12-13-2013

Privacy and Cloud Computing in Public Schools

Joel Reidenberg
Fordham University School of Law, JREIDENBERG@law.fordham.edu

N. Cameron Russell
Fordham University School of Law, nrussell2@law.fordham.edu

Jordan Kovnot
Fordham University School of Law

Thomas B. Norton
Fordham University School of Law

Ryan Cloutier
Fordham University School of Law

See next page for additional authors

Authors
Joel Reidenberg, N. Cameron Russell, Jordan Kovnot, Thomas B. Norton, Ryan Cloutier, and Daniela Alvarado

Privacy and Cloud Computing in Public Schools

December 12, 2013

Research Team

Joel R. Reidenberg
Microsoft Visiting Professor of Information Technology Policy, Princeton
Academic Study Director, Fordham CLIP

N. Cameron Russell
Executive Director, Fordham CLIP

Jordan Kovnot
Interim Director and Privacy Fellow, Fordham CLIP (through July 2013)

Thomas B. Norton
Project Fellow, Fordham CLIP

Ryan Cloutier
Project Fellow, Fordham CLIP

Daniela Alvarado
Dean's Fellow, Fordham CLIP

CLIP Center on Law and Information Policy
AT FORDHAM LAW SCHOOL

ACKNOWLEDGEMENTS

The research team would like to give a special thanks to Jamela Debelak and to Steve Mutkoski for their assistance in helping us frame this project and to the participants at a workshop held in Washington, DC, for comments on the research and an earlier draft. We would also like to thank the staff of the school districts that provided us with information.

A gift from Microsoft to the Center on Law and Information Policy at the Fordham University School of Law, New York, NY (Fordham CLIP) supported work on this study.

The views and opinions expressed in this report are those of the authors and are not presented as those of any of the sponsoring organizations or financial supporters of those organizations. Any errors and omissions are the responsibility of the authors.

PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS

EXECUTIVE SUMMARY

Today, data driven decision-making is at the center of educational policy debates in the United States. School districts are increasingly turning to rapidly evolving technologies and cloud computing to satisfy their educational objectives and take advantage of new opportunities for cost savings, flexibility, and always-available service among others. As public schools in the United States rapidly adopt cloud-computing services, and consequently transfer increasing quantities of student information to third-party providers, privacy issues become more salient and contentious. The protection of student privacy in the context of cloud computing is generally unknown both to the public and to policy-makers. This study thus focuses on K-12 public education and examines how school districts address privacy when they transfer student information to cloud computing service providers.

The goals of the study are threefold: first, to provide a national picture of cloud computing in public schools; second, to assess how public schools address their statutory obligations as well as generally accepted privacy principles in their cloud service agreements; and, third, to make recommendations based on the findings to improve the protection of student privacy in the context of cloud computing.

Fordham CLIP selected a national sample of school districts including large, medium and small school systems from every geographic region of the country. Using state open public record laws, Fordham CLIP requested from each selected district all of the district's cloud service agreements, notices to parents, and computer use policies for teachers. All of the materials were then coded against a checklist of legal obligations and privacy norms. The purpose for this coding was to enable a general assessment and was not designed to provide a compliance audit of any school district nor of any particular vendor.

The key findings from the analysis are:

- 95% of districts rely on cloud services for a diverse range of functions including data mining related to student performance, support for classroom activities, student guidance, data hosting, as well as special services such as cafeteria payments and transportation planning.

- Cloud services are poorly understood, non-transparent, and weakly governed: only 25% of districts inform parents of their use of cloud services, 20% of districts fail to have policies governing the use of online services, and a sizeable plurality of districts have rampant gaps in their contract documentation, including missing privacy policies.

- Districts frequently surrender control of student information when using cloud services: fewer than 25% of the agreements specify the purpose 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 change the terms

without notice. FERPA, however, generally requires districts to have direct control of student information when disclosed to third-party service providers.

- An overwhelming majority of cloud service contracts do not address parental notice, consent, or access to student information. Some services even require parents to activate accounts and, in the process, consent to privacy policies that may contradict those in the district's agreement with the vendor. FERPA, PPRA and COPPA, however, contain requirements related to parental notice, consent, and access to student information.

- School district cloud service agreements generally do not provide for data security and even allow vendors to retain student information in perpetuity with alarming frequency. Yet, basic norms of information privacy require data security.

In response to these findings, Fordham CLIP proposes a set of specific, constructive recommendations for school districts and vendors to be able to address the deficiencies in privacy protection. The recommendations address transparency, data governance, contract practices, and contract terms.

Recommendations for Transparency
The existence and identity of cloud service providers and the privacy protections for student data should be available on district websites, and districts must provide notice to parents of these services and the types of student information that is transferred to third parties.

Recommendations for Data Governance
Districts must establish policies and implementation plans for the adoption of cloud services by teachers and staff including in-service training and easy mechanisms for teachers to adopt, and propose technologies for instructional use. Districts must address directly and publicly any policies on the use of student data for advertiser supported services. Districts should create data governance advisory councils for advice and industry should develop mechanisms to help districts vet privacy-safe services and technologies. Finally, larger districts and state departments of education must designate a Chief Privacy Officer to provide advice and assistance.

Recommendations on Contracting Practices
Districts, as stewards of children's information, must properly document all cloud service agreements including maintaining fully executed contracts complete with all appendices and incorporated documents.

Recommendations on Contract Terms
Districts are often passive parties to cloud service contracts that are drafted by vendors and not subject to any negotiations. These agreements must more directly address privacy obligations. To accomplish this, vendors should include the following terms in their agreements: specification of the purpose of the agreement and the authority to enter into the agreement; specification of the types of data transferred or collected; the prohibition or limitation on redisclosure of student data; the prohibition or limitation on

the sale or marketing of student information without express parental consent; the assurance that districts will have exclusive control over data access and mining; the prohibition on new or conflicting privacy terms when parents are required to activate an account for their child; the allocation of responsibilities for granting parental access and correction capabilities; the specification of whether foreign storage and processing is allowed; the specification of whether other government agencies (such as social service agencies) may have access; the specification of data security and breach notification obligations; the prohibition on unilateral modifications; and the inclusion of a right for the district to audit/inspect vendors for compliance with contractual obligations.

Recommendation on the Creation of a National Research Center and Clearinghouse

School districts, cloud service providers, and policy-makers all have a tremendous need for assistance in addressing privacy. A national research center and clearinghouse should be established to prepare academic and policy research, convene stakeholders, draft model contract clauses, privacy notices and consent forms, and create a repository for research, model contracts and policies.

TABLE OF CONTENTS

I. INTRODUCTION

Today, data driven decision-making is at the center of educational policy debates in the United States. This study focuses on K-12 public education in the United States, and how school districts transfer to, or share children's information with, cloud service providers. School districts are increasingly turning to rapidly evolving technologies and cloud computing to satisfy their educational objectives and take advantage of new opportunities for cost savings, flexibility, and always-available service among others. These cloud services are provided by third-parties and enable districts to process their children's data or perform tasks online. Like in the business community, private vendors are developing new services for the education sector. Many of these cloud services are specifically geared toward K-12 schools. For example, one prominent web based student information system is reported to include data on 12 million students in all 50 states.[1] Another private company offers a K-12 survey platform and data analytics to perform "large-scale survey and analysis programs in 4,000 schools across 26 states."[2] One of the most prominent projects seeks to build a cloud database of public school children in multiple states.[3] These programs seek to improve school performance, improve the classroom experience, and enable teachers to address individual student needs.

