Student Data Privacy, Digital Learning, and Special Education: Challenges at the Intersection of Policy and Practice

William M. (Skip) Stahl, M.S., and Joanne Karger, J.D., Ed.D.
Center for Applied Special Technology, Inc.

- **Researchers at the Center on Online Learning and Students with Disabilities have identified considerable benefits—for both accountability and instructional efficacy purposes—that can be achieved when research is conducted, combining student demographic, achievement, and system usage data that are obtained through digital learning environments.**
- **At the same time, the growing prevalence of networked digital learning systems capable of collecting and storing extensive amounts of student-specific data has raised questions and concerns about student privacy, and, within the current climate of student data vigilance, the full benefits of research utilizing digital data remain elusive.**
- **Allowances for sharing student data for legitimate and authorized research purposes exist under current privacy laws, yet the complex nature of the legal requirements creates confusion with respect to how, and by whom, such research authorization should occur.**
- **Clearer federal and state-level policy guidance, combined with the creation of trusted partnerships between school personnel, digital education providers, and researchers, can overcome these limitations and benefit all students, in particular those with disabilities.**

Student Data Privacy, Digital Learning, and Students with Disabilities

The rapid adoption of digital content and delivery systems, each with its own capacity to track, store, and analyze student usage, interactions, and academic outcomes at both a highly detailed and granular level, has emerged as an area of widespread opportunity, but also of concern. The comingling of various student data sets (demographics, usage, and achievement) now possible as the result of data interoperability standards has raised the specter of dangerous and privacy-invading misuse, simultaneous with the potential for customizing education for every student. Most Internet-enabled digital learning environments can record timely information on students: where they are, what they are doing, how they got there, how long they stayed, and where they went, as well as formative and summative details of their academic achievement.

Research utilizing data from digital learning environments has the potential to improve teaching and learning in unprecedented ways. For students with disabilities, this information can provide unique insights into the impact of curriculum and school reform efforts on the progress of these students. Digital learning systems and the data they collect offer a timeliness and specificity that can be otherwise impractical or impossible to acquire. In optimal circumstances, digital data analysis can cross-reference student demographic information (age, disability

The contents of this article were developed under a grant from the U.S. Department of Education #H327U110011. However, those contents do not necessarily represent the policy of the U.S. Department of Education, and you should not assume endorsement by the Federal Government. Project Officer, Celia Rosenquist.

type, allocated accommodations and modifications, etc.) with real-time curriculum activities and academic achievement outcomes. The information that results from combining these data sets can be beneficial to students, school personnel, curriculum designers, and researchers (with respect to creating and implementing effective instructional approaches and materials), while simultaneously meeting many of the reporting requirements unique to students with disabilities.

Digital learning systems and the data they collect offer timely and specific information that can otherwise be impractical or impossible to acquire.

This positive outcome, however, can only be achieved with clear and legally compliant data-sharing procedures in place. The promising opportunities created by research involving digital student data are accompanied by the rise of serious questions regarding student privacy. Concerns abound with respect to whether data that are collected will have a subsequent negative impact on students' future life opportunities and whether hackers and commercial marketers will be able to penetrate the data system. For students with disabilities, the dangers posed are of serious consequence in light of the confidential and potentially sensitive nature of the information involved.

In the present climate, the protective vigilance triggered by the perceived liabilities inherent in large-scale data sharing is apparent, and the confusing legality of widespread data tracking threatens to limit opportunities for research. This article explores the relationship between student privacy and research on digital learning for all students, and students with disabilities in particular. The article begins with a discussion of the benefits of using digital data for students with disabilities, as well as some of the privacy concerns associated with the use of such data. Next, the article examines the legal parameters underlying the collection and use of digital data (for research purposes) for all students, and students with disabilities in particular. The article concludes with recommendations for state, district, and school personnel, as well as policy makers, to help them move forward in support of research while at the same time protecting the privacy rights of all students, including those with disabilities.

