prohibit the use of data for commercial purposes.[96]

The Legislative Agenda: Much Remains Undone

Although a number of bills address student data privacy issues, legislatures have rarely addressed student data that are not part of official educational records. California and Colorado are the only states whose laws cover data that may be collected by companies providing education technology or websites and applications. Meanwhile, schools continue to send children to the Internet to conduct research and to work and play on education-related websites and mobile applications. By doing so, they in effect send them off unsupervised to sail the digital marketing seas—where they are susceptible to and targeted for marketing.

A significant improvement in children's privacy protections occurred in December 2012, when the Federal Trade Commission updated rules under the Children's Online Privacy Protection Act (COPPA). COPPA applies to children under the age of 13.[97] Among the rule changes are several expanded definitions closing loopholes that previously allowed third parties to collect personal information from children via "plug-ins." Also significant is an expanded definition of "personal information," which now includes location (such as street address and city) available from mobile devices; photos; videos; audio recordings; screen or user names; and persistent identifiers (such as "cookies" and other hidden software).

While these changes are significant, they apply only to children under the age of 13. However, teens are especially at risk, both because they are online more than young children both in and out of school, and because adolescents are particularly susceptible to targeted marketing.[98] Although it may be impossible to impose a parental approval requirement for the online activity of teens, teenagers' personal information needs to be safeguarded. Jennifer Harris and her colleagues at the University of Connecticut's Rudd Center for Food Policy and Obesity have argued, for example, that children need policy protections from unhealthy food marketing until the age of 14.[99]

Commercializing activities in schools threaten children's psychological well-being, their physical health, and the integrity of their education.[100] The use of digital technologies in education is pervasive and growing. While these technologies show great promise, they also hold the potential to harm students profoundly if not properly managed to insure that they serve the best interests of students. It is unrealistic to expect schools to reverse the trend toward the use of educational software, Internet websites, and mobile applications; the challenge now is to protect children from the potential harms to which these developments expose them.

Policy Recommendations

To the extent that schools continue to direct high school students to online resources, and because teens are so susceptible to digital marketing strategies, they should be protected from digital marketing in the same way that younger children are. We recommend that the Federal Trade Commission extend the Children's Online Privacy Protection Act (COPPA) protections to age 14, and strengthen the protections offered to adolescents ages 15-18.

FERPA might also be strengthened. While it gives parents the right to lodge a complaint with the Education Department, it does not give them the power to sue on their own behalf.[101] Further, the only opt-out right that FERPA offers parents is to opt out of the release of "directory" information. States that require local education agencies (LEAs) to inform parents of their federal rights, therefore, offer little useful support to parents.

Further, our review of national and state legislation on student data privacy suggests that in general, although some states have addressed important concerns, overall there are still many significant gaps in the privacy protections for students. Particularly limited are opportunities for parents to correct errors in the data collected about their children, or to opt out of data collection entirely.

Another significant gap is the failure to require LEAs and private vendors to specify in advance the purpose for which any given piece of information is collected, to limit the use of that information to its original intended purpose, and to require that the data be destroyed after serving its specified purpose. Such requirements would prevent the collection of more data than necessary and would also prevent LEAs and vendors from engaging in secondary use of the data, particularly for commercial purposes. Laws that require LEAs to provide public documentation of which data are being collected and for what purposes would encourage transparency and promote compliance.

Only a handful of states explicitly prohibit commercial use of the student information addressed in their legislation, or hold private companies legally responsible for breaches of student privacy or data security. Without explicit sanctions against vendors, vendors' motivation for profit may very well overcome their motivation to protect student privacy. Legislation that simply calls for transparency or that places the onus of compliance on state officials or districts rather than on vendors is not likely to effectively secure children's personal information or adequately protect them from commercial exploitation.

We recommend that legislators developing statutory language and district leaders developing contracting policies review the comprehensive guidelines offered by the Electronic Privacy Information Center's Student Privacy Bill of Rights before taking action.[102] These guidelines are stronger and more comprehensive than the 2014 "best practices" offered by the U.S. Department of Education.[103]

We also recommend that policymakers develop policies that encompass not only the privacy of student educational records but also the wide variety of student data (including anonymized data) that may now be collected and shared. These policies should explicitly address the potential commercial use of any data collected.

Finally, we recommend that the burden of protecting student data be placed not only on schools but also on any private vendors with access to student data. This would align the interests of all parties, public and private, in protecting student privacy.

Appendix

State Laws Addressing Student Data Privacy (2011-2014): Synopses of Major Provisions, Noting Significant Gaps in Protection, Exclusions and Omissions

State Laws Enacted in 2011

20-1-213, MCA (2013)
Montana House Bill 208 (2011)

Summary:
Requires that information that a student has dropped out to be sent to the Montana Youth Challenge program (i.e., a narrowly defined bill not intended to establish broad data collection or privacy rights)

Major Provisions:
- Applies to name, address, and dates of attendance only (i.e., information to be transferred to another state agency).
- Parents can opt out of sharing data with third parties.
- Implies that LEA would be held accountable for breaches.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes, but those are irrelevant in this case.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

Ohio Rev. Code Ann. § 149.381 (2014)
Ohio House Bill 153 (2011)

Summary:
As part of the state budget bill, excludes pupil records and FERPA-protected records from review by state historical society.

Major Provisions:
- Applies to educational record data with personally identifying information.
- Written parental request is required for data release.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Does not specifically require implementation of data security procedures.

Ohio House Bill 153 (2011) (continued)
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches.

Utah Code Ann. § 53A-13-301 (2014)
Utah House Bill 145 (2011)

Summary:
Applies FERPA to state and provides for rules to protect confidentiality of student information and records.

Major Provisions:
- Applies to educational record data.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches.

State Laws Enacted in 2012

A.R.S. § 15-241 (2014)
Arizona House Bill 2663 (2012)

Summary:
Relates to underperforming school districts, relates to reclassification of such schools. Establishes criteria for letter grading of schools, requires schools to submit the data and provides for family educational rights and privacy of student records.

Major Provisions:
- Applies to educational record data.
- Holds LEA accountable for breaches.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- With respect to challenging the accuracy of data, refers to FERPA.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

W. Va. Code § 18B-2A-3 (2014)
WV SB 661 (2012)

Summary:
Provides for the collection, synthesis, and dissemination of data from state agencies; relates to communication and cooperation among state education providers; directs institutional boards of governors to cooperate in certain data-related operations; requires reports; provides for privacy protection; authorizes the Commissioner of Workforce West Virginia to share data with certain education providers.

Major Provisions:
- Applies to educational record data.
- Holds individuals accountable for breaches of the law.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

State Laws Enacted in 2013

"An act relating to school safety," KRS § 158.448 (2014)
Kentucky House Bill 354 (2013)

Summary:
Among other items related to school safety, requires the Kentucky Department of Education to develop protocols for student records within the student information system that (1) provide notice to schools receiving the records of prior offenses committed by a student transferring to a new school or district and (2) protect the privacy rights of students and parents guaranteed under FERPA; requires school council to review performance data annually.

Major Provisions:
- Applies to educational record data.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- Refers to FERPA regarding parents' right to challenge the accuracy of data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches.

"An act relating to reorganization," KRS § 151B.132 (2014)
Kentucky House Bill 240/Senate Bill 83 (2013)

Summary:
Establishes Office for Education and Workforce Statistics to oversee and maintain Kentucky Longitudinal Data System.

Major Provisions:
- Applies to educational record data.
- Requires implementation of data security procedures.
- Requires the de-identification of personally identifying information.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- With respect to challenging the accuracy of data, refers to FERPA.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches of the law.

20-7-104, MCA (2013)
Montana Senate Bill 175 (2013)

Summary:
As part of a larger bill, applies FERPA and strengthens safeguards with respect to personally identifying information; prohibits superintendent from releasing personally identifying information to any entity without parental consent.

Major Provisions:
- Applies to educational record data, especially personally identifying information.
- Specifically restricts the use of data collection for advertising and marketing purposes.
- Parental opt-in is required for release of personally identifying information.
- Implies that the Superintendent of Public Instruction would be held accountable for breaches.

