NEPC
NATIONAL EDUCATION POLICY CENTER

# Section III

# Privacy and Data Security Issues to Consider Before Adopting a Digital Platform or Learning Program

Faith Boninger and Alex Molnar
University of Colorado Boulder

September 2020

When schools import proprietary digital technologies, there is a risk that the companies involved may exploit student data. Any app or website can easily incorporate technology to collect IP addresses and other information, including which pages, content or ads children see or click on; what they download; what games they play; what device a child is using, with what operating system and settings, and so on. Educational technology platforms, particularly those from companies with contracts defining them as "school officials," can access even more data, including data from school data systems.[1] Given the economic value of data in the surveillance economy, any bit of information that can be collected *is* collected.[2] Such comprehensive information facilitates behavioral tracking, which can be used in current and future product-related research, as well for other unspecified purposes.[3]

Schools and districts now routinely collect, store, and report data for state longitudinal data systems on such things as attendance, tardiness, test scores and grades. Teachers record student behavior in classroom management applications and use "personalized" or "adaptive" learning technologies that record student keystrokes, answers, and response times as they work their way through the curriculum or take assessments.[4] The U.S. Department of Education actively encourages the use of massive student data sets (commonly referred to as "big data"[5]) to facilitate technological "innovation" on the largely unsubstantiated premise that it will lead to "deeper learning" and better assessment and support systems.[6]

While such massive amounts of specific and personal data are being collected about children at school, it is rarely clear how all this information may be used in the future. It may be used to support student learning or direct students to resources. It may also be used to manipulate students, cultivate them as current and future consumers, or sort and evaluate them for purposes unknown and unapproved by their schools or parents.[7] Corporations that gather

information from children in an educational context may claim not to use it for commercial gain, but there are no guarantees.[8] A 2018 Fordham Law School study of data brokers' sale of student lists found a wide variety of student information for sale—including a list of 14- and 15-year-old girls for family planning purposes.[9] The researchers were largely unable to discover the sources of the data for sale.[10] Moreover, the Federal Trade Commission noted that the resale of data is so common that it may be virtually impossible for consumers to determine the origin of any commercially available information about them.[11]

School contracts with digital vendors often include provisions that prohibit selling or transferring data, or using the information for purposes other than its stated educational use. However, those provisions can often be insufficient to actually protect the data from misuse by the companies that collect it or by their partners.[12] And, since data are fungible, it would be surprising if some companies do not collect and conserve data in order to, for example, increase the company's value to a prospective buyer.

Data security is also a concern.[13] High-profile breaches and hacks demonstrate that many education technology applications lack adequate data security to protect the student data collected.[14] In a 2018 report, the Federal Bureau of Investigation (FBI) noted that the "widespread collection of sensitive information by EdTech could present unique exploitation opportunities for criminals," and that education technology connected to the internet could facilitate criminals' access to data children's devices collect for education purposes.[15]

Given the massive amounts of student data collected and the threats to student privacy that virtual technologies pose, it is essential for school leaders to carefully review the privacy implications and data safeguards of any digital platform or learning program being considered. Six key issues related to student privacy are discussed below.

## Digital platforms and learning programs may share student data with third parties for unknown purposes, or in other ways fail to adequately protect student data.

It is this simple: Data that are not collected and/or stored are not available for misuse or theft. For this reason, a product that collects minimal data is preferable to a product that collects more. Consider carefully whether the analytics a product offers are really necessary. Avoid the temptation to purchase a product that offers analyses that you do not want to use now, but "might" want in the future. To protect student privacy, it would be preferable to choose a product that avoids collecting any data that you do not have a specific, immediate, interest in having. As a side benefit, a "no-frills" product may be less expensive than a product containing bells and whistles you probably won't use and that puts your students at greater risk.

Private vendors may have the slickest marketing materials, but they are not necessarily the best choice to provide virtual learning strategies. In their 2019 study of virtual schools, Miron and Elgeberi found that districts have been increasingly creating their own virtual and blended schools, and that those schools' students perform better on state assessments than students attending charter virtual schools—especially compared to charter schools managed

by for-profit education management organizations.[16] Also, unlike private companies, school districts have no financial incentive to collect and store excess student data.

## How proprietary digital platforms and learning programs operate is rarely, if ever, transparent.

Algorithms are procedures for solving a mathematical problem in a finite number of steps.[17] In software applications they are the formulas that collect, sort, and organize data. The programming of privately developed algorithms is largely hidden from the public behind the legal veil of "proprietary information." As a consequence, there is no way for either the individuals or the institutions to know what data are being collected or what is done with those data, except as the provider may choose to share that information.[18] Until regulators require that the programming in software products used by schools be transparent and reviewable, the ability of school leaders to learn how a product works is limited to their power to walk away from a deal unless they get the information and protections they demand. It is nonetheless important that school leaders make transparency an issue in any negotiation of the purchase of a digital platform or learning program.