Benefits of and Concerns with the Use of Digital Data

Benefits of the Use of Digital Data for Students with Disabilities

Educational progress reporting for students with disabilities is mandated under the Individuals with Disabilities Education Act (IDEA), the federal special education law, both with respect to the individual student (20 U.S.C. § 1414 (d)(1)(A)(i)(III)) and the group as a whole (20 U.S.C. §§ 1412 (a)(15)(C), (16)(D)(iv)). Reporting on the progress of students with disabilities is also required under the Elementary and Secondary Education Act, recently reauthorized as the Every Student Succeeds Act of 2015 (20 U.S.C. § 6311 (b)(2)(B)(xi)(III)). If sufficiently specific and accurate, this information has the potential to provide unique insights into the impact of curriculum and school reform efforts on the progress of these students. The collection of large amounts of detailed data on student activity is a new affordance of digital and online learning environments and creates new opportunities for researching and understanding student learning behavior and progress, as well as for providing more individualized support for diverse learners (Romero & Ventura, 2010; Tanenbaum, LeFloch, & Boyle, 2013).

Many online learning systems capture real-time information on students: what they are doing, where they are doing it, how they got there, how long they stayed, and where they went.

Analyzing large student data sets, especially those that triangulate student demographic information (including disability status) with academic achievement and digital system usage data, can produce meaningful correlation profiles (Bienkowski, Feng, & Means, 2012; Reshef et al., 2011). Many online learning systems capture real-time information on students: what they are doing, where they are doing it, how they got there, how long they stayed, and where they went. When these data points are combined with historical achievement data and cross-referenced with

Individualized Education Program (IEP) information, the resulting correlations can identify factors associated with greater than or less than anticipated academic growth. While not causal (i.e., the data do not identify why something is happening), the data nevertheless explain what is happening, and that information can prove useful for accountability reporting and instructional efficacy purposes. Data patterns that remain disaggregated (e.g., which students with which types of disabilities do best with which materials and supports under which circumstances) can yield information that might be otherwise unavailable.

Concerns with the Use of Digital Data for All Students, Including Those with Disabilities

While the collection and effective use of digitized student data has the potential to lead to improvements in teaching and learning for all students, including those with disabilities, parents and privacy advocates have begun to express concerns about the increased availability (to third parties) of such data. A recent survey examining the views of more than 1,000 parents regarding the use of technology in classrooms found that 79% of respondents were somewhat concerned or extremely/very concerned with privacy issues (Marketplace, 2015 as cited by Krueger & Moore, 2015b). Such privacy concerns tend to focus on what data is being tracked and stored as well as to whom and under what circumstances the information is made available (Zeide, 2014).

A major concern with privacy relates to the fear that student data could be used at a later time to stigmatize or otherwise adversely impact the student. In particular, some worry that a record of the student's negative behaviors or poor academic performance could ultimately interfere with future educational and/or employment opportunities (Sirota, 2013; Zeide, 2014). These concerns may be more pronounced with respect to students with disabilities in light of the potentially sensitive nature of the data being collected. For example, such data might describe challenges associated with the student's disability, correspond to negative labels of the student's performance, or refer to the student's specific disciplinary infractions. This kind of information, in contradistinction to the rights of these students under special education and civil rights law, could potentially be used to deny the students' access to certain classes or programs, or lead to the emergence of biases on the part of teachers and staff.

…some worry that a record of the student's negative behaviors or poor academic performance could ultimately interfere with future educational and/or employment opportunities (Sirota, 2013; Zeide, 2014).

Another concern associated with privacy relates to the safeguarding of digital student data. Parents and privacy advocates have raised the question of whether the data being collected could ultimately be used for noneducational purposes should it be accessed by hackers or commercial marketers (Kamenetz, 2014; Krueger & Moore, 2015a; Singer, 2014). While there have yet to be reports of data leaks from large student data sets at the K–12 level, evidence of such breaks have begun to appear at the postsecondary level (Kamenetz, 2014). Similarly, there is concern that student data could be sold to marketers. In a large study of the cloud computing practices of school districts, the Center on Law and Information Policy at Fordham Law School found that, in many instances, the language in district contracts with third party vendors was ambiguous and that none of the contracts that they examined contained an express provision to prohibit the sale or use of data for marketing (Reidenberg et al., 2013). Without sufficient attention to data safeguarding, there is the risk that research efforts will be hindered, and stakeholders will be unable to reap the full benefits of collecting and using digital student data.