Gaps in Protection, Exclusions and Omissions:
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- With respect to challenging the accuracy of data, refers to FERPA.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

"Current Operations and Capital Improvements Appropriations Act of 2013," 2013 N.C. Sess. Laws 360
North Carolina SB 402 (2013)

Summary:
As part of a comprehensive bill, a nonpublic school that gets scholarship grant money must report aggregate scores of students.

North Carolina SB 402 (2013) (continued)

Major Provisions:

- Applies to educational record data.
- Holds the nonpublic school that enrolls scholarship students accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

ORC Ann. 3301.0714 (2014)

Ohio House Bill 59 (2013)

Summary

As part of a larger bill, requires the assignment of a data verification code to each student; prohibits the state Board of Education and the Education Department from having access to information that would enable any data verification code to be matched to personally identifying student data.

Major Provisions:

- Applies to educational record data.
- Requires de-identification of personally identifying information.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches.

"Student Data Accessibility, Transparency, and Accountability Act of 2013," 70 Okl. St. § 3-168 (2014)

Oklahoma House Bill 1989 (2013)

Summary:

Requires compliance with FERPA, provides for data inventory, requires a data security plan, requires contracts to include privacy and security provisions.

Major Provisions:

- Applies to educational record data; excludes biometric data from the educational record.
- Requires implementation of data security procedures.
- Requires the de-identification of personally identifying information.
- Requires specification of how collected data will be used.

Oklahoma House Bill 1989 (2013) (continued)

- State Board of Education and private vendors, when relevant, would be held accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- Refers to FERPA regarding challenging the accuracy of data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not require data to be destroyed following intended use.

"An act relating to education research centers and the sharing of educational data between state agencies; redesignating certain fees as charges," Tex. Educ. Code § 1.005 (2014)

Texas House Bill 2103 (2013)

Summary:

Establishes rules for sharing of education data with education research centers.

Major Provisions:

- Applies to educational record data.
- Requires implementation of data security procedures.
- Implies that the researcher involved would be held accountable for breaches in the law.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- Refers to FERPA regarding challenging the accuracy of data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

Utah Code Ann. § 53A-1-413 (2014)

Utah Senate Bill 82 (2013)

Summary:

Creates "Student Achievement Backpack" and requires ability for parents and authorized LEA representatives to access it.

Major Provisions:

- Applies to educational record data.
- Gives parents the right to see data collected about their child.
- Requires implementation of data security procedures.
- Holds State Board of Education accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not specifically give parents the right to challenge and correct data.

Utah Senate Bill 82 (2013) (continued)

- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

State Laws Enacted in 2014

"An act to add Section 49073.6 to the Education Code, relating to pupil records," Cal Ed Code § 49073.6 (2015):

California Assembly Bill 1442 (2014)

Summary:

Restricts use of information gathered from social media to school/student safety; restricts use of that information and requires it to be destroyed when no longer needed for original use.

Major Provisions:

- Applies to data obtained from social media.
- Explicitly restricts the use of data collection for advertising and marketing purposes; data can only be used to satisfy terms of contract, and cannot be sold or shared.
- Gives parents the right to see data collected about their child.
- Gives parents the right to challenge and correct the data.
- Requires specification of use before data is collected; data may be used only for school or student safety.
- Requires destruction of data after its use for its intended purpose is completed.
- Implies that LEA will be held accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not give parents the right to opt out of data collection, storage, or use.
- Does not require implementation of data security procedures.
- Does not require de-identification of personally identifying information.

"An act to add Section 49073.1 to the Education Code, relating to pupil records," Cal Ed Code § 49073.1 (2015)

California Assembly Bill 1584 (2014)

Summary:

Amends existing law to authorize an LEA to enter into a contract with a third party to provide services for the digital storage, management, and retrieval of pupil records, or to provide digital educational software, or both.

Major Provisions:

- Applies to educational record data.
- Specifically restricts the use of data collection for advertising and marketing purposes.
- Gives parents the right to see data collected about their child.
- Gives parents the right to challenge and correct data collected about their child.
- Requires implementation of data security procedures.
- Specification of use of the data is implied (by requirement to destroy the data after its intended use is completed).
- Requires destruction of data after its use for its intended purpose is completed.

California Assembly Bill 1584 (2014) (continued)

- Holds both LEA and private company accountable for breaches of the law.

Gaps in Protection, Exclusions and Omissions:

- Does not give parents the right to opt out of data collection, storage, or use.
- Does not require deidentification of personally identifying information.

"Student Online Personal Information Protection Act," Cal Bus & Prof Code § 22584 (2015)

California Senate Bill 1177 (2014)

Summary:

Prohibits an operator or an Internet website, online service, online application, or mobile application from knowingly engaging in targeted advertising to students or their parents or legal guardians, using covered information to amass a profile about a K-12 student, selling a student's information or disclosing covered information. Requires security procedures and practices of covered information, to protect information from unauthorized access, destruction, use, modification, or disclosure.

Major Provisions:

- Applies to Internet sites and applications.
- Specifically restricts the use of data collection for advertising and marketing purposes.
- Requires implementation of data security procedures.
- Requirement to de-identify personally identifying information is implied, but not specifically discussed.
- Specification of use of the data is implied.
- Requires destruction of the data upon completion of intended use.
- Holds LEA accountable for breaches of the law.

Gaps in Protection, Exclusions and Omissions:

- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.

"Student Data Protection, Accessibility, Transparency, and Accountability Act of 2014," C.R.S. 22-2-309 (2014)

Colorado House Bill 1294 (2014)

Summary:

Requires the state's Board of Education to maintain and publish an inventory of student-level data currently in the student data system, to develop policies to comply with federal privacy law, to use aggregate data; and to a develop data security template for LEAs. Prohibits the Department of Education from providing individual student data to organizations or agencies outside the state except under specified circumstances.

Major Provisions:

- Applies to educational record and to online education services, including websites and applications.
- Specifically restricts the use of data collection for advertising and marketing purposes.
- Give parents the right to see data collected about their child.
- Requires implementation of data security procedures.
- Requires de-identification of personally identifying information.
- Requires specification of how collected data will be used.
- Requires destruction of the data upon completion of intended use.

Colorado House Bill 1294 (2014) (continued)

- Holds state Board of Education, Department of Education, or both accountable for breaches of the law.

Gaps in Protection, Exclusions and Omissions:

- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.

Fla. Stat. § 1002.22 (2014); Fla. Stat. § 1002.221 (2014); Fla. Stat. § 1008.386 (2014); Fla. Stat. § 1011.622 (2014)

Florida Senate Bill 188 (2014)

Summary:

Requires notification of privacy rights, defines and prohibits collection of biometric information, and provides for student identification numbers other than Social Security number (the original law applies to educational record data; the 2014 amendment specifically addresses biometric data).

Major Provisions:

- Applies to educational record data; specifically references biometric data.
- Requires the assignment of a code rather than the use of Social Security numbers.

Although it does not specify de-identification as the reason for the code assignment, it seems clear that the code provides for de-identification.

- Holds state agency or LEA accountable for breaches of the law.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- Refers to FERPA regarding challenging the accuracy of data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

"Kansas Student Data Privacy Act," K.S.A. § 72-6214 (2013)

Kansas Senate Bill 367 (2014)

Summary:

Restricts which data contained in a student's educational record can be disclosed and to whom it may be disclosed.

Major Provisions:

- Applies to educational record data and specifically to biometric data.
- Give parents the right to see data collected about their child.
- Requires parental "opt-in" for biometric data only; otherwise there are no opt-out provisions
- Required implementation of security procedures is implied.
- Requires the de-identification of personally identifying information.
- Data use must be specified if it is to be shared with another agency; otherwise language is vague.
- When the data are shared, requires destruction of the data upon completion of their intended use; otherwise language is vague.

Kansas Senate Bill 367 (2014) (continued)

- Holds state agency, employees or agents of the agency, or anyone with data accountable for breaches of the law.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not specifically give parents the right to challenge and correct data.