The transition to cloud services by school districts raises concerns for the privacy of the school children's data because data will no longer be maintained by the school districts themselves, but rather will be sourced in data centers operated by third-parties.[4] Just as

---

[1] *PowerSchool – About PowerSchool*, PEARSON SCHOOL SYSTEMS, http://www.pearsonschoolsystems.com/products/powerschool/(last visited Oct. 31, 2013).

[2] *About Panorama*, PANORAMA EDUCATION, https://www.panoramaed.com/about (last visited Oct. 31, 2013). Panorama Education "conduct[s] surveys of students, parents, teachers, and staff" and then "analyzes this data and presents teachers and administrators with clear and constructive feedback that they can use to improve their teaching and their schools." *Id.* Panorama Education is funded, in part, by Mark Zuckerberg's Startup: Education, Jeff Clavier's SoftTech VC, Google Ventures, Ashton Kutcher's A-Grade Investments, and Yale University. *See* Chris Reidy, *In a Funding Round with Ashton Kutcher, Zuckerberg Makes His First Ed Tech Investment in Cambridge's Panorama Education*, BOSTON GLOBE (Oct. 21, 2013), http://www.boston.com/business/innovation/blogs/inside-the-hive/2013/10/21/mark-zuckerberg-ashton-kutcher-help-seed-cambridge-firm-round/Klu1WNLkYnmZQJO2sGYbPO/blog.html (last visited Dec. 5, 2013).

[3] In February 2013, inBloom announced its launch, with plans to pilot a cloud database service in public schools in nine states: Colorado, Delaware, Georgia, Illinois, Kentucky, Louisiana, Massachusetts, New York, and North Carolina. *See InBloom Press Release*, INBLOOM, https://www.inbloom.org/inbloom-launch (last visited Nov. 5, 2013). New York and Colorado selected districts to perform the testing, specifically, the New York City Department of Education and Jefferson County, Colorado, respectively, which are both included within the data set analyzed in this report. *See id*. InBloom's database compiles personal information such as student names, addresses, and sometimes social security numbers and records learning disabilities, test scores, attendance, and even softer characteristics such as hobbies, career goals and attitudes toward school. *See* Natasha Singer, *Deciding Who Sees Students' Data*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?_r=0. In compiling these records, inBloom seeks to track student progress and even personalize lesson plans as well as create a national database shared with businesses that contract with public schools, which is advertised as a tool to improve educational materials and school curriculums across states. *See id.*; Stephanie Simon, *K-12 student database jazzes tech startups, spooks parents*, REUTERS (Mar. 3, 2013), http://www.reuters.com/article/2013/03/03/us-education-database-idUSBRE92204W20130303. InBloom's open-source code may provide an incentive for developers to create customized apps for schools, thus making the technology cheaper. *See* Singer, *supra* note 3.

[4] In August 2013, the Jefferson County Public Schools district in Colorado held a special school board meeting to voice the concerns of parents, school board members, and education and privacy advocates. *See* Nelson Garcia,

businesses have concerns about the access, use and sharing of their cloud based data, parents worry about the extensive quantity of student data being collected and the access being granted to the data.[5] Many are concerned that the data is held for an indefinite period and that the duration of storage is outside the control of the school system.[6] Similarly, parents worry about the use of children's school data by vendors for marketing purposes.[7] Services such as email and document sharing that are offered to educational institutions for no financial payment also flag privacy and data security concerns.[8] One parent group has warned in reference to the inBloom K-12 program that "[t]he plan to share personally identifiable and highly confidential student data in such an unrestricted manner, in an open-ended time frame, without parental notification or consent, is unprecedented in U.S. history, and would violate both FTC and HIPAA protections if they had authority over student records."[9]

With all the concern and publicity directed toward a few high profile projects, the actual practices and policies being deployed by most school systems to address privacy remain largely unknown. The purpose of this study is, thus, to analyze how public school districts across the country address student privacy when using free or paid cloud computing services provided by outside service providers and vendors. The study will specifically seek to examine how public schools address student privacy obligations under the Family Educational Rights and Privacy Act ("FERPA") and, where applicable, the Children's Online Privacy Protection Act ("COPPA") and the Protection of Pupil Rights Amendment ("PPRA") in their adoption of cloud computing services. The study will also address the sufficiency of student privacy protections in the context of generally-accepted privacy principles. Both the Department of Education and parent surveys

---

Jeffco debates using student data cloud system, 9NEWS.COM (Aug. 22, 2013), http://www.9news.com/news/article/351644/188/Jeffco-debates-using-student-data-cloud-system. *See also* Simon, *supra* note 3. Jefferson County Public Schools (CO) has now withdrawn its participation with inBloom altogether. *See* Vic Vela, *Jeffco Schools: Unanimous vote uproots inBloom*, OURCOLORADONEWS.COM (Nov. 15, 2013), http://www.ourcoloradonews.com/arvada/news/jeffco-schools-unanimous-vote-uproots-inbloom/article_1032f5d2-a38b-54cb-a53e-05af93df8edf.html.

[5] *See* Singer, *supra* note 3:

> InBloom seems designed to nudge schools toward maximal data collection. School administrators can choose to fill in more than 400 data fields. Many are facts that schools already collect and share with various software or service companies: grades, attendance records, academic subjects, course levels, disabilities. Administrators can also upload certain details that students or parents may be comfortable sharing with teachers, but not with unknown technology vendors. InBloom's data elements, for instance, include family relationships ("foster parent" or "father's significant other") and reasons for enrollment changes ("withdrawn due to illness" or "leaving school as a victim of a serious violent incident").

[6] Andrew Ujifusa, *John White Withdraws Louisiana Student Data from inBloom*, EDUCATION WEEK (Apr. 26, 2013), http://blogs.edweek.org/edweek/state_edwatch/2013/04/john_white_backtracks_on_controversial_inbloom_deal_in_louisiana.html.

[7] Corinne Lestch and Ben Chapman, *New York parents furious at program, inBloom, that compiles private student information for companies that contract with it to create teaching tools*, N.Y. DAILY NEWS (Mar. 13, 2013), http://www.nydailynews.com/new-york/student-data-compiling-system-outrages-article-1.1287990#ixzz2juM5Mx1g.

[8] *See, e.g.*, Chris Hoofnagle, *The Good, Not So Good, and Long View on Bmail*, THE BERKELEY BLOG (Mar. 6, 2013), http://blogs.berkeley.edu/2013/03/06/the-good-not-so-good-and-long-view-on-google-mail/.

[9] *See* Ujifusa, *supra* note 6.

indicate that the current statutory rules may be too narrow for the context of cloud computing in public schools.[10]

The study seeks to provide the first national picture of privacy and cloud computing in public schools and seeks to provide educational leaders and policy-makers with useful recommendations based on the information gathered through the project. Part II will first set out the basic statutory obligations for the treatment of school children's data. Part III describes the research methodology, including the process of selecting a meaningful and representative sample of school districts. Part IV provides the findings and analysis. Finally, Part V offers policy recommendations with respect to the sufficiency of student privacy protections and cloud services for primary and secondary school settings.