Legal Requirements Pertaining to Student Privacy

For a clearer understanding of the current student data privacy landscape and its effect on efforts to conduct research involving digital student data as an indicator of educational impact with respect to all students, in particular those with disabilities, a review of applicable federal statutes and regulations, as well as corresponding state-level initiatives, is warranted.

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA), originally enacted in 1974, prohibits educational agencies or institutions from denying parents and eligible students certain rights with respect to student education records (20 U.S.C. § 1232g; 34 C.F.R. § 99.1 *et seq.*). FERPA applies to all students and is not limited to students with disabilities. Under FERPA, parental rights, or student rights in the case of a student who has reached the age of 18 or attended a postsecondary institution, include the right to inspect and review the student's education records and to request an amendment to or challenge the information contained in these records in order to ensure that it is not inaccurate or misleading. (20 U.S.C. §§ 1232g(a)(1), (2); 34 C.F.R. §§ 99.10–99.12, 99.20–99.22).

In addition, except under certain narrow circumstances, FERPA prohibits educational agencies or institutions from disclosing personally identifiable information (PII) contained in the student's education records to a third party without the prior written consent of the student's parents (or an eligible student) (20 U.S.C. § 1232g(b); 34 C.F.R. §§ 99.30–99.39). PII includes information such as the student's name, names of the student's family members, address of the student or his/her family, the student's social security number, the student's date of birth or "other information that … is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty" (34 C.F.R. § 99.3).

…FERPA prohibits educational agencies or institutions from disclosing personally identifiable information (PII) contained in the student's education records to a third party without the prior written consent of the student's parents (or an eligible student) (20 U.S.C. § 1232g(b); 34 C.F.R. §§ 99.30–99.39).

What follows is a discussion of specific circumstances, relevant to the present article, under which FERPA permits PII to be released without prior written consent. These exceptions, which apply to all students, including those with disabilities, pertain to the conducting of research that utilizes digital student data. Because these legal requirements are complex and confusing, they likely contribute to a level of uncertainty on the part of educational personnel who make decisions about entering into research agreements.

Organizations Conducting Studies. The exception to the "prior written consent" requirement that is perhaps most pertinent to the current discussion is the exception for "organizations conducting studies for, or on behalf of, educational agencies or institutions" (20 U.S.C. § 1232g (b)(1)(F)). Although an educational agency using the studies' exception is not required to initiate the study or agree with or endorse the conclusions/results of the study (34 C.F.R. § 99.31(a)(6)(iv)), the phrase "for, or on behalf of" indicates that the agency or institution agrees with the purposes of the study and retains control over the information from the education records that is disclosed (U.S. Department of Education, 2008, at 15581).

According to FERPA regulations, educational agencies or institutions may invoke the studies' exception only if:

(A) The study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information;
(B) The information is destroyed when no longer needed for the purposes for which the study was conducted; and
(C) The educational agency or institution…enters into a written agreement with the organization (34 C.F.R. §§ 99.31(a)(6)(iii)(A)-(C)).

This written agreement must include the purpose, scope, and duration of the study, as well as the information that will be disclosed (34 C.F.R. § 99.31(a)(6)(iii)(C)(1)). In addition, the agreement must require that all PII be used only for the purposes of the study and that the study be conducted in a manner that does not permit personal identification of parents and students (34 C.F.R. §§ 99.31(a)(6)(iii)(C)(2), (3)). Finally, the agreement must require that the organization destroy all PII when no longer needed for the purposes of the study and specify the time period in which the information must be destroyed (34 C.F.R. § 99.31(a)(6)(iii)(C)(4)).