"Student Data Accessibility, Transparency and Accountability Act of 2014," Idaho Code § 33-133 (2014)

Idaho Senate Bill 1372 (2014)

Summary:

Defines and establishes provisions for data collected as part of educational record, for confidential data, for data security

Major Provisions:

- Applies to educational record data.
- Specifically restricts the use of data collection for advertising and marketing purposes.
- Give parents the right to see data collected about their child.
- Parental "opt-in" is required for secondary uses of the data only.
- Requires implementation of data security procedures.
- Requires the de-identification of personally identifying information.
- Requires specification of how collected data will be used.
- Requires destruction of the data upon completion of intended use.
- Holds State Board of Education accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not specifically give parents the right to challenge and correct data.

"Personal Online Account Privacy Protection Act," La. R.S. §§ 51:1951-1955 (2014)

Louisiana House Bill 340 (2014)

Summary:

Prohibits employers and educational institutions from requesting or requiring certain individuals to disclose information that allows access to or observation of personal online accounts.

Major Provisions:

- Applies to personal electronic devices or accounts.
- Implies that the educational institution will be held accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

"An act to enact R.S. 17:3913 and 3996(B)(34), relative to student information; to limit the type of information to be collected on students; to prohibit the collection of certain information; to prohibit the sharing of student information; to provide exceptions; to provide for access by parents and specified others to certain student information stored in public school computer systems; to provide for student identification numbers; to provide definitions; to provide criminal penalties; and to provide for related matters," La. R.S. § 17:3913 (2015) and La. R.S. § 3996(B)

Louisiana House Bill 1076 (2014)

Summary:

Provides for limitations and prohibitions on the collection and sharing of student information and provides penalties for violations.

Major Provisions:

- Applies to educational record data and specifically to personally identifying information.
- Specifically restricts the use of data collected for advertising and marketing purposes.
- Gives parents the right to see data collected about their child.
- Parental "opt-in" is required for release of personally identifying information.
- Requires implementation of data security procedures.
- Requires de-identification of personally identifying information; but if LEA contracts with a provider, it can transfer personally identifying information.
- Requires destruction of the data upon completion of intended use.
- Any person who violates the law can be held accountable.

Gaps in Protection, Exclusions and Omissions:

- Does not specifically give parents the right to challenge and correct data.
- Does not require the data's intended use to be specified in advance.

Resolve, Directing a Study of Social Media Privacy in School and in the Workplace, Maine HP 838 - Legislative Document 1194 - R. 112 (2014)

Maine House Proposal 838 (2014)

Summary:

Directs the Joint Standing Committee on Judiciary to study issues about social media and personal email privacy in school and the workplace.

Major Provisions:

- Applies to personal email and social media accounts; requires study of privacy concerns.

"An act to make appropriations to aid in the support of the public schools, the intermediate school districts, community colleges, and public universities of the state; to make appropriations for certain other purposes relating to education; to provide for the disbursement of the appropriations; to authorize the issuance of certain bonds and provide for the security of those bonds; to prescribe the powers and duties of certain state departments, the state board of education, and certain other boards and officials; to create certain funds and provide for their expenditure; to prescribe penalties; and to repeal acts and parts of acts," MCLS § 388.1694a (2014), MCLS § 388.1817 (2014), MCLS § 388.1704c (2014).

Michigan House Bill 5314 (2014)

Summary:

Education appropriations bill creates Center for Educational Performance and Information to create, maintain, and enhance this state's P-20 longitudinal data system; Requires state and/or

Michigan House Bill 5314 (2014) (continued)

LEAs to maintain data privacy and institute procedures to that effect.

Major Provisions:

- Applies to educational record data.
- Gives parents the right to see data collected about their child.
- Requires the de-identification of personally identifying information.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches.

"An Act to Ensure the Privacy and Security of Student Educational Records, as Recommended by the Joint Legislative Oversight Committee on Information Technology," N.C. Gen. Stat. § 115C-402.5 (2014) and N.C. Gen. Stat. § 115C-402.15 (2014)

North Carolina Senate Bill 815 (2014)

Summary:

Directs the State Board of Education (State Board) to ensure student data accessibility, transparency, and accountability relating to the student data system. Requires LEAs to notify parents of their rights under state and federal law regarding student records.

Major Provisions:

- Applies to educational record data; addresses biometric data.
- Gives parents the right to see data collected about their child.
- Requires implementation of data security procedures.
- Specification of data use is implied by the requirement to produce an annual report that includes use.
- Destruction of data after its specified use is implied in the security requirements.
- Contracts must include penalties for noncompliance with the law, but the law does not specify who is held accountable.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not require de-identification of personally identifying information.

"An act relative to the collection and disclosure of student data," N.H. Rev. Stat. Ann. §§ 189:65 -189: 68 (2014)

New Hampshire House Bill 1587 (2014)

Summary:

Regulates the collection and distribution of student data; limits disclosure of personally relevant information.

New Hampshire House Bill 1587 (2014) (continued)

Major Provisions

- Applies to educational record data; also specifically to biometric data, student physical tracking, and surveillance of electronic devices.
- Gives parents the right to see data collected about their child.
- Requirement to specify the data's intended use in advance is implied by the requirement to destroy the data upon completion of its intended use.
- Requires destruction of the data upon completion of intended use.
- Implies that the school and/or the state Department of Education would be held accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.

NY CLS Educ § 2-c (2014) and NY CLS Educ § 2-d (2014)

New York Senate Bill 6356-D/Assembly Bill 8556-D (2014)

Summary:

A budget bill that among other things, amends the education law in relation to prohibiting the release of student information to certain entities (Subpart K); and in relation to protecting student privacy and ensuring data security (Subpart L)

Major Provisions:

- Applies to educational record data and specifically refers to biometric data.
- Specifically restricts the use of data collection for advertising and marketing purposes.
- Give parents the right to see data collected about their child.
- Gives parents the right to challenge and correct data, but specifically denies private right of action.
- The law does not specifically give parents the right to opt out of data collection, but it does require parental "opt-in" for a company to further release the child's information.
- Requires implementation of data security procedures.
- Requires specification of how collected data will be used.
- Requires destruction of the data upon completion of intended use.
- Holds private company accountable for breaches of the law.

Gaps in Protection, Exclusions and Omissions:

- Does not require de-identification of personally identifying information.

Ohio Rev. Code Ann. § 3301.0714 (2014)

Ohio House Bill 487

Summary:

Adds language on standards for statewide information management system to protect confidentiality of student data; also adds language barring collection of certain data in the course of school testing.

Major Provisions:

- Applies to educational record data and specifically addresses biometric data.
- Requires implementation of data security procedures.

Ohio House Bill 487 (continued)
- Requires the de-identification of personally identifying information.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches.

"Parents' Bill of Rights," 25 Okl. St. § 2001 (2014), 25 Okl. St. § 2002 (2014), 25 Okl. St. § 2003 (2014)
Oklahoma House Bill 1384 (2014)

Summary:
Creates parents' bill of rights.

Major Provisions:
- Applies to educational record data and specifically to biometric and other biological records.
- Gives parents the right to see data collected about their child.
- Requires parental "opt-in" for biometric or biological data; allows parents to opt out except for "necessary items" of the educational record.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not specifically give parents the right to challenge and correct data.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches of the law.

R.I. Gen. Laws § 16-103-3 (2014), R.I. Gen. Laws § 16-103-4 (2014)
Rhode Island House Bill 7124 (2014)

Summary:

Forbids school from demanding private social media account info; cloud providers can't use data for commercial purposes.

Major Provisions:

- Applies to any data created by a student or processed by cloud provider.
- Specifically restricts the use of data collection for advertising and marketing purposes.
- Holds educational institution accountable for breaches of the law.

Gaps in Protection, Exclusions and Omissions:

- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.