II. STATUTORY FRAMEWORK

Three federal statutes are critical for the protection of student data when districts transfer or collect that information through cloud computing service arrangements. FERPA[11] governs the disclosure by school districts of educational records and will apply when those records are shared in the cloud. The PPRA[12] regulates the disclosure of certain types of information about school children for analyses or evaluations related to a number of specified characteristics and might apply to various cloud computing activities of districts. And lastly, COPPA[13] regulates the online or web-based collection of information from children and may apply to various cloud services. This Part will outline each of these statutes and their applicability to cloud processing of children's school information.

A. FERPA[14]

FERPA was enacted in 1974 and provides certain minimum privacy protections for educational records.[15] FERPA was passed to protect the privacy of student educational records by regulating to whom and under what circumstances those records may be disclosed. FERPA applies to educational agencies and institutions that receive federal funds administered by the Secretary of Education.[16] Under FERPA, an educational agency or institution is "any public or

---

[10] The chief privacy officer of the Department of Education has indicated that FERPA should be seen as "a floor" for compliance and not the ceiling. *See Privacy and Security Initiatives from the U.S. Department of Education,* EDUCASE REVIEW ONLINE (Feb. 26, 2013), *available at* http://www.educause.edu/ero/article/privacy-and-security-initiatives-and-recommendations-us-department-education (last visited Dec. 10, 2013). A recent parent survey similarly indicated that 75% of parents disapproved of practices including collecting student information and tracking students online for marketing or advertising. *See* Brunswick Insight/SafeGov, 2012 NATIONAL DATA PRIVACY IN SCHOOLS SURVEY at 6 (Jan. 2013), *available at* http://www.safegov.org/media/43502/brunswick_edu_data_privacy_report_jan_2013.pdf (last visited Dec. 10. 2013).

[11] 20 U.S.C. § 1232g (2012). Regulations under FERPA are codified at 34 C.F.R. § 99 (2011).

[12] 20 U.S.C. § 1232h (2012).

[13] 15 U.S.C. § 6501-6506 (2012). Regulations under COPPA are codified at 34 C.F.R. § 98 (1984).

[14] This section is adapted from Fordham CLIP's prior work *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems* (October 28, 2009), *available at* http://ssrn.com/abstract=1495743.

[15] *See generally* 20 U.S.C. § 1232g.

[16] 34 C.F.R. § 99.1.

private agency or institution which is the recipient of funds"[17] if the institution "provides educational services or instruction, or both, to students" or if the institution "is authorized to direct and control public elementary or secondary…educational institutions."[18] FERPA's requirements and prohibitions therefore apply to the districts that receive federal funds. The U.S. Department of Education has the authority to withhold all federal funding to institutions and agencies that do not comply with the provisions of FERPA.[19]

1. Educational Records

FERPA defines educational records to include information "directly related to a student" and "maintained by an educational agency or institution or by a party acting for such agency or institution."[20] These records may include student files, student system databases kept in storage devices, or recordings and/or broadcasts.[21] Records regarding each student that are generated by the local schools are educational records under FERPA, and therefore, disclosures by the local schools to third-party cloud service providers must meet FERPA's requirements. Educational records are comprised of two types of information, directory information and non-directory information, and these two components have different disclosure protections under FERPA.

Directory information may include any of the following: "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student."[22] Educational institutions are required to notify parents regarding what information from the above list they have defined as directory information.[23] Schools may typically disclose directory information without written consent from parents; however, a parent can choose to restrict the release of directory information by submitting a formal request to the school to limit disclosure.[24] Disclosure of directory information therefore operates under an opt-out system. Educational institutions are free to publicly disclose this information unless a parent submits a request to opt-out of disclosure.

Educational records may also consist of non-directory information. Non-directory information is all other information related to a student and maintained by an educational agency or institution including, without limitation, social security numbers or student identification numbers.[25] Subject to certain exceptions discussed below, prior written consent is required before institutions can disclose non-directory information. Prior written consent must include the following elements:

- Specification of the records to be disclosed;
- The purpose of the disclosure;

[17] 20 U.S.C. § 1232g(a)(4).
[18] 34 C.F.R. § 99.1.
[19] 20 U.S.C. § 1232g.
[20] 34 C.F.R. § 99.3.
[21] 20 U.S.C. § 1232g(a)(4)(A).
[22] 20 U.S.C. § 1232g(a)(5)(A).
[23] 20 U.S.C. § 1232g(a)(5)(B).
[24] *See id.*
[25] *See*, *e.g.*, 34 C.F.R. § 99.3 (2011).

- Identification of the party or class of parties to whom the disclosure is to be made;
- Date;
- Signature of the parent of the student whose record is to be disclosed; and
- Signature of the custodian of the educational record.[26]

In addition, educational faculty and staff can only access non-directory information if they have a legitimate academic interest to do so.[27]

2. Rights Afforded Under FERPA

FERPA provides parents of K-12 students with the following rights regarding educational records:

- The right to inspect and review their child's education records;[28]
- The right to seek to amend information in the records they believe to be inaccurate, misleading, or an invasion of privacy;[29]
- The right to annual notification of information concerning their rights;[30] and
- The right to consent prior to the disclosure of non-directory and personally identifiable information in their child's education records.[31]

These rights, however, will not apply to many cloud services that do not involve "educational records."

When a student turns 18 years old or enters a post-secondary institution, these rights transfer from the parents to the student.[32] Educational agencies and institutions receiving federal funding must comply with each of these rights with respect to the information they provide to third parties.

Parents also have the right to inspect and review their child's educational records maintained by the school.[33] Schools are not required to provide copies of the records to parents unless it is impossible for parents or eligible students to review the records onsite. When copies are needed, schools may charge a fee for such copies.[34]

Parents who obtain access to educational records pursuant to FERPA and find information that they consider inaccurate, misleading, or a violation of privacy may initiate a request to amend those records.[35] If the educational agency or institution involved declines to make the requested amendments, then they must afford the students or parents an opportunity for

[26] 20 U.S.C. § 1232g(b)(2).
[27] 20 U.S.C. § 1232g(b)(1)(A).
[28] 20 U.S.C. § 1232g(a)(1).
[29] 20 U.S.C. § 1232g(a)(2).
[30] 20 U.S.C. § 1232g(e).
[31] 20 U.S.C. § 1232g(b).
[32] 34 C.F.R § 99.5. The educational institution may, however, disclose the student's educational records to his/her parents if the student is the parents' tax dependent. 20 U.S.C. § 1232g(b)(1)(H); 34 C.F.R. § 99.31(a)(8).
[33] 20 U.S.C. § 1232g(a)(1).
[34] 34 C.F.R. § 99.11.
[35] 20 U.S.C. § 1232g(a)(2).

a hearing to challenge the content of the records.[36] This hearing must be conducted within a reasonable time of the parent's request and on reasonable advance notice to the parents.[37] The decision of the agency or institution must be based solely on the evidence presented at the hearing.[38] If the records are not found to be inaccurate, misleading, or in violation of the student's rights, the parents have the right to place a statement in the records commenting on the contested information or stating why they disagree with the decision of the agency or institution.[39]

A school must annually notify parents of their rights under FERPA.[40] The notice must inform parents that they may inspect and review their children's education records, seek amendment of inaccurate or misleading information in their children's educational records, and consent to most disclosures of personally identifiable information from the educational records.[41] The annual notice must include a description of who is considered to be a school official and a definition of a legitimate educational interest.[42] Means of notification can include a local newspaper, calendars, student programs guide, rules handbook, or other means likely to inform parents.[43]

Finally, prior written consent is generally required before institutions can disclose non-directory, personally identifiable information.[44] This general restriction applies any time a school or district agency discloses non-directory, personally identifiable information outside of such school or agency. Disclosures to state departments of education or third party vendors are therefore prohibited unless they meet the requirements of one of the exceptions discussed below. It is important to note for purposes of this report that information which is disclosed only with a student ID number, rather than a student name, is still personally identifiable under FERPA and subject to this heightened protection. Only when an agency or institution removes all personally identifiable information and assigns the records non-personal identifiers are disclosures to outside parties permitted without prior consent.