## The contract language associated with digital platforms and learning program requires expert review.

In 2017, the Electronic Frontier Foundation researched the privacy policies of 152 education technology services used in schools. They found that only 118 of the 152 had published privacy policies. Especially important with respect to data security, of that 118, only 78 mentioned data retention policies and only 46 reported using encryption (and in the latter case, encryption tended to be mentioned with respect to billing information and not necessarily with respect to other stored student data).[19]

When privacy policies and terms of service do exist, they may contain clauses that sound reasonable on the surface but actually present a risk to students. The Terms of Service for the Summit Learning Program, for example, warn schools that their use of the services is entirely at their own risk, that there are no warranties whatsoever, and that they waive any right to a class action suit and agree in advance to binding arbitration.[20]

Our examination of platform privacy policies found vague disclosures of how the vast amounts of information collected from children and teachers would be used. The company Instructure, for example, uses the information collected from its virtual learning platform, Canvas, to improve websites, apps, and services, and to "personalize and improve" users' experience with the platform. Companies may also share aggregated and so-called "de-identified" data without notice to users, despite evidence that such de-identified data is easily re-identified.[21] Pearson's Schoolnet is designed to collect and hold data on every assessment children take in their classes and for district and state testing purposes, with no published privacy policy for parents to evaluate.[22] How data collected by these digital platforms may be used in the future is unknown.

We do have some hint, however, of the extent of the possibilities for exploiting student data. Companies using predictive analytics are already collecting and combining data from assorted sources (including insurance claims, digital health records, housing records, and personal information about a person's friends, family and roommates) for use in algorithms that produce "risk scores" to identify individuals at risk of opioid addiction or overdose. These scores are sold to doctors, insurers and hospitals to be used in their decision-making.[23] Further, several hundred education technology companies partner with Amazon Web Services (AWS) in an initiative called EdStart. Marachi and Quill noted that although these companies may promise compliance with U.S. data privacy laws, once data are collected and combined across international borders, companies may no longer be held to the laws of the country where the data were originally gathered. Stored in international servers, the data may be transferred or sold without any oversight.[24]

## Digital platforms and learning programs often send students to third-party sites whose content and privacy policies have not been adequately vetted.

When children enter the Internet environment, even if they enter from a responsible site with a thorough and transparent privacy policy, they are quickly exposed to other commercial sites that may be less concerned about their privacy. As they move around the Internet, using educational sites and jumping off from them to surf or play on other sites, their activity is constantly tracked and recorded for future use.[25] 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 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.[26]

Digital educational technology provides the opportunity for students to take breaks by shifting to additional sites. But some products actively direct students to other sites.[27] Summit Learning and Canvas, for example, connect children to third-party sites (such as YouTube) that collect data for advertising purposes. Both Summit Learning and Instructure (Canvas's parent company) deny responsibility for any use a third party might make of children's or teachers' data. YouTube is not part of the educational suite of applications that Google offers to schools. The implication is that YouTube tracks users, regardless of whether they arrived at YouTube from an educational site or even from one of Google's educational applications. Parents are thus in the impossible position of being responsible for reviewing the lengthy and often incomprehensible privacy policies of the numerous third-party sites or agreeing to their terms with no understanding of the implications. They are then further responsible for independently negotiating with their schools and districts if they are unwilling to have their children be subject to policy provisions. This is literally impossible for virtually all parents.

Thus, when a cloud-based learning management system, such as Canvas, sends students to multiple third-party sites, multiple vendors gain access to student browsing information (e.g., what the students view and metadata about their interactions). This creates such a

complex set of dynamic relational data drawn from multiple sources that it is impossible for students or their families to verify or even be aware of data being circulated about them.[28]

## "De-identified" student data can be easily re-identified.

As noted above, the digital technology industry promotes data de-identification (also called anonymization) as the solution to concerns about tracking.[29] Even if student data is de-identified, however, students' personally identifiable information (PII) may not be fully or permanently protected.

Using only de-identified behavioral tracking data, marketers can target a given computer's user with advertisements and other communications geared specifically to appeal to and influence that user. Google, for instance, has repeatedly been accused of doing exactly this. The state of New Mexico sued Google in February 2020 for violating the Children's Online Privacy Protection Act (COPPA). [30] The suit accuses Google of using school-assigned Chromebooks and "G Suite for Education" accounts to illegally collect information including students' online behavior, location, voice recordings, contact lists, and passwords. It further accuses Google of using the personal information it illegally collects for advertising purposes. When the child is the primary or only user of the device (as is certainly the case when that device is a school-assigned Chromebook, for instance),[31] marketers do not need student identification at all in order to target specific students.

This being the case, the editor of the trade publication *Advertising Age*, Ken Wheaton, bluntly called data de-identification "a load of horseshit . . . a clever bit of technical and verbal misdirection used by marketers and tech people to keep regulators at bay." [32] He explains, "You might not know my name (but you probably do), but that hardly matters if you know every move I make, every breath I take."[33]

Computer scientists and data experts have known for over a decade that complex de-identified datasets—such as student datasets—can easily be re-identified.[34] If a handful of datapoints in an de-identified dataset match a handful of datapoints in another, identified dataset, the de-identified data are no longer anonymous. For these reasons, school leaders should not be reassured by promises that student data is de-identified. Instead, they should ask questions about the nature and amount of de-identified data held by the vendor of any product they are considering, what those data are used for, how they are protected from misuse and theft, and how and when they will be destroyed.