Rhode Island House Bill 7124 (2014) (continued)

- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

S.D. Codified Laws § 13-3-51 (2014), S.D. Codified Laws §§ 13-3-51.1 - 13-3-51.6 (2014)

South Dakota Senate Bill 63 (2014)

Summary:

- Provides that the state's existing student record statute does not authorize the collection of information that is not necessary for funding calculations, student academic progress determinations, or reports required by law, prohibits students from being surveyed without consent on personal topics, prohibits the submitting of personally identifying information to the US Department of Education and requires the Education Department to develop security measures for the data.

Major Provisions:

- Applies to educational record data, especially personally identifying and private information.
- Requires implementation of data security procedures.
- Holds the State Department of Education accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

Utah Code Ann. § 63J-1-602.3 (2014), Utah Code Ann. §§ 53A-1b-101 - 53A-1b-111 (2014)

Utah House Bill 96 (2014)

Summary:

Creates the School Readiness Board, which provides grants to certain early childhood education programs, and may enter into certain contracts with private entities (including providers of education tech for school readiness) to provide funding for early childhood education programs for at-risk students.

Major Provisions:

- Applies to educational record data.
- Requires the de-identification of personally identifying information.
- Implies that the School Readiness Board would be held accountable for breaches.

Gaps in Protection, Exclusions and Omissions:

- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.

Va. Code Ann. § 22.1-287.01 (2014)
Virginia HB 449 (2014)

Summary:
Forbids members/employees of local school boards or the state Department of Education from transmitting a student's "personally identifying information" (as FERPA defines it) to a federal agency or its representative.

Major Provisions:
- Applies to educational record data.

Gaps in Protection, Exclusions and Omissions:
- Does not restrict the use of data collection for advertising and marketing purposes.
- Does not give parents the right to see data collected about their child.
- Does not specifically give parents the right to challenge and correct data.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not specifically require implementation of data security procedures.
- Does not require de-identification of personally identifying information.
- Does not require the data's intended use to be specified in advance.
- Does not require data to be destroyed following intended use.
- Contains no provision regarding accountability for breaches.

Wyo. Stat. § 21-2-202 (2014)
Wyoming Senate Bill 79 (2014)

Summary:
Requires a data security plan for education accountability and assessment data by the Department of Enterprise Technology Services to include privacy and security, breach planning, the prohibition of the sale of student information to private entities or organizations, and the security of all personally identifying information.

Major Provisions:
- Applies to educational record data.
- Specifically restricts the use of data collection for advertising and marketing purposes.
- Requires implementation of data security procedures.
- Specification of data use is implied.
- Requirement to destroy data after intended use is implied.

Gaps in Protection, Exclusions and Omissions:
- Although it does not explicitly give parents the right to see data, it refers to FERPA, which does.
- With respect to challenging the accuracy of data, refers to FERPA.
- Makes no provision for parents to opt out of data collection, storage, or use.
- Does not require de-identification of personally identifying information.
- Contains no provision regarding accountability for breaches.

Notes and References

1 Neuborne, E. (2001, August 13). For kids on the web, it's an ad, ad, ad, ad world: How to help yours see the sales pitches behind online games. *Business Week*. Retrieved August 20, 2009, from http://www.businessweek.com/magazine/content/01_33/b3745121.htm.

2 comScore, Inc. (2009, January 30). *2008 Digital Year in Review*. Reston, VA: Author. Retrieved August 4, 2009, from http://www.comscore.com/Press_Events/Presentations_Whitepapers/2009/2008_Digital_Year_in_Review.

3 MacMullan, J., Wright, H., Linders, H. & de Vera, A. (2009, March). *New media, same old tricks: A survey of the marketing of food to children on food company websites*. Consumers International. Retrieved August 20, 2009, from http://consint.live.rss-hosting.co.uk/files/98978/FileName/Newmedia,sameoldtricks-ENWebversionFINAL100309.pdf.

Chester, J., and Montgomery, K. (2007, May). *Interactive food and beverage marketing: Targeting children and youth in the digital age*. Berkeley, CA: Public Health Institute. Retrieved August 19, 2009, from http://digitalads.org/documents/digiMarketingFull.pdf.

4 Greenwich Public Schools (2014, December 23). iPads for Elementary Students, Chromebooks for Secondary Students. Author. Retrieved January 2, 2015, from http://www.greenwichschools.org/uploaded/district/pdfs/News_Archives/News_Archives_2014-15/PR_-_DLE_Phase_III_Device_122314.pdf.

Waldman, B. (2014, October 14). Technology Is Not the Answer: A Student's Perspective. *Education Week*. Retrieved January 2, 2015, from http://www.edweek.org/ew/articles/2014/10/15/08waldman.h34.html?cmp=ENL-EU-NEWS2.

5 Takeuchi, L.M. and Vaala, S. (2014, October). Level Up Learning: A National Survey on Teaching with Digital Games. *The Joan Ganz Cooney Center at Sesame Workshop*. Retrieved October 21, 2014, from http://www.joanganzcooneycenter.org/publication/level-up-learning-a-national-survey-on-teaching-with-digital-games/.

6 Takeuchi, L.M. and Vaala, S. (2014, October). Level Up Learning: A National Survey on Teaching with Digital Games. *The Joan Ganz Cooney Center at Sesame Workshop*. Retrieved October 21, 2014, from http://www.joanganzcooneycenter.org/publication/level-up-learning-a-national-survey-on-teaching-with-digital-games/.

7 Some examples of webinars promoted to education professionals are:

"Amplifying Student Potential With Tablets & Chromebooks," offered by *Education Week* on December 17, 2014, with content provided by Google for Education;

"Empowering Students With Project-Based Learning and Google Tablets," offered by *Education Week* on November 24, 2014, with content provided by Google for Education;

"How Much Digital Literacy Do Students Need?" offered by *Education Week* on November 24, 2014, with content provided by learning.com and underwritten by Carnegie Corporation of New York;

"Building Better Ed-Tech Strategies for the Pre-K-5 Crowd" offered by *Education Week* on October 21, 2014.

Education Week webinar listings retrieved January 2, 2015, from http://www.edweek.org/ew/marketplace/webinars/webinars.html#archived.

"App Smashing: Combining Apps for Innovative Student Projects," offered by Common Sense Media on November 24, 2014;

"Teachers as Designers of Technology, Pedagogy, and Content (TPACK)" offered by Common Sense Media on October 30, 2014;

"Khan Academy's Video-based Instruction" offered by Common Sense Media on August 27, 2014.

Common Sense Media webinar listings retrieved January 2, 2014, from https://www.graphite.org/appy-hour .

"Top 5 Digital Tools of 2014," offered by edWeb.net on December 15, 2014;

"Journeys in Blended Learning: Key Landmarks for Your School's Progress," offered by edWeb.net on December 16, 2014;

"Encouraging Student Collaboration Using TodaysMeet and Lino," offered by edWeb.net on December 16, 2014.

edWeb.net webinar listings retrieved January 2, 2014, from http://home.edweb.net/upcoming-webinars/.

8 Chester, J., and Montgomery, K. (2007, May). Interactive food and beverage marketing: Targeting children and youth in the digital age. Berkeley, CA: Public Health Institute. Retrieved October 7, 2014, from http://digitalads.org/documents/digiMarketingFull.pdf.

Montgomery, Kathryn C. & Chester, Jeff (2009). Interactive food and beverage marketing: Targeting adolescents in the digital age. *Journal of Adolescent Health, 45*, S18-S29.

Simon, S. (2014, May 15). Data mining your children. *Politico*. Retrieved October 3, 2014, from http://www.politico.com/story/2014/05/data-mining-your-children-106676.html.

9 Simon, S. (2014, May 15). Data mining your children. *Politico*. Retrieved October 3, 2014, from http://www.politico.com/story/2014/05/data-mining-your-children-106676.html.

10 Simon, S. (2014, May 15). Data mining your children. *Politico*. Retrieved October 3, 2014, from http://www.politico.com/story/2014/05/data-mining-your-children-106676.html.

11 Simon, S. (2014, May 15). For sale: Student 'hopes and dreams.' *Politico*. Retrieved October 7, 2014, from http://www.politico.com/story/2014/05/student-data-privacy-market-106692.html.