3. Exceptions to the Right to Consent to Disclosure of Educational Records

FERPA's general rule requiring written parental consent for disclosure of non-directory information in educational records has several exceptions that are relevant for the cloud computing context. First, as discussed above, educational records may be released without consent if all personally identifiable information has been removed.[45] Additional exceptions include disclosures in connection with studies undertaken on behalf of the school when such research can be conducted confidentially and anonymously and disclosures in connection with

---

36 34 C.F.R. § 99.21.
37 34 C.F.R. § 99.22(a).
38 34 C.F.R. § 99.22(f).
39 34 C.F.R. § 99.21(b)(2).
40 20 U.S.C. § 1232g(e).
41 U.S. DEP'T OF EDUC., *FERPA for Parents*, http://www.ed.gov/policy/gen/guid/fpco/ferpa/parents.html (last visited Nov. 7, 2013).
42 *Id.*
43 *Id.*
44 20 U.S.C. § 1232g(b).
45 20 U.S.C. § 1232g(a)(5).

audits and evaluations of programs conducted by local, federal, or state officials and their authorized representatives.[46]

FERPA allows an educational agency or institution to disclose educational records without prior written consent to school officials within the agency or institution who have legitimate educational interests.[47] Under this exception, a third party, including a contractor, consultant, or volunteer, may be considered a school official if such party (i) "performs an institutional service or function for which the…institution would otherwise use employees;" (ii) "is under the direct control of the…institution with respect to the use and maintenance of education records;" and (iii) is subject to certain FERPA requirements governing the use and redisclosure of personally identifiable information from education records.[48] With respect to these limitations as to use and redisclosure of information, school districts may not disclose personally identifiable information from an education record unless (i) the recipient will not disclose such information without prior consent of the parent or eligible student, and (ii) the officers, employees, and agents of the recipient party only use the personally identifiable information for the purposes for which the disclosure was made.[49] However, a third party authorized by the institution may be included in the exception regardless of whether the school has specifically identified the party as a "school official" in its annual FERPA notice. For purposes of this report, this exception covers instances when a third party accesses educational records at the direction of school officials for regular academic functions, provided the third party and the educational agency have a contract authorizing such access. However, school district contracts must impose the above requirements on third party vendors receiving personally identifiable information.

Another exception to the written consent requirement arises for educational agencies or institutions that disclose personally identifiable, non-directory information to organizations conducting studies on behalf of the educational agency or institution. To be in compliance, these studies must be conducted in order to develop, validate, or administer predictive tests, administer student aid programs, or improve instruction.[50] The agency or institution may release information without prior written consent only if the study is conducted in a manner that does not permit personal identification of parents or students by anyone outside of the research organization and as long as the information is destroyed when no longer needed for the purposes for which the study was conducted.[51] Recipients of information under this exception may not redisclose personally identifiable information outside of the research organization.[52] Under this exception a school or school district may disclose educational records to a third party vendor that such school or district has contracted with for research purposes provided that the information disclosed to such vendors remains confidential and there is a schedule for deletion of such records following the completion of the stated purpose.

---

[46] 20 U.S.C. § 1232g(b)(1)-(5).
[47] 20 U.S.C. § 1232g(b)(1)(A); 34 C.F.R. § 99.31(a)(1).
[48] 34 C.F.R. § 99.31(a)(1)(i)(B).
[49] 34 C.F.R. § 99.33(a).
[50] 20 U.S.C. § 1232g(b)(1)(F); 34 C.F.R. § 99.31(a)(6).
[51] *Id*.; 20 U.S.C. § 1232g(b)(1)(F).
[52] *Id.*

B. PPRA

The Protection of Pupil Rights Amendment, also known as the Hatch Amendment, applies to state or local education agencies that receive funding from the United States Department of Education. It aims to protect the rights of students and parents by creating conditions to funding for these agencies.[53] Specifically, it ensures the rights of students and parents surrounding the collection and use of information for marketing purposes as well as information regarding certain physical exams.[54]

1. Rights Afforded Under the PPRA

First, all material used in connection with any required survey, analysis, or evaluation of students that is funded in whole or in part by the US Department of Education, including instructional materials, must be made available for parents to inspect prior to use with their child.[55] Second, schools and contractors must acquire parental consent before a minor student is required to participate in any surveys, analyses or evaluations funded by the Department of Education that may reveal information regarding any of the following eight protected categories:

- Political affiliations or beliefs of the student or his or her parents;
- Mental or psychological problems of the student or the student's family;
- Sex behavior or attitudes;
- Illegal, anti-social, self-incriminating, or demeaning behavior;
- Critical appraisals of other individuals with whom respondents have close familial relationships;
- Legally recognized privileged or analogous relationships;
- Religious practices or beliefs; or
- Income other than as required by law to determine eligibility for programs or financial assistance.[56]

In addition, the PPRA empowers a parent the opportunity to opt a student out of (1) surveys involving protected personal information; (2) non-emergency, invasive physical exams; or (3) activities involving the collection, disclosure, or use of personal information obtained from students for marketing, sale, or for other distribution of the information to third parties.[57]

Local education agencies are required to notify parents of their rights under the PPRA annually at the beginning of the school year and within a reasonable time of any substantive change made to relevant district policies.[58] In addition, these agencies must notify through U.S. mail or e-mail the parents of students involved in the following specific activities or surveys and

---

[53] 20 U.S.C. § 1232h.

[54] U.S. DEP'T OF EDUC., *Model Notification of Rights under the Protection of Pupil Rights Amendment (PPRA),* http://www2.ed.gov/policy/gen/guid/fpco/pdf/ppranotice.pdf (last visited Nov. 7, 2013) [hereinafter PPRA Model Notification Letter].

[55] 20 U.S.C. § 1232h(a); PPRA Model Notification Letter.

[56] 20 U.S.C. § 1232h(b).

[57] 20 U.S.C. § 1232h(c)(2)(A)(ii); PPRA Model Notification Letter.