## Digital platforms and learning programs may not adequately secure student data.

It is more effective, but more expensive and therefore less common, to incorporate security into technology development from the beginning of a project rather than at its end.[35] It is also expensive, and therefore less common, to correct issues that may be unearthed by an algorithmic audit. For these reasons, the number of security breaches in public schools is growing. The Cybersecurity Research Center counted 348 cybersecurity incidents in 2019

alone, nearly three times as many as were reported in 2018.[36] Approximately half of these incidents resulted from the actions of insiders to the school community, primarily education technology vendors.[37]

Current legal protections for student privacy are extremely limited.[38] Federal law theoretically prohibits the use of data held by private companies for purposes unspecified in their contracts,[39] and over 425 companies have signed onto a self-regulatory pledge that bans "behavioral targeting of advertisements."[40] Companies are, however, unlikely to be held to account for security breaches or for misuse of children's data. The Family Educational Rights and Privacy Act (FERPA) threatens to withhold funding to schools as a result of data misuse, but this punishment has never actually been imposed.[41] A November 2018 audit found not only a two-year backlog in the Department of Education's Privacy Office's processing of FERPA complaints, but also that the Privacy Office is unable to resolve many of the complaints because of "significant control weaknesses" and unresolved policy questions about FERPA.[42]

Citizens may bring complaints to the Federal Trade Commission (FTC) if they believe a signatory company has violated the Student Privacy Pledge. Like the U.S. Department of Education, however, the FTC seems disinclined to act decisively to censure technology companies. For example, it still has not acted on the 2015 complaint brought against Google by the Electronic Frontier Foundation.[43] It did, however, rule against Google in September 2019 for collecting personal information from children on YouTube in violation of the Children's Online Privacy Protection Act (COPPA). In that case, the amount of the fine levied was the equivalent of less than three months of the advertising revenue Google makes from children's videos, prompting critics to note that in effect, Google would not be discouraged from violating COPPA in the future.[44]

In many cases, state legislation designed to protect student privacy by prohibiting commercial use of student data explicitly exempts data collected from students for "adaptive" or "personalized" student learning purposes.[45] Such language nullifies other clauses of these bills designed to prevent tracking of students, because tracking is an essential aspect of "personalized" student learning. In other words, school and district leaders should hold any product they adopt to a higher standard than compliance with relevant state or federal privacy laws requires.

*Current legal protections for student privacy are extremely limited.*

Because of the ease with which de-identified data may be re-identified, data experts refer to "Five Safes" by which data can and should be secured: Data should de-identified. Data collected should be analyzed only by trained and accredited specialists. Data analyses should be done in a secure setting. Data should be secured in a way that prevents unauthorized removal of any data. Data analyses done should be checked and confirmed as non-disclosive.[46] This framework used in government and research settings is designed to provide comprehensive and long-term integrity of any data collected. There is no legal requirement for private companies to use this framework, but to the extent that they do, students' data will be more effectively protected.

## Research Landscape Related to Digital Platforms and/or Learning Programs in a Virtual Environment: Data Privacy

**Michael K. Barbour, Touro University California**

There has been no research in the field of K-12 distance, online, and blended learning focused on student data privacy practices beyond that of Boninger and her colleagues in 2019 and 2020.[47] The only other information available is from educational bloggers, investigative reporters, and whistleblowing teachers.

For example, in 2008, Arizona-based blogger David Safier revealed that the Arizona Virtual Academy (a K12, Inc.-managed virtual school) had outsourced the grading of middle school, and a year later high school, student papers to a private company based in India in an effort to cut costs.[48] According to Safier's reports, the practice was revealed when parents began to question the nature of comments on the students' work, and then began to complain to the virtual charter school (which appears to be when Safier first began investigating the issue). Safier questioned whether commenting on and/or scoring student work constituted direct or indirect teaching duties (Arizona law required that those with teaching duties had to obtain a Fingerprint Clearance Card or Fingerprint Criminal History Check).

In a follow-up to his original blog entry, Safier reported that in addition to the Arizona Virtual Academy, nine additional virtual charter schools operated by K12, Inc. (in California, Colorado, Idaho, Illinois, Minnesota, Ohio, Pennsylvania, and Washington) also outsourced grading.[49] As a part of his second entry, he outlined exactly how the process worked, based on the evidence he was able to piece together. Several months later the story was picked up by *Education Week*,[50] but the story was not distributed by the media specifically in any of the affected states.

Five years later Travis Manning, a teacher activist, wrote a letter to the editor of the *Idaho Press* noting that the Idaho Virtual Academy was one of the nine other online charter schools operated by K12, Inc. that Safier had referred to in his original piece.[51] At the time of Manning's letter, the legislature in Idaho was debating K-12 virtual learning policy. In the months that followed, officials from both the Idaho Virtual Academy and K12, Inc. confirmed the story.[52]

Interestingly, the officials claimed that it had been a small pilot project that ended rather quickly. However, Safier's original investigation of the outsourcing detailed that the grading practice existed for at least 10 different K12, Inc.-operated virtual charter schools for at least two school years, and it also included tutoring services in four states (California, Colorado, Idaho, and Pennsylvania) for an unknown amount of time.