12 Simon, S. (2014, May 15). For sale: Student 'hopes and dreams.' *Politico*. Retrieved October 7, 2014, from http://www.politico.com/story/2014/05/student-data-privacy-market-106692.html.

For federal privacy law, see:
Family Educational Rights and Privacy Act (FERPA). 20 U.S.C. § 1232g (2012).

Privacy Technical Assistance Center (2014, February). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. U.S. Department of Education. Retrieved February 16, 2015, from http://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf .

13 Although Bing for Schools and Google Apps for Education do not serve ads when children use them on school computers, they do when used from home. In school or at home, they necessarily lead children to sites that they do not control and that often do serve ads and track user behavior for further marketing purposes.

14 www.funbrain.com. Retrieved October 15, 2014.

15 A 2010 *Wall Street Journal* investigation of data tracking and sales via Internet sites found that Dictionary.com was a top venue using tracking technology.

Angwin, J. (2010, July 30). The Web's New Gold Mine: Your Secrets. *Wall Street Journal*. Retrieved October 29, 2014, from http://online.wsj.com/articles/SB10001424052748703940904575395073512989404.

16 Chester, J., and Montgomery, K. (2007, May). *Interactive food and beverage marketing: Targeting children and youth in the digital age*. Berkeley, CA: Public Health Institute. Retrieved August 19, 2009, from http://digitalads.org/documents/digiMarketingFull.pdf.

17 Chester, J., and Montgomery, K. (2007, May). *Interactive food and beverage marketing: Targeting children and youth in the digital age*. Berkeley, CA: Public Health Institute. Retrieved August 19, 2009, from http://digitalads.org/documents/digiMarketingFull.pdf;

Angwin, J. and Tigas, M. (2015, January 14). Zombie Cookie: The Tracking Cookie That You Can't Kill. *ProPublica*. Retrieved January 15, 2015, from http://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill.

18 Pearson Education, Inc. (2000-2014). Privacy Statement (October 2013). Retrieved October 15, 2014, from http://fen.com/resources/privacy-policy-children.html.

19 Pearson Education, Inc. (2000-2014). Privacy Statement (October 2013). Retrieved October 15, 2014, from http://fen.com/resources/privacy-policy-children.html.

20 Common Sense Media (2014, January). Student Privacy Survey. Author. Retrieved January 26, 2015, from https://www.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf.

Class Size Matters (n.d.). New York State inBloom one-page flyer. Author. Retrieved February 3, 2015, from http://www.classsizematters.org/wp-content/uploads/2013/12/Privacy-Fact-Sheet-rev-5.pdf .

21 Simon, S. (2014, May 15). For sale: Student 'hopes and dreams.' *Politico*. Retrieved October 7, 2014, from http://www.politico.com/story/2014/05/student-data-privacy-market-106692.html.

22 Class Size Matters (n.d.). New York State inBloom one page flyer. Author. Retrieved February 9, 2015, from http://www.classsizematters.org/wp-content/uploads/2013/12/Privacy-Fact-Sheet-rev-5.pdf.

NYC Public School Parents (2013, July 24). FAQ on inBloom Inc.: what is the state and your school district doing? Author. Retrieved August 30, 2013, from http://nycpublicschoolparents.blogspot.com/2013/07/faq-on-inbloom-inc-what-is-your-school.html.

23 Noguchi, S. (2014, August 31). California Legislature passes stiffest U.S. bill to protect K-12 students' online data. Mercurynews.com. Retrieved January 2, 2015, from http://www.mercurynews.com/education/ci_26444107/online-privacy-california-passes-nations-stiffest-protections-k;

Singer, S. (2015, February 8). Uncovering Security Flaws in Digital Education Products for Schoolchildren. New York Times. Retrieved February 6, 2015, from http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html.

24 Singer, S. (2015, February 8). Uncovering Security Flaws in Digital Education Products for Schoolchildren. *New York Times*. Retrieved February 6, 2015, from http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html.

25 Kaye, K. (2015, March 23). How Did They Find Out? *Advertising Age* (21-22); online as: Kaye, K. (2015, March 23). Sophisticated Health Data Industry Needs Self-Reflection. *Advertising Age*. Retrieved April 1, 2015, from http://adage.com/article/privacy-and-regulation/sophisticated-health-data-industry-reflection/297719/;

Wheaton, K. (2015, March 23). Hocus Pocus! Your Data Has Been Anonymized! Now They'll Never Find You! *Advertising Age*. Retrieved March 30, 2015, from http://adage.com/article/ken-wheaton/data-anonymized-find/297713/.

26 Carr, D.F. (2013, March 26). Hope Battles Fear Over Student Data Integration. *Information Week*. Retrieved August 29, 2013, from http://www.informationweek.com/education/instructional-it/hope-battles-fear-over-student-data-inte/240151687;

inBloom, Inc., and Affiliantes (2013). FAQ. Author. Retrieved August 29, 2013, from https://www.inbloom.org/faq.

27 Saporta, M., & Sams, D. (2013, March 1). InBloom may spark 'edtech' boom. *Atlanta Business Chronicle*. Retrieved January 7, 2014, from http://www.bizjournals.com/atlanta/print-edition/2013/03/01/inbloom-may-spark-edtech-boom.html.

28 Carol Burris is a frequent guest blogger at the *Washington Post*, The Answer Sheet blog, http://www.washingtonpost.com/blogs/answer-sheet/.

Jason France blogs as Crazy Crawfish, https://crazycrawfish.wordpress.com.

Susan Ohanian blogs at http://www.susanohanian.org/.

Diane Ravitch blogs at http://dianeravitch.net/.

29 American Federation of Teachers (2013, May 31). AFT Statement on Privacy and Security Concerns about inBloom and Other Data Collection Efforts. Author. Retrieved August 30, 2013, from http://www.aft.org/newspubs/press/2013/053113.cfm;

Crazy Crawfish (2013, March 28). Your Children For Sale . . . Sold! *Crazy Crawfish's Blog*. Retrieved August 30, 2013, from https://crazycrawfish.wordpress.com/2013/03/28/your-children-for-sale-sold/;

NYC Public School Parents (2013, July 24). FAQ on inBloom Inc.: what is the state and your school district doing? Author. Retrieved August 30, 2013, from http://nycpublicschoolparents.blogspot.com/2013/07/faq-on-inbloom-inc-what-is-your-school.html;

Ohanian, S. (2013, July 18). NC Lieutenant Governor Has 67 Questions about Common Core. *Susanohanian.org*. Retrieved August 30, 2013, from http://www.susanohanian.org/core.php?id=530;

Ravitch, D. (2013, April 8). Why is the US Department of Education Weakening FERPA? *Diane Ravitch's Blog*, Retrieved August 30, 2013, from http://dianeravitch.net/2013/04/08/why-is-the-us-department-of-education-weakening-ferpa/;

Simon, S. (3013, March 3). K-12 student database jazzes tech startups, spooks parents. *Reuters*. Retrieved August 30, 2013, from http://www.reuters.com/article/2013/03/03/us-education-database-idUSBRE92204W20130303.

30 inBloom, Inc., and Affiliates (2013). FAQ. Author. Retrieved August 29, 2013, from https://www.inbloom.org/faq;

inBloom, Inc., and Affiliates (2013). Privacy Commitment. Author. Retrieved August 29, 2013, from https://www.inbloom.org/privacy-commitment.

31 Family Educational Rights and Privacy Act (FERPA). 20 U.S.C. § 1232g (2012).

32 inBloom, Inc., and Affiliates (2013). FAQ. Author. Retrieved August 29, 2013, from https://www.inbloom.org/faq;

inBloom, Inc., and Affiliates (2013). Privacy Commitment. Author. Retrieved August 29, 2013, from https://www.inbloom.org/privacy-commitment;

Ravitch, D. (2013, April 8). Why Is the US Department of Education Weakening FERPA? *Diane Ravitch's Blog*. Retrieved August 30, 2013, from http://dianeravitch.net/2013/04/08/why-is-the-us-department-of-education-weakening-ferpa/.