Audits and Evaluations. An additional exception to the "prior written consent" requirement permits "authorized representatives" to have access to education records in connection with an audit or evaluation (34 C.F.R. § 99.35(a)(1)). An authorized representative includes any entity or individual designated by a state or local educational authority to conduct any audit or evaluation (34 C.F.R. § 99.3). The state or local educational authority must use reasonable methods to ensure to the greatest extent practicable that the authorized representative uses PII only to carry out the audit or evaluation, protects the PII from further disclosures or other uses, and destroys the PII in accordance with specific requirements (34 C. F.R. § 99.35(a)(2)). Similar to the studies' exception, the audit and evaluations' exception also requires the state or local educational authority to use a written agreement that provides for specific assurances (34 C. F.R. § 99.35(a)(3)). The United States Department of Education has provided examples of best practices that apply to data sharing under both the audit/ evaluation and studies exceptions (U.S. Department of Education, 2011 at 75649).

Directory Information and Electronic Personal Identifiers. FERPA permits educational agencies and institutions to disclose "directory information" without first obtaining written consent if parents (or eligible students) have been provided notice of the kinds of information that are being designated as directory information and have been provided the opportunity to opt out of having directory information released (34 C.F.R. § 99.37). Directory information refers to information that is a part of an education record that, if disclosed, would not generally be considered harmful or constitute an invasion of privacy (34 C.F.R. § 99.3). Directory information may include a student's name, address, telephone number, email address, date of birth, and other identifying information (20 U.S.C. § 1232g(a)(5)(A)). The fact that some information, such as a student's name and address, can be identified as both private/protected (PII) and public/disclosable (directory information) likely creates understandable confusion in the minds of the education personnel charged with enforcing statutory privacy requirements.

FERPA regulations further specify that directory information does not include a student's Social Security Number (SSN) or student identification number except for electronic personal identifiers (34 C.F.R. § 99.3). Given the prevalence of electronic personal identifiers in online student learning systems, this exception has implications for research involving digital student data. The regulations state that a student's "ID number, user ID, or other unique personal identifier used by a student for purposes of accessing or communicating in electronic systems" may be included under directory information "only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password or other factor known or possessed only by the authorized user" (34 C.F.R. § 99.3).

Moreover, the FERPA regulations state that an educational agency or institution, or any party that has received education records or information from education records, may release, without consent, information from education records that has been de-identified through the removal of all PII, "provided that the educational agency or institution or other party has made a reasonable determination that a student's identity is not personally identifiable…and taking into account other reasonably available information" (34 C.F.R. § 99.31(b)(1)).

The regulations also allow for the release of de-identified student-level data from education records for the specific purpose of education research through the attachment of a code to each record that would allow the recipient to match information from the same source (34 C.F.R. § 99.31(b)(2)). The releasing party may not disclose any information that explains how the codes were generated and assigned or that would allow the recipient to identify a student based on the code (34 C.F.R. § 99.31(b)(2)(i)). In addition, the code, which may not be based on a student's SSN or other personal information, may not be used for any purpose other than identifying a de-identified record used for education research and cannot be used to ascertain PII about a student (34 C.F.R. §§ 99.31(b)(2) (ii)-(iii)). According to the U.S. Department of Education (2008), these provisions are intended to help "establish an appropriate balance that facilitates educational research and accountability while preserving the privacy protections in FERPA" (15585).

Individuals with Disabilities Education Act

Eligible children with disabilities are entitled to additional privacy protections concerning confidentiality of records under IDEA (34 C.F.R. §§ 300.610-300.627). These requirements underscore the

fact that there may be sensitive information contained in the education records of students with disabilities. The IDEA regulations refer back to FERPA in a number of instances. Similarly, a note appearing at the beginning of the FERPA regulations specifically references the requirements regarding the confidentiality of information under IDEA (34 C.F.R. § 99.2).