More recently, a group of teachers attempting to organize on behalf of the California Teachers Association lodged a number of complaints against the California Virtual Academies (virtual charter schools operated by K12, Inc.),[53] including that the cyber charter school "permitted overly wide staff access to sensitive student data, such as psychological reports and special education status."[54] However, the California Department of Education did not conduct an investigation and closed the matter due to a lack of data on the part of the complainants.[55] In 2016, the California Virtual Academy (2016) reported to their employees that they had "learned of an incident that might affect the security of your personal information,"[56] although there was no mention or additional coverage indicating that this breach may have impacted student data.

These kinds of reports are similar to those described in the Network for Public Education's 2018 guide, *Online Learning: What Every Parent Should Know*, as a part of a section entitled "Is Privacy Sufficiently Protected When Students Learn Online?"[57] The section details how in Pennsylvania, K12 Inc. was violating "federal privacy law by requiring parents who enroll their children to waive their rights to have their children's personal information protected from unrestricted disclosure and/or commercial use,"[58] as well as data breaches by companies like Schoolzilla and a growing number of schools and districts. However, beyond these isolated reports, there is no empirical research into privacy within the virtual education literature. Given this situation, it is incumbent on school leaders to thoroughly assess the potential risks to student privacy posed by any digital platform and/or learning program they are considering for adoption.

## Conclusion

Unfortunately, there are real risks to students' privacy posed by any collection of data about them. School and district leaders can minimize the risks by making judicious choices of platforms and programs. To avoid introducing significant privacy threats, we recommend that a school's educational program be the framework used to consider of any technology for adoption. In other words, technology and applications should not drive the curriculum, pedagogy, assessment, or data collection and record-keeping practices of the schools. We recommend that school and district leaders consider:

- The pedagogical values, goals, and practices they hope to achieve before considering the adoption of a particular digital educational product;
- The ways in which any digital educational product would advance their self-defined values, goals, and practices;
- The potential negative consequences—in this case, for student privacy—that may be associated with the use of that product and devise strategies for avoiding them;
- Which of their defined values, goals, and practices can be best achieved by non-digital means and which require digital means;

As they assess the suitability of any particular project, we recommend that they consider:

- The extent to which, and for what purposes, the product collects, stores, and shares student data;
- The transparency of the product's operation;
- The details of privacy-related contract language associated with the product;
- Whether and to which third-party sites the product directs students;
- What the product does with de-identified data; and
- How the collected data are secured.

# Notes and References Section III

1 Rotenberg, M. & Barnes, K (2013, January 28). Amassing student data and dissipating privacy rights. *Educause Review Online*. Retrieved July 13, 2020, from http://www.educause.edu/ero/article/amassing-student-data-and-dissipating-privacy-rights

2 Professor and information law expert Frank Pasquale notes that "data is the fuel of the information economy, and the more data a company already has, the better it can monetize it."

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information* (p.141). Cambridge, MA: Harvard University Press.

3 Alim F., Cardozo, N., Gebhart, G., Gullo, K, & Kalia, A. (2017, April 13). *Spying on students: School-issued devices and student privacy*. Electronic Frontier Foundation. Retrieved July 13, 2020, from https://www.eff.org/wp/school-issued-devices-and-student-privacy

4 Almohammadi, K., Hagras, H., Alghazzawi, D., & Aldabbagh, G. (2017). A survey of artificial intelligence techniques employed for adaptive educational systems within e-learning platforms. *Journal of Artificial Intelligence and Soft Computing Research, 7*(1). Retrieved July 13, 2020, from https://content.sciendo.com/view/journals/jaiscr/7/1/article-p47.xml

Pearson & EdSurge (2016). Decoding Adaptive. Retrieved September 15, 2020, from https://www.pearson.com/content/dam/one-dot-com/one-dot-com/global/Files/about-pearson/innovation/Pearson-Decoding-Adaptive-v5-Web.pdf

5 The Oxford English Dictionary defines "big data" as "data of a very large size, typically to the extent that its manipulation and management present significant logistical challenges."

Press, G. (2013, June 18). Big data news: A revolution indeed. *Forbes.com*. Retrieved July 13, 2020, from http://www.forbes.com/sites/gilpress/2013/06/18/big-data-news-a-revolution-indeed/#1e6d81397b9f

6 U.S. Department of Education Office of Educational Technology (2013). *Expanding evidence approaches for learning in a digital world*. Author. Retrieved July 13, 2020, from http://tech.ed.gov/wp-includes/ms-files.php?file=2013/02/Expanding-Evidence-Approaches.pdf

See also:

Saltman, K.J. (2016, April 19). Corporate schooling meets corporate media: Standards, testing, and technophilia. Review of Education, Pedagogy, and Cultural Studies, 38(2), 105-123. Retrieved July 13, 2020, from https://www.researchgate.net/publication/301537110_Corporate_schooling_meets_corporate_media_Standards_testing_and_technophilia