33 inBloom, Inc., and Affiliantes (2013). FAQ. Author. Retrieved August 29, 2013, from https://www.inbloom.org/faq.

34 Stern, G. (2013, October 28). Several area districts to forfeit funding over state plans for student data collection. *Lohud.com*. Retrieved November 18, 2013, from http://www.lohud.com/article/20131027/NEWS/310270027?gcheck=1&nclick_check=1;

Kamisar, B. (2013, November 13). New York Parents Sue to Block inBloom Program. *Education Week*. Retrieved January 7, 2014, from http://blogs.edweek.org/edweek/marketplacek12/2013/11/lawsuit_filed_in_new_york_to_halt_inbloom_program.html.

35 Ravitch, D. (2013, May 31). How Will inBloom Help Students and Schools? Diane Ravitch's Blog. Retrieved August 29, 2013, from http://dianeravitch.net/2013/05/31/how-will-inbloom-help-students-and-schools/.

36 Resmovits, J. (2013, January 22). Immense Unease Over Advertisers Nabbing Student Data: Poll. *Huffington Post*. Retrieved January 29, 2014, from http://www.huffingtonpost.com/2014/01/22/student-data-privacy-poll_n_4640688.html;

Singer, N. (2014, February 25). Regulators weigh in on online educational services. *New York Times*. Retrieved February 26, 2014, from http://bits.blogs.nytimes.com/2014/02/25/regulators-weigh-in-on-online-educational-services/;

U.S. Department of Education, Privacy Technical Assistance Center (2014, February 25). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. Author. Retrieved February 26, 2014, from http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf.

37 Fitzgerald, B. (2014, April 3). New York Pulls Out Of inBloom. Ho Hum. Funny Monkey. Retrieved January 15, 2015, from http://funnymonkey.com/blog/new-york-pulls-out-inbloom-ho-hum.

38 Reidenberg, J.R. (2014, January 13, 2014). Personal communication (telephone, with Faith Boninger).

39 Reidenberg, J.R., Russell, N.C., Kovnot, J., Norton, T.B., Cloutier, R., & Alvarado, D. (2013, December 12). Privacy and Cloud Computing in Public Schools. *Center on Law and Information Policy at Fordham Law School*. Retrieved January 10, 2013, from http://ir.lawnet.fordham.edu/clip/2/.

40 Reidenberg, J.R., Russell, N.C., Kovnot, J., Norton, T.B., Cloutier, R., & Alvarado, D. (2013, December 12). Privacy and Cloud Computing in Public Schools. *Center on Law and Information Policy at Fordham Law School*. Retrieved January 10, 2013, from http://ir.lawnet.fordham.edu/clip/2/.

41 Reidenberg, J.R. (2014, January 13, 2014). Personal communication (telephone, with Faith Boninger).

42 "An act to add Section 49073.6 to the Education Code, relating to pupil records, " Cal Ed Code § 49073.6 (2015)

43 "An act to add Section 49073.1 to the Education Code, relating to pupil records," Cal Ed Code § 49073.1 (2015)

44 "Student Online Personal Information Protection Act," Cal Bus & Prof Code, §§ 22584-22585 (2015)

45 Noguchi, S. (2014, August 31). California Legislature Passes Stiffest U.S. Bill to Protect K-12 Students' Online Data. *San Jose Mercury News*. Retrieved January 2, 2015, from http://www.mercurynews.com/education/ci_26444107/online-privacy-california-passes-nations-stiffest-protections-k.

46 Future of Privacy Forum and The Software & Information Industry Association (2014). Student Privacy Pledge. Retrieved October 16, 2014, from http://studentprivacypledge.org/.

47 Future of Privacy Forum and The Software & Information Industry Association (2014). Student Privacy Pledge. Retrieved October 16, 2014, from http://studentprivacypledge.org/.

48 Future of Privacy Forum and The Software & Information Industry Association (2014). Student Privacy Pledge. Retrieved October 16, 2014, from http://studentprivacypledge.org/.

49 Future of Privacy Forum and The Software & Information Industry Association (2014). Student Privacy Pledge: Signatories—Currently 130. Retrieved April 8, 2015, from http://studentprivacypledge.org/?page_id=22.

50 Hattem, J. (2015, February 5). Obama joins bipartisan push on student privacy. *The Hill*. Retrieved February 9, 2015, from http://thehill.com/policy/technology/231841-white-house-working-with-bipartisan-group-on-student-privacy;

Herold, B. (2015, January 29). Draft of President Obama's Student-Data-Privacy Bill Raises Questions. *Education Week*. Retrieved March 30, 2015, from http://blogs.edweek.org/edweek/DigitalEducation/2015/01/federal_student-data-privacy_draft_bill.html;

"Student Online Personal Information Protection Act," Cal Bus & Prof Code § 22584 (2015).

51 Podesta, J. (2015, February 5). Big Data and Privacy: 1 Year Out. *The White House Blog*. Retrieved February 11, 2015, from http://www.whitehouse.gov/blog/2015/02/05/big-data-and-privacy-1-year-out.

52 Common Sense Media (2014, January). Student Privacy Survey. Author. Retrieved January 26, 2015, from https://www.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf.

53 Barnes, K. (2014, March 6). Why a 'Student Privacy Bill of Rights' is desperately needed. *Washington Post*. Retrieved January 7, 2015, from http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.

54 Electronic Privacy Information Center (n.d.). Student Privacy Bill of Rights. Author. Retrieved January 7, 2014, from https://epic.org/privacy/student/bill-of-rights.html.

55 20 U.S.C. § 1232h

Family Educational Rights and Privacy Act (FERPA). 20 U.S.C. § 1232g (2012).

56 20 U.S. Code § 1232h

The Protection of Pupil Rights Amendment (PPRA, 20 U.S.C. § 1232h; 34 CFR Part 98) is only one piece of the section on protection of pupil rights. This 1978 amendment, also known as the Hatch Amendment, specifically addressed the collection of personal data for "survey, analysis, or evaluation" purposes. The collection and use of information for marketing purposes is addressed later in the section.

57 Privacy Technical Assistance Center (2014, February). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. U.S. Department of Education. Retrieved February 16, 2015, from http://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

58 However, the law does not provide parents private right of action to institute a lawsuit. Parents can submit a complaint to the Family Policy Compliance Office, which is designated to review complaints and violations under FERPA.

Barnes, K (2014, October 31). Personal communication (telephone) with Faith Boninger.

59 Electronic Privacy Information Center (n.d.). Family Educational Rights and Privacy Act (FERPA). Author. Retrieved January 5, 2015, from https://epic.org/privacy/student/ferpa/default.html;

Family Educational Rights and Privacy Act (FERPA). 20 U.S.C. § 1232g (2012).

60 34 CFR § 99.31(a)(3)

34 CFR § 99.35(a)(1).

Electronic Privacy Information Center (EPIC) (n.d.). EPIC v. The U.S. Department of Education. Author. Retrieved October 21, 2014, from http://epic.org/apa/ferpa/.

Ravitch, D. (2013, April 8). Why Is the US Department of Education Weakening FERPA? *Diane Ravitch's Blog*. Retrieved August 30, 2013, from http://dianeravitch.net/2013/04/08/why-is-the-us-department-of-education-weakening-ferpa/.

United States Department of Education (2012). Family Educational Rights and Privacy Act Regulations Author. Retrieved October 21, 2014, from http://www2.ed.gov/policy/gen/guid/fpco/pdf/2012-final-regs.pdf.

61 Rotenberg, M. & Barnes, K (2013, January 28). Amassing Student Data and Dissipating Privacy Rights. *Educause Review Online*. Retrieved January 5, 2015, from http://www.educause.edu/ero/article/amassing-student-data-and-dissipating-privacy-rights.