At the same time, the IDEA regulations offer additional protections. Under IDEA, the state educational agency (SEA) must give adequate notice to parents, describing the children on whom PII is maintained, the types of information sought, the methods for gathering and using such information, and a summary of the policies and procedures that districts must follow regarding storage, disclosure to third parties, retention and destruction of PII, and a description of the rights of parents and children regarding PII, including their rights under FERPA (34 C.F.R. § 300.612). Moreover, the SEA must inform parents when information is no longer needed, and the information (except for certain permanent record information) must be destroyed at the request of the parents (34 C.F.R. § 300.624). The SEA must also have in effect policies and procedures, including sanctions, to ensure that its obligations—consistent with the confidentiality of records requirements—are being met (34 C.F.R. § 300.626). Further, each district must have one official who is responsible for ensuring the confidentiality of any PII, must provide training to all persons who are collecting or using PII, and must maintain for public inspection a current listing of the names and positions of all employees who may have access to PII (34 C.F.R. §§ 300.623(b)-(d)). It is important for these requirements, which pertain to students with disabilities receiving special education and related services under IDEA, to be taken into account by states and districts as part of their overall data activities.

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA; 15 U.S.C. §§ 6501-6506) was enacted in 1998 when it became apparent that the Internet and web-based applications had the capability of tracking, eliciting, or otherwise collecting user information. COPPA was designed to protect children under the age of 13 from having their PII used for commercial purposes. The Federal Trade Commission (FTC), which was granted authority to issue and enforce regulations under COPPA, has interpreted the statute as allowing a school to consent (on behalf of the parent) to the disclosure of PII when the school contracts with a third party operator to offer noncommercial online programs that are solely for the benefit of the students and school, including online research and organizational tools (FTC, 2015). In this circumstance, the third party organization, upon request by the school, must provide details of the types of PII it intends to collect; an opportunity to review the child's personal information and/or have the information deleted; and an opportunity to prevent further use or online collection of a child's personal information. Additional requested information may include steps to safeguard the security of the information and how and when it will be removed from third party access. The FTC has advised that, as a best practice, the school should consider making third party operators' notices about their information collection practices available to parents (FTC, 2015).

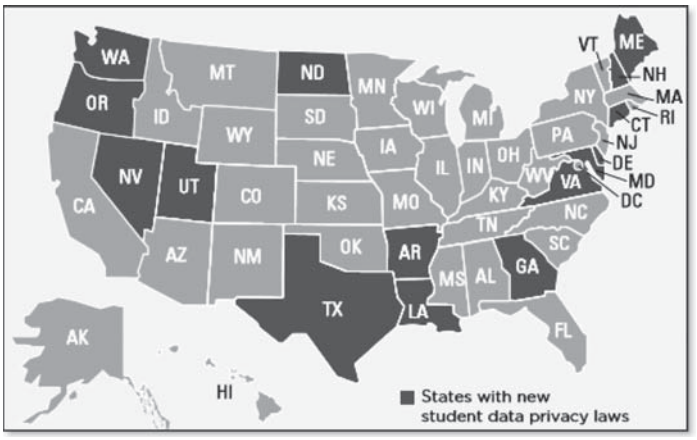
In response to the privacy issues that COPPA was designed to protect, the Software and Information Industry Association (SIIA) has joined with the Future of Privacy Forum (FPF) to craft a "Student Privacy Pledge" to be signed by education industry vendors, including those involved in research, to document their due diligence in protecting student data and adhering to COPPA provisions (FPF & SIIA, 2015). This approach is intended to provide schools with protective consistency as they consider contracts with commercial digital service providers.

State Statutes

In part because of the confusion of the federal requirements regarding student privacy, there has also been extensive activity related to data privacy at the state level. The 2015 publication by the Data Quality Campaign (DQC), "State Student Data Privacy Legislation: What Happened in 2015, and What Is Next?" reported that in 2015, 182 bills were introduced in 46 states, including 28 new student data privacy laws passed in 15 states (see *Figure 1*; DQC, 2015b).