[58] 20 U.S.C. § 1232h(c)(2)(A)(i); U.S. DEP'T OF EDUC., *Letter to Local Superintendents* (March 2011), *available at* http://www2.ed.gov/policy/gen/guid/fpco/pdf/pprasuper.pdf [hereinafter PPRA Superintendents' Letter].

must provide an opportunity for parents to opt out their child from participation in these surveys or activities:

- The administration of any survey involving one of the above eight protected areas if it is not funded in whole or in part with funds from the U.S. Department of Education;
- Activities involving the collection, disclosure or use of personal information collected from students for marketing purposes, or to sell or otherwise provide the information to others for marketing purposes; and
- Any non-emergency, invasive physical examination or screening required as a condition of attendance, administered by the school and scheduled by the school in advance, or not necessary to protect the immediate health and safety of the student or of other students. This does not include physical examinations or screenings required or permitted by state law, including those permitted without parental notification.[59]

Rights of inspection, consent, and opt-out under the PPRA belong to parents and transfer to students upon reaching age 18 or at emancipation under relevant state law.[60] State agencies and local school districts are also required to develop policies in consultation with parents that address the collection, disclosure and use of personal information collected from students for sale or marketing purposes.[61]

C. COPPA

The Children's Online Privacy Protection Act of 1998 empowers the FTC to regulate the operators of commercial websites or online services targeted to children in the collection and use of personal information obtained from children.[62] COPPA defines "personal information" to include (1) a first and last name; (2) an address; (3) an e-mail address; (4) a telephone number; (5) a Social Security number; or (6) any other identifier that the FTC may determine permits the physical or online contacting of a specific individual.[63]

If a website is directed at children or the operator knowingly collects personal information from children under 13, COPPA requires that the website obtain parental notice and consent. Specifically, COPPA empowers the FTC to require that operators of websites who knowingly collect personal information from children do the following:

- Provide parental notice of their information practices;
- Obtain prior parental consent for collection, use, and/or disclosure of personal information from children;
- Empower parents, upon request, to review the personal information from their children;
- Provide a parent with the opportunity to prevent further use of personal information that has already been collected or the future collection of personal information from that child;

[59] PPRA Superintendents' Letter.
[60] 20 U.S.C. § 1232h(c)(5)(B).
[61] 20 U.S.C. § 1232h(c)(1)(E).
[62] 15 U.S.C. §§ 6501-6506.
[63] 15 U.S.C. § 6501(8).

- Limit the collection of personal information from a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and
- Establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information.[64]

In response to this legislation, the FTC passed the Children's Online Privacy Protection Rule ("Rule")[65] to protect children under age 13, and to apply to operators of a website or mobile application directed to children as well as to operators of a website or online service directed at general audiences that have actual knowledge that they collect personal information from children.[66] It requires that a website operator: (1) provide notice on the website service that it collects information from children, what information it collects, and how much it uses this information;[67] (2) obtain verifiable parental consent prior to any collection, use, or disclosure of personal information from children; (3) provide reasonable means for a parent to preview information collected from a child and to refuse its use or maintenance;[68] (4) not condition participation in a game, the offering of a prize or another activity on a child's disclosure of personal information than reasonably necessary to participate in the activity;[69] and (5) establish and maintain reasonable measures to protect the confidentiality, security, and integrity of personal information.[70] In effect, the Rule codifies and clarifies the notice and consent requirements set forth by COPPA.

In addition, the rule sets forth a "totality of factors" test for determining whether a commercial website or other online service is targeted to children.[71] This test requires the FTC to consider:

> the subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The commission will also consider competent and reliable empirical evidence regarding audience composition; evidence regarding the intended audience; and whether a site uses animated characters and/or child-oriented activities.[72]

---

[64] 15 U.S.C. § 6502(b)(1).
[65] 16 C.F.R. § 312.2 (2013).
[66] 16 C.F.R. § 312.3 (2013); BUREAU OF CONSUMER PROT. BUS. CTR., *Complying with COPPA: Frequently Asked Questions*, http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions (last visited Nov. 6, 2013).
[67] 16 C.F.R. § 312.4 (2013).
[68] 16 C.F.R. §§ 312.5-312.6 (2013).
[69] 16 C.F.R. § 312.7 (2013).
[70] 16 C.F.R. §§ 312.3 & 312.8 (2013).
[71] Children's Online Protection Privacy Rule, 77 Fed. Reg. 46643-01, 46646 (proposed Aug. 16, 2012) (codified at 16 C.F.R. § 312.2) (citing Letter from Susan L. Fox, Vice President, Gov't Relations, The Walt Disney Co., to the Federal Trade Comm'n, Office of the Sec'y (on file with Fordham CLIP), *available at* http://www.ftc.gov/os/comments/copparulereview2011/00368-82393.pdf).
[72] 16 C.F.R. § 312.2.

The FTC received numerous comments concerning the application of the Rule in the educational setting.[73] Some providers called for an exception to the parental consent requirement, stating that the school should be considered a consent-provider.[74] The Federal Trade Commission, however, in its recently updated guidance on COPPA notes that whether a school can provide consent in loco parentis "will depend on the nature of the relationship between the online service and the school or child, and the nature of the collection, use, or disclosure of the child's personal information."[75] Notwithstanding, it is important to note for purposes of this report that, if information is obtained directly from school districts, and not from a child under 13, COPPA and the Rule do not apply. Likewise, if information derives from a child's parent, then COPPA and the Rule are also inapplicable.

III. METHODOLOGY

In developing this study, Fordham CLIP's goal was to report on how public school districts address student privacy when using online services and to identify trends in compliance with student privacy obligations. In particular, Fordham CLIP sought to report on the content of cloud computing contracts, internal district policies, and the transparency of the outsourcing of student data to the parents of those children. For purposes of the study, Fordham CLIP defined cloud computing as any computing activity that collected or transferred student information for processing by third parties over the Internet.

To conduct the analysis, Fordham CLIP first selected a national sample of public school districts. These districts were then asked to provide a comprehensive set of documents including contracts, district policies and notices to parents. The documents were then systematically coded with respect to statutory requirements for student privacy and norms of fair information practice. The results were then analyzed to present an aggregate national picture of the treatment of children's personal information when schools use cloud computing services. The study did not seek to and does not report generally on the compliance of any individual school district with legal obligations. For citation purposes, this report thus uses code numbers in the analysis sections to reference specific districts' vendor agreements, policies and notifications. Where examples are used from specific districts, this report cites districts by their location in one of the four regional census zones used by the U.S. Census (northeast, south, midwest and west) rather than by the identity of the district. All referenced documents are on file with Fordham CLIP and are available on request for verification of the accuracy of this report.