7 For discussion of concerns about possible future uses, see:

Saltman, K.J. (2016, April 19). Corporate schooling meets corporate media: Standards, testing, and technophilia. *Review of Education, Pedagogy, and Cultural Studies, 38*(2), 105-123. Retrieved July 13, 2020, from https://www.researchgate.net/publication/301537110_Corporate_schooling_meets_corporate_media_Standards_testing_and_technophilia

Tulenko, J. (2016, April 5). *Why digital education could be a double-edged sword*. PBS. Retrieved July 13, 2020, from http://www.pbs.org/newshour/bb/why-digital-education-could-be-a-double-edged-sword/

8 Abamu, J. (2017, May 15). *Edmodo's tracking of students and teachers revives skepticism surrounding 'free' edtech tools*. EdSurge. Retrieved July 13, 2020, from https://www.edsurge.com/news/2017-05-15-edmodo-s-tracking-of-students-and-teachers-revives-skepticism-surrounding-free-edtech-tools

Brown, E. & Frankel, T.C. (2016, October 11). Facebook-backed school software shows promise — and raises privacy concerns. *Washington Post*. Retrieved July 13, 2020, from https://www.washingtonpost.com/local/education/facebook-backed-school-software-shows-promise--and-raises-privacy-concerns/2016/10/11/2580f9fe-80c6-11e6-b002-307601806392_story.html

Cardozo, N. (2015, October 14). *Internet companies: Confusing consumers for profit*. Electronic Frontier Foundation. Retrieved July 13, 2020, from https://www.eff.org/deeplinks/2015/10/Internet-companies-confusing-consumers-profit

Singer, N. (2015, March 5). Digital learning companies falling short of student privacy pledge. *New York Times*. Retrieved July 13, 2020, from http://bits.blogs.nytimes.com/2015/03/05/digital-learning-companies-falling-short-of-student-privacy-pledge/

9 Russell, N.C., Reidenberg, J.R., Martin, E., Norton, T.B (2018, June 6). *Transparency and the marketplace for student data* (p.3). Center on Law and Information Policy, Fordham University. Retrieved July 13, 2020, from https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1003&context=clip

10 Russell, N.C., Reidenberg, J.R., Martin, E., Norton, T.B (2018, June 6). *Transparency and the marketplace for student data* (p.3). Center on Law and Information Policy, Fordham University. Retrieved July 13, 2020, from https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1003&context=clip

11 Federal Trade Commission (2014, May). *Data brokers: A call for transparency and accountability* (p. iv). Retrieved July 13, 2020, from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

For examples, see:

Boninger, F., Molnar, A., & Saldaña, C.M. (2019). Personalized learning and the digital privatization of curriculum and teaching. Boulder, CO: National Education Policy Center. Retrieved July 13, 2020, from http://nepc.colorado.edu/publication/personalized-learning

Boninger, F., Molnar, A., & Saldaña, C. (2020). *Big claims, little evidence, lots of money: The reality behind the Summit Learning Program and the push to adopt digital personalized learning platforms*. Boulder, CO: National Education Policy Center. Retrieved July 9, 2020, from http://nepc.colorado.edu/publication/summit-2020

Marachi, R. & Quill, L. (2020). The case of Canvas: Longitudinal datafication through learning management systems. *Teaching in Higher Education, 25*(4), 418-434. Retrieved July 13, 2020, from https://www.tandfonline.com/doi/abs/10.1080/13562517.2020.1739641?journalCode=cthe20

12 Boninger, F., Molnar, A., & Saldaña, C. (2020). *Big claims, little evidence, lots of money: The reality behind the Summit Learning Program and the push to adopt digital personalized learning platforms*. Boulder, CO: National Education Policy Center. Retrieved July 9, 2020, from http://nepc.colorado.edu/publication/summit-2020

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information* (p.141). Cambridge, MA: Harvard University Press.

13 Newman, L.H. (2020, July 1). Schools already struggled with cybersecurity. Then came Covid-19. *Wired*. Retrieved July 13, 2020, from https://www.wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19/

14 Frida Alim and her colleagues report results of and follow-up to an online survey they conducted in 2015-2016. As part of the follow-up, they contacted all the companies that provided software applications reported by their respondents as being used in their or their children's schools. They examined the privacy policies, data retention practices, and use of encryption in these applications. The other references here point to specific

examples of security breaches.

Alim F., Cardozo, N., Gebhart, G., Gullo, K, & Kalia, A. (2017, April 13). *Spying on students: School-issued devices and student privacy*. Electronic Frontier Foundation. Retrieved July 13, 2020, from https://www.eff.org/wp/school-issued-devices-and-student-privacy

Edwards, E. (2017, April 11). Primary school pupils' data held to ransom by hackers. *Irish Times*. Retrieved July 13, 2020, from https://www.irishtimes.com/news/ireland/irish-news/primary-school-pupils-data-held-to-ransom-by-hackers-1.3044951

Gurney, K. (2017, June 18). Hack attacks highlight vulnerability of Florida schools to cyber crooks. Miami Herald. Retrieved July 13, 2020, from http://www.miamiherald.com/news/local/education/article156544589.html