These state legislative efforts addressed a variety of data privacy concerns, including providing access to researchers in the use of digital data. The majority of bills addressing this issue focused on the legitimate purposes for which data may be released to researchers.

Figure 1. As of August 24, 2015, 28 student data privacy bills have been signed into law in 15 states. These 15 states represent a diverse cross-section of the country. The states represent different regions and political environments. Source: Data Quality Campaign (2015b).



Student Data Privacy and Digital Learning: Recommendations for Policy and Practice for All Students, Including Those with Disabilities

The current climate surrounding the use of student data for research is understandably stormy. Efforts to constrain the use of student data to legitimate educational purposes and to protect against marketers, spammers, and identity thieves permeate state legislative sessions and shine a bright spotlight on state- and district-level student data practices and decision making. The confusing nature of key aspects of federal privacy law generates a heightened sense of vigilance among education personnel with student data access, and research initiatives may consequently be blocked from conducting any student data analysis. To begin to address some of the confusion and help assuage fears, targeted federal and state-level guidance is needed.

Not surprisingly, the PTAC publication, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices," is one of PTAC's most requested documents.

A number of guiding documents have been developed by the Privacy Technical Assistance Center (PTAC), established by the U.S. Department of Education at http://ptac.ed.gov/ in response to the rapid growth and adoption of digital learning, including full-time virtual, blended, and supplemental instructional options. Not surprisingly, the PTAC publication, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices," is one of PTAC's most requested documents. This document addresses the legal requirements concerning student privacy in the context of online educational services (PTAC, 2015b). Because the federal statutes pertaining to student privacy are complex and contain a range of authorized exceptions, this guidance highlights the uniqueness of each individual circumstance.

PTAC's document "Protecting Student Privacy While Using Online Educational Services: Model Terms of Service" offers more specific language for crafting a contract with a digital learning provider, or an authorized exemption agreement for research purposes (PTAC, 2015a). This document specifies privacy-related entries that traditionally appear in a Terms of Service agreement and contrasts "Good" agreement language with language that is designated "WARNING!" due to implications that are too broad or too vague. Guidance of this type can be extremely helpful for educational personnel who may not be experts in student data privacy requirements but who, nevertheless, are responsible for making good faith efforts in this regard. Additionally, in 2014, DQC and the Consortium for School Networking (DQC & CoSN) issued "10 Foundational Principles for Using and Safeguarding Students' Personal Information." These principles, which have been endorsed by the Council of Chief State School Officers (CCSSO, 2015), provide guidance on the development and implementation of processes and procedures to use and safeguard digital student data. The first five principles commit to the use of student data to improve learning, assist in personalizing instruction, enhance the role of teachers, and keep parents informed of student progress. Principles 6 through 10 provide suggestions as to how, to what extent, and by whom student data should be used, in order to ensure that privacy protections are in place. In another document, DQC (2015a) describes three broad areas

that should be addressed in the context of data safeguarding: (1) transparency (i.e., clarity and availability of information regarding data activities); (2) governance (i.e., roles/responsibilities as well as structures that need to be in place to support effective data management); and (3) data protection procedures (i.e., specific processes and procedures to protect data security). Principles 6 through 10 of the "10 Foundational Principles" address all three of these areas.

Although not explicitly mentioned in the "10 Foundational Principles," students with disabilities should be included as part of overall decisions regarding data safeguarding. For example, with respect to transparency, it is important for parents of students with disabilities to understand the intersection of their rights under FERPA and IDEA, to be notified of the specific data (both PII and non-PII) being collected, and to have the right to correct or amend the information that is collected. Similarly, in thinking about governance structures related to data safeguarding, districts should ensure that special education personnel are not only informed about data collection and safeguarding procedures, but are also involved in the decision-making process. Finally, it is also important to ensure that special education personnel and parents are involved in the development process of data protection procedures.