A. Selection of Districts

To select a national sample of school districts, Fordham CLIP used the nine geographic divisions adopted by the U.S. Census.[76] Within each of these nine geographic areas, Fordham

---

[73] 64 Fed. Reg. 212 59899, 59903 (Nov. 3, 1999).
[74] *Id*.
[75] Fed. Trade Comm'n, COMPLYING WITH COPPA: FREQUENTLY ASKED QUESTIONS—A GUIDE FOR BUSINESS AND PARENTS AND SMALL ENTITIY COMPLIANCE, at FAQ M (July 2013), *available at* http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools (last visited Dec. 10, 2013).
[76] *See* U.S. Census Bur., Regions and Divisions, www.census.gov/geo/www/us_regdiv.pdf. The four US census regions and nine divisions are as follows:

CLIP selected six school districts. These districts were chosen from lists of regular districts that were generated by searches based on enrollment size of the Common Core of Data database maintained by the National Center on Education Statistics of the U.S. Department of Education.[77] For each geographic area, the two largest districts based on enrollment were included,[78] two mid-size districts with enrollments between 1,000 and 20,000 students were included,[79] and two small districts with enrollments fewer than 1,000 were included.[80] Districts from six states, however, were excluded because the open public record laws in those states deny non-residents the right of access to district documents.[81] Among the six selected districts in each geographical area, Fordham CLIP sought to avoid more than one district from the same state and sought to include districts distributed across each of the demographic classifications used by the U.S. Department of Education (i.e. urban, suburban, and rural districts). [82]
The following table shows the fifty-four districts selected for the data set representing a cross-section of the size and type of school systems across the United States:

TABLE OF SELECTED DISTRICTS

District Name	City	State	Locale	Size (Students)
Allendale School District	Allendale	NJ	Suburb: Large	Small (952)
Bamberg 2 School District	Denmark	SC	Rural: Fringe	Small (878)
Blackfoot School District 55	Blackfoot	ID	Town: Distant	Medium (4,445)
Boston Public Schools	Boston	MA	City: Large	Large (56,037)

---

1) Northeast region: New England division (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont); Middle Atlantic division (New Jersey, New York, Pennsylvania);
2) South region: South Atlantic division (Delaware, District of Columbia, Florida, Georgia, Maryland, North Carolina, South Carolina, Virginia, West Virginia); East South Central division (Alabama, Kentucky, Mississippi, Tennessee); West South Central division (Arkansas, Louisiana, Oklahoma, Texas);
3) Midwest region: East North Central division (Illinois, Indiana, Michigan, Ohio, Wisconsin); West North Central division (Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota); and
4) West region: Mountain division (Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, Wyoming); Pacific division (Alaska, California, Hawaii, Oregon, Washington).

[77] U.S. Department of Education, Nat'l Ctr. for Ed. Statistics, Common Core of Data, Search for Public School Districts, http://nces.ed.gov/ccd/districtsearch/ [hereinafter "CCD database"]. The search filters were "regular" district and "number of students." Several searches of the CCD database "Search for Public School Districts" feature (*available at* http://nces.ed.gov/ccd/districtsearch/) demonstrated major break points in student enrollment figures. Based on these points, Fordham CLIP designated districts as either Large, Medium, or Small as follows:

Large:	Districts with more than 20,000 students
Medium:	Districts with between 1,000 and 20,000 students
Small:	Districts with fewer than 1,000 students

[78] These districts were identified by searching the CCD database for districts with enrollment greater than 100,000 students.
[79] The CCD database included 6,660 regular school districts with enrollments between 1,000 and 20,000 students.
[80] The CCD database included 5,834 regular school districts with enrollments fewer than 1,000 students.
[81] These six states are: Alabama, Arkansas, Delaware, Georgia, Tennessee, and New Hampshire.
[82] *See* NAEP – The NAEP Glossary of Terms, http://nces.ed.gov/nationsreportcard/glossary.aspx# ("NAEP results are reported for four mutually exclusive categories of school location: city, suburb, town, and rural. The categories are based on standard definitions established by the Federal Office of Management and Budget using population and geographic information from the U.S. Census Bureau. Schools are assigned to these categories in the NCES Common Core of Data based on their physical address.") (last visited Sept. 20, 2013); *see also* Common Core of Data (CCD) – Identification of Rural Locales, http://nces.ed.gov/ccd/rural_locales.asp#defs (last visited Sept. 20, 2013).

Bowling Green Independent School District	Bowling Green	KY	City: Small	Medium (3,877)
Burlington School District	Burlington	VT	City: Small	Medium (3,632)
City of Chicago School District 299	Chicago	IL	City: Large	Large (405,644)
Clark County School District	Las Vegas	NV	Suburb: Large	Large (314,059)
Cowan Community Schools	Muncie	IN	Rural: Fringe	Small (761)
Dawson Springs Independent School District	Dawson Springs	KY	Town: Remote	Small (717)
Desoto County School District	Hernando	MS	Rural: Fringe	Large (31,916)
Dora Consolidated Schools	Dora	NM	Rural: Remote	Small (283)
Drew School District[83]	Drew	MS	Rural: Distant	Small (548)
Echo School District	Echo	OR	Town: Distant	Small (264)
Gilmer County Schools	Glenville	WV	Rural: Remote	Small (943)
Hawaii Department of Education	Honolulu	HI	Suburb: Large	Large (179,601)
Holmes County School District	Bonifay	FL	Rural: Distant	Medium (3,374)
Houston Independent School District	Houston	TX	City: Large	Large (204,245)
Island Park Union Free School District	Island Park	NY	Suburb: Large	Small (688)
Jefferson City Public Schools	Jefferson City	MO	City: Small	Medium (8,891)
Jefferson County Public Schools	Louisville	KY	City: Large	Large (97,331)
Jefferson County School District No. R-1	Golden	CO	Suburb: Large	Large (85,979)
Jefferson Parish Public School System	Harvey	LA	Suburb: Large	Large (45,230)
Jesup Community School District	Jesup	IA	Rural: Distant	Small (877)
London City Schools	London	OH	Town: Distant	Medium (2,059)
Los Angeles Unified School District	Los Angeles	CA	City: Large	Large (667,273)
Madison County School District	Flora	MS	Rural: Fringe	Medium (11,811)
Maricopa Unified School District #20	Maricopa	AZ	Rural: Distant	Medium (5,966)
Mercer Island School District	Mercer Island	WA	Suburb: Large	Medium (4,223)
Miami-Dade County Public Schools	Miami	FL	Suburb: Large	Large (347,366)
Millburn Township Public Schools	Millburn	NJ	Suburb: Large	Medium (4,937)
Milwaukee School District	Milwaukee	WI	City: Large	Large (80,934)
Muskogee Public Schools	Muskogee	OK	Town: Distant	Medium (6,417)
New Prague Area Schools	New Prague	MN	Town: Distant	Medium (3,823)
New Town School District	New Town	ND	Rural: Remote	Small (767)
New York City Department of Education	New York	NY	City: Large	†
North Stonington Public Schools	Stonington	CT	Rural: Fringe	Small (796)
Omaha Public Schools	Omaha	NE	City: Large	Large (49,405)
Orleans Parish Schools	New Orleans	LA	City: Large	Medium (10,493)
Pennsbury School District	Fallsington	PA	Suburb: Large	Medium (10,850)
Peoria Public Schools District 150	Peoria	IL	City: Midsize	Medium (14,254)

[83] As of July 1, 2012, this district is consolidated with the Sunflower County School District.
† The data are not applicable. *See Search for Public School Districts – Search Results*, http://nces.ed.gov/ccd/districtsearch/district_list.asp?Search=1&details=1&InstName=new+york+city+&DistrictID=&Address=52+chambers&City=&State=&Zip=&Miles=&County=&PhoneAreaCode=&Phone=&DistrictType=1&DistrictType=2&DistrictType=3&DistrictType=4&DistrictType=5&DistrictType=6&DistrictType=7&NumOfStudents=&NumOfStudentsRange=more&NumOfSchools=&NumOfSchoolsRange=more ("[†] indicates that the data are not applicable. For example, the enrollment and staff characteristics for districts that opened in the 2011-2012 school year will not be available until the full 2011-2012 file is released.").