62 Family Educational Rights and Privacy Act (FERPA). 20 U.S.C. § 1232g (2012).

Rotenberg, M. & Barnes, K (2013, January 28). Amassing Student Data and Dissipating Privacy Rights. *Educause Review Online*. Retrieved January 5, 2015, from http://www.educause.edu/ero/article/amassing-student-data-and-dissipating-privacy-rights.

63 Rotenberg, M. & Barnes, K (2013, January 28). Amassing Student Data and Dissipating Privacy Rights. *Educause Review Online*. Retrieved January 5, 2015, from http://www.educause.edu/ero/article/amassing-student-data-and-dissipating-privacy-rights.

64 Privacy Technical Assistance Center (2014, February). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. U.S. Department of Education. Retrieved February 16, 2015, from http://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

65 Privacy Technical Assistance Center (2014, February). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. U.S. Department of Education. Retrieved February 16, 2015, from http://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

66 Retrieved October 21, 2014, from http://www.markey.senate.gov/imo/media/doc/2014-07-14_StudentPriv_BillText.pdf.

67 We conducted a combination of legislative searches to find bills passed in the last two legislative sessions. We modeled our first search on our prior work. Using the Open States database, we searched for the following two terms:

1. privacy AND ("student information" OR "student data")

2. sale AND ("student information" OR "student data")

This search allowed us to choose our own syntax and to examine specifically the possibility that legislatures would address the commercial sale of student information. We complemented the Open States search by searching the National Council of State Legislatures (NCSL) database using the keyword "privacy" for state education bills signed into law. Limited to bills that had been classified as education-related, this second search unearthed several relevant enacted bills that slipped through our Open States search.

The Open States database can be accessed at http://openstates.org/.

The NCSL database can be accessed at http://www.ncsl.org/research/education/education-bill-tracking-database.aspx.

Our prior work using the Open States database can be found at:

Molnar, A, Boninger, F., Harris, M.D., Libby, K.M., & Fogarty, J. (2013). *Promoting Consumption at School: Health Threats Associated with Schoolhouse Commercialism—The Fifteenth Annual Report on Schoolhouse Commercializing Trends: 2011-2012*. Boulder, CO: National Education Policy Center. Retrieved January 3, 2015, from http://nepc.colorado.edu/publication/schoolhouse-commercialism-2012.

68 Although threats to student privacy are certainly a problem at the post-secondary level as well, we limit our inquiry here to K-12.

69 Our search of the Open States database using the search term *privacy AND ("student information" OR "student data")* yielded 251 bills introduced that contained those words. Of those, 59 were signed into law. We followed the same process for the search term *sale AND ("student information" OR "student data")*: 145 introduced bills contained those words, with 43 of them signed into law. We reviewed the bills that had been signed into law for relevance (many bills contain these words in irrelevant contexts) and overlap, leaving 26 relevant bills that became law.

70 Important, but outside the scope of our inquiry here, are the issues faced is by families historically marginalized by schools and for whom the stakes are particularly high (e.g. undocumented students, students and families whose native language is not English, or homeless children). These children and their families may be frightened of data collection for any purpose.

71 Of course, accountability measures must be enforced in order to be effective. While essential, enforcement is outside the scope of this report.

72 20-1-213 MCA (2013)

73 "Student Data Accessibility, Transparency, and Accountability Act of 2013," 70 Okl. St. § 3-168 (2014)

"Parents' Bill of Rights," 25 Okl. St. § 2001 (2014)

25 Okl. St. § 2002 (2014)

25 Okl. St. § 2003 (2014)

74 "Student Data Accessibility, Transparency, and Accountability Act of 2013," 70 Okl. St. § 3-168 (2014)

75 "Student Data Accessibility, Transparency, and Accountability Act of 2013," 70 Okl. St. § 3-168 (2014)

25 Okl. St. § 2002 (2014)

76 "An Act to Ensure the Privacy and Security of Student Educational Records, as Recommended by the Joint Legislative Oversight Committee on Information Technology," N.C. Gen. Stat. § 115C-402.5 (2014), N.C. Gen. Stat. § 115C-402.15 (2014)

77 "An act relative to the collection and disclosure of student data," N.H. Rev. Stat. Ann. §§ 189:65 -189: 68 (LexisNexis 2014)

78 "An act relative to the collection and disclosure of student data," N.H. Rev. Stat. Ann. §§ 189:65 -189: 68 (LexisNexis 2014)

"Student Data Accessibility, Transparency, and Accountability Act of 2013." 70 Okl. St. § 3-168 (2014)

Fla. Stat. § 1002.22 (2014); Fla. Stat. § 1002.221 (2014); Fla. Stat. § 1008.386 (2014); Fla. Stat. § 1011.622 (2014)

"Kansas Student Data Privacy Act," K.S.A. § 72-6214 (2013)

La. R.S. § 17:3913 (2015).

NY CLS Educ § 2-c (2014); NY CLS Educ § 2-d (2014)

"An Act to Ensure the Privacy and Security of Student Educational Records, as Recommended by the Joint Legislative Oversight Committee on Information Technology," N.C. Gen. Stat. § 115C-402.5 (2014) and N.C. Gen. Stat. § 115C-402.15 (2014).

Ohio Rev. Code Ann. § 3301.0714 (LexisNexis 2014).

79 "An act relative to the collection and disclosure of student data," N.H. Rev. Stat. Ann. §§ 189:65 -189: 68 (LexisNexis 2014)

80 "An act to add Section 49073.1 to the Education Code, relating to pupil records," Cal Ed Code § 49073.1 (2015)

"An act to add Section 49073.6 to the Education Code, relating to pupil records". Cal Ed Code § 49073.6 (2015)

"Student Online Personal Information Protection Act," Cal Bus & Prof Code § 22584 (2015).

81 "Student Data Protection, Accessibility, Transparency, and Accountability Act of 2014," C.R.S. 22-2-309 (2014)

82 R.I. Gen. Laws §§ 16-103-3 - 16-103-4 (2014)

83 "Personal Online Account Privacy Protection Act," La. R.S. §§ 51:1951-1955 (2014)

"AN ACT relative to the collection and disclosure of student data.," N.H. Rev. Stat. Ann. §§ 189:65 -189: 68 (2014)

In addition, Maine enacted legislation in 2014 to require a study of social media privacy in school (20-A M.R.S. § 19351 [2014]).

84 Electronic Privacy Information Center (n.d.). EPIC Student Privacy Freedom of Information Act Request: Department of Education's FERPA Enforcement. Author. Retrieved January 7, 2015, from https://www.epic.org/foia/ed/ferpa/default.html.

85 Cal Ed Code § 49073.6 (2015)

86 NY CLS Educ § 2-d (2014)

New York State Education Department (2014, July 29). Parents' Bill of Rights for Data Privacy and Security. Author. Retrieved January 8, 2015, from http://www.p12.nysed.gov/docs/parents-bill-of-rights.pdf.

87 NY CLS Educ § 2-c (2014)

NY CLS Educ § 2-d (2014)

88 "Student Data Accessibility, Transparency and Accountability Act of 2014," Idaho Code § 33-133 (2014)

89 "An act to enact R.S. 17:3913 and 3996(B)(34), relative to student information; to limit the type of information to be collected on students; to prohibit the collection of certain information; to prohibit the sharing of student information; to provide exceptions; to provide for access by parents and specified others to certain student information stored in public school computer systems; to provide for student identification numbers; to provide definitions; to provide criminal penalties; and to provide for related matters," La. R.S. § 17:3913 (2014), La. R.S. § 3996(B) (2014)

20-7-104, MCA (2013)

90 "Kansas Student Data Privacy Act," K.S.A. § 72-6214 (2013)

"Parents' Bill of Rights," 25 Okl. St. § 2001 (2014)

25 Okl. St. § 2002 (2014)

25 Okl. St. § 2003 (2014)

91 "Parents' Bill of Rights," 25 Okl. St. § 2001 (2014)

25 Okl. St. § 2002 (2014)

25 Okl. St. § 2003 (2014)

92 Although Ohio law excludes personally identifying information from the data that can be held by the state historical society, it does allow parents to opt in to allow the historical society to hold that information.