Wan, T. (2017, April 20). Schoolzilla 'file configuration error' exposes data for more than 1.3M students, staff. *EdSurge*. Retrieved July 13, 2020, from https://www.edsurge.com/news/2017-04-20-schoolzilla-file-configuration-error-exposes-data-for-more-than-1-3m-students-staff

15 United States Federal Bureau of Investigation (2018, September 13). *Education technologies: Data collection and unsecured systems could pose risks to students*. Author. Retrieved July 13, 2020, from https://www.ic3.gov/media/2018/180913.aspx

16 Molnar, A., Miron, G., Elgeberi, N., Barbour, M.K., Huerta, L., Shafer, S.R., & Rice, J.K. (2019). *Virtual schools in the U.S. 2019 (Section 1: Full-time virtual and blended schools: Enrollment, student characteristics, and performance*, p. 3). Boulder, CO: National Education Policy Center. Retrieved July 9, 2020, from http://nepc.colorado.edu/publication/virtual-schools-annual-2019

17 Cuban, L. (2016, July 27). Consumer choice in schooling: Algorithms and personalized learning (Part 1). *Larry Cuban on School Reform and Classroom Practice*. Retrieved July 13, 2020, from https://larrycuban.wordpress.com/2016/07/27/consumer-choice-in-schooling-algorithms-and-personalized-learning-part-1/

18 For example:

Consumer Financial Protection Bureau (2016, June 13). *What is a FICO score?* Author. Retrieved July 13, 2020, from https://www.consumerfinance.gov/askcfpb/1883/what-is-fico-score.html

Hao, K. & Stray, J. (2019, October 17). Can you make AI fairer than a judge? Play our courtroom algorithm game. *MIT Technology Review*. Retrieved July 13, 2020, from https://www.technologyreview.com/2019/10/17/75285/ai-fairer-than-judge-criminal-risk-assessment-algorithm/

19 Alim, F., Cardozo, N., Gebhart, G., Gullo, K., & Kalia, A. (2017, April 13). *Spying on students: School-issued devices and student privacy* (pp. 15-16). Electronic Frontier Foundation. Retrieved July 13, 2020, from https://www.eff.org/wp/school-issued-devices-and-student-privacy

20 Summit Learning (2020. June 22). Partner schools terms of service [website]. Retrieved July 13, 2020, from https://www.summitlearning.org/privacy-center/partner-terms-of-service

21 Narayanan, A. & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. *SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy,* pp. 111-125. Retrieved July 13, 2020, from https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

For discussion of re-identification of data collected by educational software, see:

Boninger, F., Molnar, A., & Saldaña, C. (2020). *Big claims, little evidence, lots of money: The reality behind the Summit Learning Program and the push to adopt digital personalized learning platforms*. Boulder, CO: National Education Policy Center. Retrieved July 13, 2020, from http://nepc.colorado.edu/publication/summit-2020

22 Pearson Education Inc. (2015). *Schoolnet instructional improvement system: Powering classroom achievement*. Retrieved July 13, 2020, from https://www.pearsonassessments.com/content/dam/school/global/clinical/us/assets/schoolnet/schoolnet-overview-brochure.pdf

Sulerzyski, V. (2018, December 17). Personal correspondence (email) with Faith Boninger.

23 Ravindranath,M. (2019, February 3). How your health information is sold and turned into 'risk scores.' *Politico*. Retrieved July 13, 2020, from https://www.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978

24 Marachi, R. & Quill, L. (2020). The case of Canvas: Longitudinal datafication through learning management systems (p. 423). *Teaching in Higher Education, 25*(4), 418-434. Retrieved July 13, 2020, from https://www.tandfonline.com/doi/abs/10.1080/13562517.2020.1739641?journalCode=cthe20

25 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 July 13, 2020, from http://digitalads.org/documents/digiMarketingFull.pdf

Simon, S. (2014, May 15). The big biz of spying on little kids. Politico. Retrieved July 13, 2020, from http://www.politico.com/story/2014/05/data-mining-your-children-106676.html

26 "Family Educational Rights and Privacy Act" (FERPA). 20 U.S.C. § 1232g. Retrieved July 13, 2020, from https://www.law.cornell.edu/uscode/text/20/1232g

Simon, S. (2014, May 15). For sale: Student 'hopes and dreams.' Politico. Retrieved July 13, 2020, from https://www.politico.com/story/2014/05/student-data-privacy-market-106692

27 Boninger, F., Molnar, A., & Saldaña, C.M. (2019). *Personalized learning and the digital privatization of curriculum and teaching* (pp. 34-35, 38). Boulder, CO: National Education Policy Center. Retrieved July 13, 2020, from http://nepc.colorado.edu/publication/personalized-learning

28 Marachi, R. & Quill, L. (2020). The case of Canvas: Longitudinal datafication through learning management systems (pp. 424-425). *Teaching in Higher Education, 25*(4): 418-434. Retrieved July 13, 2020, from https://www.tandfonline.com/doi/abs/10.1080/13562517.2020.1739641?journalCode=cthe20

See also:

Federal Trade Commission (2014, May). *Data brokers: A call for transparency and accountability* (p. iv). Retrieved July 9, 2020, from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