Petersburg City School District	Petersburg	AK	Town: Remote	Small (490)
Portland Public Schools	Portland	ME	City: Small	Medium (6,970)
Providence Public School District	Providence	RI	City: Mid-Size	Large (23,573)
Queen Anne's County Public Schools	Centreville	MD	Town: Fringe	Medium (7,781)
Refugio Independent School District	Refugio	TX	Town: Distant	Small (732)
Rivendell Interstate School District	Orford	NH	Rural: Remote	Small (514)
San Luis Coastal Unified School District	San Luis Obispo	CA	City: Small	Medium (7,234)
St. Ignace Area Schools	Saint Ignace	MI	Town: Remote	Small (623)
Sublette County School District #9	Big Piney	WY	Rural: Remote	Small (672)
The School District of Philadelphia	Philadelphia	PA	City: Large	Large (166,233)
Velma-Alma Schools	Velma	OK	Rural: Remote	Small (451)
Wake County Public School System	Raleigh	NC	City: Large	Large (144,173)
Wichita Public Schools	Wichita	KA	City: Large	Large (49,329)

B. Collection of District Data

Following the selection of districts for the national sample, the Fordham CLIP team made initial telephone calls to district central offices using the contact information provided by the school districts to the National Center for Education Statistics. These calls sought to obtain the following documents on a voluntary, cooperative basis:

- All contracts or user agreements the district might have for free or paid computing services with outside service providers/vendors involving data about students (e.g. hosting services for school work or projects, student information systems, student demographic databases, web services, course/grade management services, document management services, email services for students, teachers, and administrators).
- All district computer use policies with respect to staff and teachers' use of free or paid third-party services that might host or process student information.
- All notices circulated by the district to parents about student data privacy.
- All notices circulated by the district to parents about the use of free or paid third-party computing services that receive student data.

Generally, the Fordham CLIP team encountered significant difficulty reaching any district personnel who were familiar with the district's outsourcing practices and those who were familiar with the district's contracts typically asked for a formal document request.

As a result, and to be consistent across all the districts, Professor Reidenberg sent formal open records act requests to each of the fifty-four districts. A sample copy of the request letter is attached as Appendix A. All of the documents that Fordham CLIP requested qualified as "public records" under the state statutes and, consequently, each district was required by its state law to provide the requested documents in the district's possession.

In addition to the public record requests, Fordham CLIP reviewed the websites of each of the fifty-four districts for any publicly available documents. This search was performed in order to confirm to the extent possible the completeness of the document production by the districts and to review the transparency of data practices.

C. District Responses

Of the fifty-four selected districts, twenty-three responded to the open public records requests by August 15, 2013, the Fordham CLIP data collection cut-off date and a date beyond the statutory response period imposed by the state public records laws. Nineteen of these responding districts submitted documents and each represented that their submissions were complete.[84] Four of the responding districts represented that they did not have any data outsourcing contracts and that all data processing was handled internally by the school district.[85] Fordham CLIP's web sweep revealed, however, that three of these four districts used external computing services through which student data was likely to be transferred to third parties.[86] These erroneously responding districts may not have understood or may have been unaware of their outsourcing arrangements. Because of this discrepancy and the lack of documents for these apparent outsourcing arrangements, these three districts were excluded from the comprehensive analysis.

The remaining thirty-one districts either failed to respond at all in violation of state law, requested time extensions beyond the data collection cut-off date, or provided documents after the statutory period had expired and beyond the study's data collection cut-off date.

For the comprehensive analysis, the data set therefore consisted of materials from the following twenty districts:

---

[84] These districts were: Echo School District, Holmes County School District, Jefferson City Public Schools, Jefferson County Public Schools (CO), Jefferson County Public Schools (KY), London City Schools, Maricopa Unified School District #20, Mercer Island School District, Millburn Township Public Schools, Omaha Public Schools, Pennsbury School District, Peoria Public Schools District 150, Portland Public Schools, Providence Public School District, Queen Anne's County Public Schools, Refugio Independent School District, San Luis Coastal Unified School District, Sublette County School District #9, and the Wake County Public School System.

[85] These districts were: Burlington School District, Drew School District/Sunflower County School District, Houston Independent School District, and Stonington Public Schools.

[86] The Burlington School District appears to use third-party Gmail services, the mybucks.com service for the cafeteria, and an outsourced assessment tool. *See* BURLINGTON SCH. DIST., http://burlington-school-food-proj.district.bsd.schoolfusion.us (containing link to mybucks.com) (last visited Nov. 20, 2013); BURLINGTON SCH. DIST., http://www.bsdvt.org/ (containing link to "BSD gmail," link to "vcat" for "BSD Comprehensive Assessment Tool") (last visited Nov. 20, 2013). The Drew School District, now consolidated with the Sunflower County School District, appears to outsource district email, and the district's website has links to the following outside services: EZ Test Tracker, MOTE Data Entry, Mississippi Student Information System (MSIS), and SAM7 Student Administration Manager. *See* DREW SCH. DIST., http://www.drew.k12.ms.us/HTML/links.htm (visited May, 2013) (page not accessible as of Oct. 24, 2013). The Stonington Public Schools appear to have a portal to third party services offered through PowerSchool and Google. *See* STONINGTON PUB. SCHS., http://www.stoningtonschools.org/page.cfm?p=2477 (containing student registration links for PowerSchool) (last visited Nov. 20, 2013); STONINGTON PUB. SCHS., http://www.stoningtonschools.org/page.cfm?p=2480 (containing link to student log-in for Google Apps for Education) (last visited Nov. 20, 2013). Each of these districts reported that it had no agreements responsive to our document request.

TABLE OF RESPONDING AND ANALYZED DISTRICTS

District Name	State	Census Region	Locale	Size (Students)
Echo School District	OR	Pacific	Town: Distant	Small (264)
Holmes County School District	FL	South Atlantic	Rural: Distant	Medium (3,374)
Houston Independent School District	TX	West South Central	City: Large	Large (204,245)
Jefferson City Public Schools	MO	West North Central	City: Small	Medium (8,891)
Jefferson County Public Schools	KY	East South Central	City: Large	Large (97,331)
Jefferson County School District No. R-1	CO	Mountain	Suburb: Large	Large (85,979)
London City Schools	OH	East North Central	Town: Distant	Medium (2,059)
Maricopa Unified School District #20	AZ	Mountain	Rural: Distant	Medium (5,966)
Mercer Island School District	WA	Pacific	Suburb: Large	Medium (4,223)
Millburn Township Public Schools	NJ	Mid Atlantic	Suburb: Large	Medium (4,937)
Omaha Public Schools	NE	West North Central	City: Large	Large (49,405)
Pennsbury School District	PA	Mid Atlantic	Suburb: Large	Medium (10,850)
Peoria Public Schools District 150	IL	East North Central	City: Mid-size	Medium (14,254)
Portland Public Schools	ME	New England	City: Small	Medium (6,970)
Providence Public School District	RI	New England	City: Mid-size	Large (23,573)
Queen Anne's County Public Schools	MD	South Atlantic	Town: Fringe	Medium (7,781)
Refugio Independent School District	TX	West South Central	Town: Distant	Small (732)
San Luis Coastal Unified School District	CA	Pacific	City: Small	Medium (7,234)
Sublette County School District #9	WY	Mountain	Rural: Remote	Small (672)
Wake County Public School System	NC	South Atlantic	City: Large	Large (144,173)

In addition to the comprehensive analysis, Fordham CLIP considered the material provided by these twenty districts, as well as the three districts that responded inaccurately, for general observations. The sweep also provided anecdotal information for two of the large non-responding districts: the New York City Department of Education and the Los Angeles Unified School District. This anecdotal information is also referenced where relevant for general observations.