One model piece of legislation at the state level is California's SB-1177, "The Student Online Personal Information Protection Act" (SOPIPA). Enacted in 2014, SOPIPA provides some clear legal and policy guidance related to the prohibition against the use of student data for advertising or marketing. The law also provides a FERPA-aligned exemption for "legitimate research purposes" and includes "student identifiers" in its extensive list of "covered" information that is considered associated with personal identification but may, nevertheless, be used for appropriate research (SOPIPA, 2015). This law, which helps to strike a balance between protecting student privacy rights and facilitating the use of student data for research purposes, has formed the basis for a number of additional state legislative initiatives.

Moving Forward

Given the legal complexities that exist in accurately safeguarding the data (in digital learning environments) that can identify, record, and cross-reference student interactions on a minute-by-minute basis, resistance to sharing that information—even for well-documented and Institutional Review Board–compliant research efforts—is understandable. At the same time, the value of conducting student data research, and its potential to improve educational services for all students, including those with disabilities, is compelling. The goal, therefore, should be to create an environment in which responsible researchers are able to conduct research that will ensure the protection of the privacy rights of students. Clearer federal and state-level policy guidance, combined with the creation of trusted partnerships between schools, digital education providers, and researchers, can help overcome some of the challenges—to the benefit of all students—those with disabilities in particular. The specificity of statutes such as CA SB-1177 can help disperse ambiguities by building on the foundation of federal student privacy law and serving as a model, while adding clarifying detail to guide decisions at the school level and help states and districts move forward in support of research involving digital student data.

References

Bienkowski, M., Feng, M., & Means, B. (2012). *Enhancing teaching and learning through educational data mining and learning analytics*. Washington, DC: Office of Educational Technology, U.S. Department of Education. Retrieved from https://tech.ed.gov/wp-content/uploads/2014/03/edm-la-brief.pdf

Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq*. (2016).

Council of Chief State School Officers. (2015). *CCSSO commits to student data principles*. Washington, DC: Author. Retrieved from http://www.ccsso.org/News_and_Events/Press_Releases/CCSSO_Commits_to_Student_Data_Principles_.html

Data Quality Campaign. (2015a). *Roadmap to safeguarding student data*. Washington, DC: Author. Retrieved from http://dataqualitycampaign.org/wp-content/uploads/2016/03/DQC-roadmap-safeguarding-data-June24.pdf

Data Quality Campaign. (2015b). *State student data privacy legislation: What happened in 2015, and what is next?* Washington, DC: Author. Retrieved from http://dataqualitycampaign.org/wp-content/uploads/2016/03/DQC-Student-Data-Laws-2015-Sept23.pdf

Data Quality Campaign & Consortium for School Networking. (2014). *Student data principles: 10*

foundational principles for using and safeguarding students' personal information. Washington, DC: Author. Retrieved from http://studentdataprinciples.org/wp-content/uploads/2015/03/Student-Data-Principles-FINAL.pdf

Every Student Succeeds Act of 2015, reauthorizing the Elementary and Secondary Education Act, 20 U.S.C. § 6301 *et seq*.; 34 C.F.R. § 200.1 *et seq*. (2016).

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 C.F.R. § 99.1 *et seq*. (2016).

Federal Trade Commission. (2015). *Complying with COPPA: Frequently asked questions*. Washington, DC: Author. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Future of Privacy Forum and The Software & Information Industry Association. (2015). *Student privacy pledge*. Washington, DC: Author. Retrieved from http://studentprivacypledge.org/

Individuals with Disabilities Education Act (IDEA), 20 U.S.C. § 1401 *et seq*.; 34 C.F.R. § 300.1 *et seq. (*2016).

Kamenetz, A. (2014). What parents need to know about big data and student privacy. *National Public Radio*. Retrieved from http://www.npr.org/sections/alltechconsidered/2014/04/28/305715935/what-parents-need-to-know-about-big-data-and-student-privacy

Krueger, K.R., & Moore, B. (2015a). New technology "clouds" student data privacy. *Phi Delta Kappan*, *96*(5), 19–24.

Krueger, K.R., & Moore, B. (2015b). Only trust can allay data privacy concerns. *Phi Delta Kappan*, *97*(2), 80.