29 Wheaton, K. (2015, March 23). Hocus pocus! Your data has been anonymized! Now they'll never find you! *Advertising Age*. Retrieved July 13, 2020, from http://adage.com/article/ken-wheaton/data-anonymized-find/297713/

30 State of New Mexico v. Google LLC (D. New Mexico 2020). Retrieved September 3, 2020, from https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Sues_Google_for_Illegally_Collecting_Personal_Data_of_New_Mexican_School_Children.pdf

The text of the Children's Online Privacy Protection Act (COPPA) can be found at:

*Children's Online Privacy Protection Act of 1998*, 15 U.S.C. §§ 6501-6506. Retrieved January 8, 2015, from http://www.law.cornell.edu/uscode/text/15/chapter-91

31 Greenwich Public Schools (2014, December 23). *iPads for elementary students, Chromebooks for secondary students* [press release]. Retrieved July 13, 2020, from http://www.greenwichschools.org/uploaded/district/pdfs/News_Archives/News_Archives_2014-15/PR_-_DLE_Phase_III_Device_122314.pdf

32 Wheaton, K. (2015, March 23). Hocus pocus! Your data has been anonymized! Now they'll never find you! *Advertising Age*. Retrieved July 13, 2020, from http://adage.com/article/ken-wheaton/data-anonymized-find/297713/

33 Wheaton, K. (2015, March 23). Hocus pocus! Your data has been anonymized! Now they'll never find you! *Advertising Age*. Retrieved July 13, 2020, from http://adage.com/article/ken-wheaton/data-anonymized-find/297713/

34 Narayanan, A. & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. *SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy,* pp. 111-125. Retrieved July 13, from https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

Narayanan, A. and Shmatikov, V. (2019, May 21). *Robust de-anonymization of large sparse datasets: a decade later*. Unpublished manuscript. Retrieved July 13, 2020, from https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf

Kreuter, F. (2019, September 4). Personal communication (telephone) with Faith Boninger.

For discussion of the "5 Safes" approach to protecting the privacy of data, see:

Stokes, P. (2017, January 27). The 'five safes' – Data privacy at ONS [blog post]. *National Statistical*. Retrieved July 13, 2020, from https://blog.ons.gov.uk/2017/01/27/the-five-safes-data-privacy-at-ons/

35 Winterton, J. (2017, February 8). Personal communication (in person) with Faith Boninger.

36 Levin, D.A. (2020). *The state of K-12 cybersecurity: 2019 year in review* (p. 7). Arlington, VA: EdTech Strategies LLC/The K-12 Cybersecurity Resource Center. Retrieved July 13, 2020, from https://k12cybersecure.com/year-in-review/

37 Levin, D.A. (2020). *The state of K-12 cybersecurity: 2019 year in review* (p. 8). Arlington, VA: EdTech Strategies LLC/The K-12 Cybersecurity Resource Center. Retrieved July 13, 2020, from https://k12cybersecure.com/year-in-review/

38 For further discussion, see:

Boninger, F. & Molnar, A. (2016). *Learning to be watched: Surveillance culture at school—The eighteenth annual report on schoolhouse commercializing trends, 2014-2015*. Boulder, CO: National Education Policy Center. Retrieved July 13, 2020, from http://nepc.colorado.edu/publication/schoolhouse-commercialism-2015

Alim F., Cardozo, N., Gebhart, G., Gullo, K., & Kalia, A. (2017, April 13). *Spying on students: School-issued devices and student privacy*. Electronic Frontier Foundation. Retrieved July 13, 2020, from https://www.eff.org/wp/school-issued-devices-and-student-privacy

39 "Family Educational Rights and Privacy Act" (FERPA). 20 U.S.C. § 1232g. Retrieved July 13, 2020, from https://www.law.cornell.edu/uscode/text/20/1232g

40 Future of Privacy Forum and The Software & Information Industry Association (2016). *Student Privacy Pledge: Signatories*. Retrieved July 13, 2020, from https://studentprivacypledge.org/signatories/

41 For the text of the law, see:

"Family Educational Rights and Privacy Act" (FERPA). 20 U.S.C. § 1232g. Retrieved July 13, 2020, from https://www.law.cornell.edu/uscode/text/20/1232g

42 U.S. Department of Education Office of Inspector General (2018, November 26). Office of the Chief Privacy Officer's Processing of Family Educational Rights and Privacy Act Complaints (ED-OIG/A09R0008). Retrieved July 13, 2020, from https://www2.ed.gov/about/offices/list/oig/auditreports/fy2019/a09r0008.pdf

43 For discussion of the lack of accountability associated with the Student Privacy Pledge, see:

Boninger, F. & Molnar, A. (2016). *Learning to be watched: Surveillance culture at school—The eighteenth annual report on schoolhouse commercializing trends, 2014-201* (pp. 17-18). Boulder, CO: National Education Policy Center. Retrieved July 13, 2020, from http://nepc.colorado.edu/publication/schoolhouse-commercialism-2015

Frida Alim and her colleagues at the Electronic Frontier Foundation (EFF) report on the Federal Trade Commission's inactivity with respect to EFF's complaint about Google. For EFF's report, see:

Alim F., Cardozo, N., Gebhart, G., Gullo, K, & Kalia, A. (2017, April 13). *Spying on students: School-issued devices and student privacy* (p.25). Electronic Frontier Foundation. Retrieved July 13, 2020, from https://www.eff.org/wp/school-issued-devices-and-student-privacy

44 Campaign for Commercial-Free Childhood (2019, September 4). *Advocates who filed the privacy complaint against Google/YouTube laud improvements, but say FTC settlement falls far short* [press release]. Retrieved July 9, 2020, from https://www.commondreams.org/newswire/2019/09/04/advocates-who-filed-privacy-complaint-against-googleyoutube-laud-improvements

45 For examples, see:

"Oregon Student Information Protection Act," ORS 336.184. Retrieved July 13, 2020, from https://www.oregonlaws.org/ors/336.184

"Student Data Transparency and Security Act," C.R.S. § 22-16-101 et seq. Retrieved July 13, 2020, from http://www.cde.state.co.us/dataprivacyandsecurity/crs22-16-101

"Student Online Personal Information Protection Act," Cal Bus & Prof Code § 22584 (2015). Retrieved May 19, 2020, from https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.2.&article=

46 Stokes, P. (2017, January 27). The 'five safes' – Data privacy at ONS [blog post]. *National Statistical*. Retrieved July 13, 2020, from https://blog.ons.gov.uk/2017/01/27/the-five-safes-data-privacy-at-ons/

47 Boninger, F., Molnar, A., & Saldaña, C.M. (2019). *Personalized learning and the digital privatization of curriculum and teaching* (pp. 8-9). Boulder, CO: National Education Policy Center. Retrieved July 9, 2020, from http://nepc.colorado.edu/publication/personalized-learning

Boninger, F., Molnar, A., & Saldaña, C. (2020). *Big claims, little evidence, lots of money: The reality behind the Summit Learning Program and the push to adopt digital personalized learning platforms* (Appendix A), Boulder, CO: National Education Policy Center. Retrieved July 9, 2020, from http://nepc.colorado.edu/publication/summit-2020

48 Safier, D. (2008a, August 7). AZ online charter school outsources education. *Blog for Arizona: Arizona and national politics and policy from a liberal perspective*. Retrieved July 19, 2020, from https://arizona.typepad.com/blog/2008/08/az-online-chart.html

49 Safier, D. (2008a, August 25). An explanation of the AZVA outsourcing process. *Blog for Arizona: Arizona and national politics and policy from a liberal perspective*. Retrieved July 19, 2020, from https://arizona.typepad.com/blog/2008/08/an-explanation.html

50 Trotter, A. (2008, September 5) K12 Inc. scraps India outsourcing. *Education Week*. Retrieved July 19, 2020, from https://www.edweek.org/ew/articles/2008/09/10/03outsource.h28.html

51 Manning, T. (2013, September 2013). More reasons you should be concerned with K12 Inc. *Idaho Press*. Retrieved July 19, 2020, from https://www.idahopress.com/members/more-reasons-you-should-be-concerned-with-k-inc/article_38a0056a-27c4-11e3-aaed-0019bb2963f4.html

52 Cotterell, A. (2013, October 14). Idaho's largest charter school confirms it outsourced student papers to India. *Boise State Public Radio: NPR in Idaho*. Retrieved July 19, 2020, from https://www.boisestatepublicradio.org/post/idahos-largest-charter-school-confirms-it-outsourced-student-papers-india#stream/0

53 Colby, L. (2015, June 18). Teachers at online school say it abused student privacy and misused funds. *Bloomberg*. Retrieved July 19, 2020, from https://www.bloomberg.com/news/articles/2015-06-18/teachers-at-k12-s-schools-allege-privacy-funding-violations

54 Brown, E. (2015, June 19). Teachers allege problems at California virtual schools run by Va.-based company K12 Inc. (¶ 9). *The Washington Post*. Retrieved July 19, 2020, from https://www.washingtonpost.com/local/education/teachers-allege-problems-at-california-virtual-schools-run-by-va-based-company-k12-inc/2015/06/19/dd3b4ab0-1699-11e5-89f3-61410da94eb1_story.html

55 Kim, Y. (2014, November 18). *Public communication to H. Madom*. Retrieved July 19, 2020, from http://k12.mediaroom.com/download/CA+Dept+of+Ed+letter+dismissing+CA+Teachers+Assoc+SPED+complaints+Nov+2014.pdf

56 California Virtual Academies (2016, January 13). *Notice of data breach* (¶ 1) Retrieved July 19, 2020, from https://oag.ca.gov/system/files/CAVA%20Notice%20of%20Data%20Breach_Teacher%20Notice_0.pdf

57 Network for Public Education (2018). *Online learning: What every parent should know*. Retrieved July 19, 2020, from https://npe.wpengine.com/wp-content/uploads/2019/01/Online-Learning-What-Every-Parent-Should-Know.pdf

58 Network for Public Education (2018). *Online learning: What every parent should know* (p. 16). Retrieved July 19, 2020, from https://npe.wpengine.com/wp-content/uploads/2019/01/Online-Learning-What-Every-Parent-Should-Know.pdf