Ohio Rev. Code Ann. § 149.381 (LexisNexis 2014).

93 "An act to add Section 49073.1 to the Education Code, relating to pupil records," Cal Ed Code § 49073.1 (2015).

"Kansas Student Data Privacy Act," K.S.A. § 72-6214 (2013)

NY CLS Educ § 2-c (2014), NY CLS Educ § 2-d (2014)

"Student Data Accessibility, Transparency, and Accountability Act of 2013," 70 Okl. St. § 3-168 (2014)

"An act relating to education research centers and the sharing of educational data between state agencies; redesignating certain fees as charges," Tex. Educ. Code § 1.005 (2014).

94 Kansas requires specification of use only when the data is shared. North Carolina and Wyoming law imply a need for specification because they require the data to be destroyed when its specified use is complete.

"An act to add Section 49073.6 to the Education Code, relating to pupil records," Cal Ed Code § 49073.6 (2015)

"An act to add Section 49073.1 to the Education Code, relating to pupil records," Cal Ed Code § 49073.1 (2015)

"Student Online Personal Information Protection Act," Cal Bus & Prof Code § 22584 (2015)

"Student Data Protection, Accessibility, Transparency, and Accountability Act of 2014," C.R.S. 22-2-309 (2014)

"Student Data Accessibility, Transparency and Accountability Act of 2014," Idaho Code § 33-133 (2014)

"Kansas Student Data Privacy Act," K.S.A. § 72-6214 (2013)

"An Act to Ensure the Privacy and Security of Student Educational Records, as Recommended by the Joint Legislative Oversight Committee on Information Technology," N.C. Gen. Stat. § 115C-402.5 (2014), N.C. Gen. Stat. § 115C-402.15 (2014)

NY CLS Educ § 2-c (2014), NY CLS Educ § 2-d (2014)

Wyo. Stat. § 21-2-202 (2014)

"Student Data Accessibility, Transparency, and Accountability Act of 2013," 70 Okl. St. § 3-168 (2014)

95 "An act to add Section 49073.6 to the Education Code, relating to pupil records," Cal Ed Code § 49073.6 (2015)

"An act to add Section 49073.1 to the Education Code, relating to pupil records," Cal Ed Code § 49073.1 (2015)

"Student Online Personal Information Protection Act," Cal Bus & Prof Code § 22584 (2015)

"Student Data Protection, Accessibility, Transparency, and Accountability Act of 2014," C.R.S. 22-2-309 (2014)

"Student Data Accessibility, Transparency and Accountability Act of 2014," Idaho Code § 33-133 (2014)

"Kansas Student Data Privacy Act," K.S.A. § 72-6214 (2013)

"An act to enact R.S. 17:3913 and 3996(B)(34), relative to student information; to limit the type of information to be collected on students; to prohibit the collection of certain information; to prohibit the sharing of student information; to provide exceptions; to provide for access by parents and specified others to certain student information stored in public school computer systems; to provide for student identification numbers; to provide definitions; to provide criminal penalties; and to provide for related matters," La. R.S. § 17:3913 (2015)

"An Act to Ensure the Privacy and Security of Student Educational Records, as Recommended by the Joint Legislative Oversight Committee on Information Technology," N.C. Gen. Stat. § 115C-402.5 (2014), N.C. Gen. Stat. § 115C-402.15 (2014)

NY CLS Educ § 2-c (2014), NY CLS Educ § 2-d (2014)

Wyo. Stat. § 21-2-202 (2014)

96 "An act to add Section 49073.6 to the Education Code, relating to pupil records," Cal Ed Code § 49073.6 (2015)

"An act to add Section 49073.1 to the Education Code, relating to pupil records," Cal Ed Code § 49073.1 (2015)

"Student Online Personal Information Protection Act," Cal Bus & Prof Code § 22584 (2015)

"Student Data Protection, Accessibility, Transparency, and Accountability Act of 2014," C.R.S. 22-2-309 (2014)

"Student Data Accessibility, Transparency and Accountability Act of 2014," Idaho Code § 33-133 (2014)

"Kansas Student Data Privacy Act," K.S.A. § 72-6214 (2013)

"An act to enact R.S. 17:3913 and 3996(B)(34), relative to student information; to limit the type of information to be collected on students; to prohibit the collection of certain information; to prohibit the sharing of student information; to provide exceptions; to provide for access by parents and specified others to certain student information stored in public school computer systems; to provide for student identification numbers; to provide definitions; to provide criminal penalties; and to provide for related matters," La. R.S. § 17:3913 (2015)

20-7-104, MCA (2013)

"An Act to Ensure the Privacy and Security of Student Educational Records, as Recommended by the Joint Legislative Oversight Committee on Information Technology," NY CLS Educ § 2-c (2014), NY CLS Educ § 2-d (2014)

R.I. Gen. Laws § 16-103-3 (2014)

R.I. Gen. Laws § 16-103-4 (2014)

Wyo. Stat. § 21-2-202 (2014)

97 "Children's Online Privacy Protection Act,"15 U.S. Code Chapter 91. Retrieved January 8, 2015, from http://www.law.cornell.edu/uscode/text/15/chapter-91.

98 Harris, J.L., Heard, A., & Schwartz, M. (2014, January). *Older but still vulnerable: All children need protection from unhealthy food marketing*. Yale Rudd Center for Food Policy and Obesity. Retrieved November 3, 2014, from http://www.yaleruddcenter.org/resources/upload/docs/what/reports/Protecting_Older_Children_3.14.pdf.

Pechmann, C., Levine, L., Loughlin S., & Leslie, F. (2005). Impulsive and selfconscious: Adolescents' vulnerability to advertising and promotion. *Journal of Public Policy Marketing, 24*, 202–21.

99 Harris, J.L., Heard, A., & Schwartz, M. (2014, January). *Older but still vulnerable: All children need protection from unhealthy food marketing*. Yale Rudd Center for Food Policy and Obesity. Retrieved November 3, 2014, from http://www.yaleruddcenter.org/resources/upload/docs/what/reports/Protecting_Older_Children_3.14.pdf.

100 Molnar, A. and Boninger, F. (in press). *Sold Out: How Marketing in School Threatens Children's Well-Being and Undermines their Education*. Lanham, MD: Rowman & Littlefield.

Molnar, A, Boninger, F., Harris, M.D., Libby, K.M., & Fogarty, J. (2013). Promoting Consumption at School: Health Threats Associated with Schoolhouse Commercialism—The Fifteenth Annual Report on Schoolhouse Commercializing Trends: 2011-2012. Boulder, CO: National Education Policy Center. Retrieved January 3, 2015, from http://nepc.colorado.edu/publication/schoolhouse-commercialism-2012.

101 The Secretary of Education designated the Family Policy Compliance Office (FPCO) of U.S. Department of Education to "Investigate, process, and review complaints and violations under [FERPA]": 34 CFR § 99.60(b)(1)

In April 2014, EPIC submitted a Freedom of Information Act request to the U.S. Education Department for documents detailing parent and student complaints about the misuse of educational records. According to EPIC, the documents reveal that the Department failed to investigate many FERPA complaints.

Electronic Privacy Information Center (2014, October 15). EPIC Student Privacy Freedom of Information Act Request: Department of Education's FERPA Enforcement. Author. Retrieved February 11, 2015, from https://www.epic.org/foia/ed/ferpa/default.html.

The Education Secretary has designated the Education Department's Family Policy Compliance Office ("FPCO") to "investigate, process, and review complaints and violations under [FERPA]." The FCPO may investigate complaints that parents or students file, or alternatively, the FCPO may conduct "its own investigation when no complaint has been filed or a complaint has been withdrawn, to determine whether an educational agency or institution or other recipient of Department funds under any program administered by the Secretary has failed to comply with [FERPA]."

102 Barnes, K. (2014, March 6). Why a 'Student Privacy Bill of Rights' is desperately needed. *Washington Post*. Retrieved January 7, 2015, from http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.

103 Privacy Technical Assistance Center (2014, February). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. U.S. Department of Education. Retrieved February 16, 2015, from http://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.