Marketplace. (2015). *Parents' attitudes toward education technology (study conducted by Lieberman Research Worldwide)*. Los Angeles, CA: Author. Retrieved from http://cms.marketplace.org/sites/default/files/Education%20Technology%20-%20APM%20Marketplace%20Report.pdf

Privacy Technical Assistance Center. (2015a). *Protecting student privacy while using online educational services: Model terms of service*. Washington, DC: U.S. Department of Education. Retrieved from http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf

Privacy Technical Assistance Center. (2015b). *Protecting student privacy while using online educational services: Requirements and best practices*. Washington, DC: U.S. Department of Education. Retrieved from http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf

Reidenberg, J., Russell, N.C., Kovnot, J., Norton, T.B., Cloutier, R., & Alvarado, D. (2013). *Privacy and cloud computing in public schools (Center on Law and Information Policy Book 2)*. New York, NY: Center on Law and Information Policy, Fordham Law School. Retrieved from http://ir.lawnet.fordham.edu/clip/2

Reshef, D.N., Reshef Y.A., Finucane H.K., Grossman S.R., McVean G., Turnbaugh P. J., … Sabeti, P.C. (2011). Detecting novel associations in large data sets. *Science*, *334*(6062), 1518–1524. doi:10.1126/science.1205438

Romero, C., & Ventura, S. (2010). Educational data mining: a review of the state of the art. *IEEE Transactions on, Systems, Man, and Cybernetics, Part C: Applications and Reviews*, *40*(6), 601–618.

Singer, N. (2014). With tech taking over in schools, worries rise. *New York Times*. Retrieved from http://www.nytimes.com/2014/09/15/technology/with-tech-taking-over-in-schools-worries-rise.html

Sirota, D. (2013). Big data means kids' "permanent records" might never be erased. *Motherboard*. Retrieved from http://motherboard.vice.com/blog/permanent-records-are-hurting-kids

Student Online Personal Protection Act (SOPIPA), CA Senate Bill No. 1177. (2014). Retrieved from: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177

Tanenbaum, C., LeFloch, K., & Boyle, A. (2013) "Are personalized learning environments the next wave of K-12 education reform?" *Education Issue Paper Series: American Institutes for Research*, 1–21. Retrieved from http://www.air.org/files/AIR_Personalized_Learning_Issue_Paper_2013.pdf

U.S. Department of Education. (2008). *Family Educational Rights and Privacy Act; Proposed Rule* (March 28, 2008). 73 Fed. Reg. 15574-15602. Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2008-03-24/pdf/E8-5790.pdf

U.S. Department of Education. (2011). *Family Educational Rights and Privacy Act; Final Rule* (December 2, 2011). 76 Fed. Reg. 75604-75660. Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf

Zeide, E. (2014). *The proverbial "permanent record."* New York, NY: Information Law Institute, New York University School of Law. Retrieved from http://dx.doi.org/10.2139/ssrn.2507326

About the Authors

William (Skip) Stahl, M.S., Center for Applied Special Technology, Inc., 40 Foundry Street, Wakefield, MA 01880, Email: sstahl@cast.org.

Mr. Stahl is Senior Policy Analyst, is the Center for Applied Special Technology (CAST) Project Director of the Center on Online Learning and Students with Disabilities, and Co-Director of the National Center on Accessible Educational Materials for Learning at CAST. Mr. Stahl has extensive experience in the development of technical standards, policies, and

implementation practices related to accessible instructional materials, and a keen interest in the role of data in assessing the impact of digital learning and student with disabilities. Email: sstahl@cast.org

Joanne Karger, J.D., Ed.D., is a Policy Analyst and Research Scientist at CAST. Previously, Dr. Karger was an attorney at the Boston office of the Center for Law and Education, a national, legal advocacy organization that promotes the right of all students, in particular those from low-income backgrounds, to a high-quality education. She has a law degree from Boston College Law School and a doctorate in education from the Harvard Graduate School of Education, where her research focused on special education law and policy.