D. Analytic Approach

Fordham CLIP developed a checklist to identify comprehensively the privacy protections that districts provide when they transfer their children's online data to third parties. The checklist was designed to include the basic contractual protections that are mandated by the Family Educational Rights and Privacy Act,[87] the Protection of Pupil Rights Amendment,[88] and the Children's Online Privacy Protection Act.[89] In addition, the checklist included several norms of fair information practices such as data security that are not required by the relevant statutes, but are nonetheless vital protections and widely considered important for ensuring privacy. The checklist is, in effect, an inventory of the elements that should appear in the documents if privacy is being protected effectively by school districts when they share or enable the gathering of their students' data. The checklist is reproduced in Appendix B.

---

[87] 20 U.S.C. § 1232g; 34 C.F.R. Part 99.
[88] 20 U.S.C. § 1232h; 34 C.F.R. Part 98.
[89] 15 U.S.C. §§ 6501-6506.

The Fordham CLIP team coded each of the documents received from the responding districts according to the checklist. The aggregate coding results are attached in Appendix C.[90]

IV. FINDINGS

School districts across the country are widely sharing student information with third parties through cloud computing arrangements. Nineteen of the twenty districts (95%) reported outsourcing some type of school function involving student information.[91] The research demonstrated that these arrangements take a variety of forms and specific findings relate to the different types of arrangements. The first section of this Part thus maps out the different types of activities and functions that school districts rely on cloud services to perform. Next, this Part describes general observations and trends arising from the document requests. Finally, this Part presents detailed findings related to each type of cloud computing arrangement revealed by the research. All referenced documents from the school districts are on file with Fordham CLIP.

A. Diversity and Typology of Cloud Services in Public Schools

The school districts provided Fordham CLIP with many different types of agreements reflecting a broad range of school functions that involved the transfer of student data to third parties. Because the privacy issues will vary by context, Fordham CLIP determined that the diverse functions needed to be analyzed by type. Fordham CLIP grouped the agreements into seven categories. Each of these categories represents a set of functions that schools outsource to third parties and that involved the transfer of student data. These categories provide a snapshot of cloud computing in public schools across the United States as of August 15, 2013, and are as follows:

1. Data Analytics Functions

Data analytics services are those that aggregate and analyze student data. For example, one provider of data analytics services describes this function as the "systems that can deliver a complete performance picture, which reports and analyzes the results from all a district's important assessments, including but not limited to state high stakes and other state tests, national norm referenced tests, early literacy assessments, and any non-proprietary formative assessments."[92] Such data analysis systems provide a "big picture view"[93] that enable educators to "better measure performance against local, state, and federal standards; make informed, collaborative decisions for student, school, and district improvement; and target students, teachers, and schools in need of assistance."[94]

---

[90] In coding the documents, a "1" or "Yes" on the checklist means that the element is present. A "0" or "No," means that the element is not present or cannot be ascertained from the documentation that was provided by the district. In some cases, an element was not applicable to a particular document and was thus marked "N." In other cases, an element was unknown and was accordingly marked as "U."

[91] *See supra* Table of Responding Districts.

[92] *Pearson – Analyzing Student Data*, PEARSONSCHOOLSYSTEMS.COM, http://www.pearsonschoolsystems.com/solutions/dataanalysis/ (last visited Oct. 2, 2013).

[93] *Id*.

[94] *Id*.

2. Student Reporting Functions

Student reporting services provide metrics of individual student progress and attendance, as well as communicate with parents regarding such data. These functions are very similar to data analytics, but focus more on the individual student's reports than on a cohort.

3. Guidance Functions

Guidance function services are those tools used by school guidance departments to assist with and track student college planning and application processes.

4. Special School Functions

Special school functions are those non-instructional functions that are part of the management of a school district's activities. These functions include services such as the management of student transportation and payment mechanisms for student lunch programs. Traditionally, these services might have been performed in-house by school districts.

5. Hosting, Maintenance, and Backup Functions

Hosting, maintenance, and backup functions include website and data hosting, as well as maintenance contracts for hardware systems running proprietary software installed by cloud services companies.

6. Classroom Functions

Classroom functions provide students and teachers with online learning, collaboration, and individual assessment tools. Many of these classroom function agreements provided online services for students to complete classwork and homework, submit assignments, and work collaboratively with teachers and other students online.

7. Unidentifiable Functions

Unidentifiable functions are those contracts governing any cloud services whose purpose could not be determined from the text of the provided documents.

B. General Trends

Fordham CLIP observed a number of general trends in the treatment of student information from the research process and the data collected from the schools. As discussed below, public school districts have embraced the use of cloud services, but district practices were surprisingly opaque. School district documentation was also often poorly maintained and data governance procedures appear to be quite weak. Similarly, data governance and contracting practices have much room for improvement.

1. Broad Use of Cloud Services by Public Schools

Public school districts have embraced the use of cloud services for the education of students. As previously noted, 95% of reporting districts relied on at least one type of cloud service to process student information.[95] The following table shows the frequency of use for each type of service by the reporting districts.

Category of Service	Percentage of Reporting Districts
Data Analytics Functions	25%
Student Reporting Functions	25%
Guidance Functions	25%
Special School Functions	25%
Hosting, Maintenance, and Backup Functions	50%
Classroom Functions	50%
Unidentifiable Functions	55%

These different categories of cloud services are adopted in all regions of the country and by districts of all types and sizes. For data analytics services, large and small districts across the country outsourced student information, as shown by the table below of those districts reporting data analytics agreements:

District Name	State	Census Region	Locale	Size (Students)
Echo School District	OR	Pacific	Town: Distant	Small (264)
Jefferson County Public Schools	KY	East South Central	City: Large	Large (97,331)
Omaha Public Schools	NE	West North Central	City: Large	Large (49,405)
Providence Public School District	RI	New England	City: Mid-size	Large (23,573)
Sublette County School District #9	WY	Mountain	Rural: Remote	Small (672)

Similarly, the distribution of districts that outsource student reporting data include large, medium and small districts in multiple geographic regions of the country. This distribution is reflected in the following table showing those districts that outsource student reporting functions:

District Name	State	Census Region	Locale	Size (Students)
Jefferson County Public Schools	CO	Mountain	Suburb: Large	Large (85,979)
Mercer Island School District	WA	Pacific	Suburb: Large	Medium (4,223)
Omaha Public Schools	NE	West North Central	City: Large	Large (49,405)
Providence Public School District	RI	New England	City: Mid-size	Large (23,573)
Sublette County School District #9	WY	Mountain	Rural: Remote	Small (672)

[95] *See supra* Table of Responding Districts (all districts, except Houston Independent School District).

Responding districts that rely on cloud services for guidance functions tended to be the larger and medium size suburban districts, as shown in the following table:

District Name	State	Census Region	Locale	Size (Students)
Jefferson County Public Schools	CO	Mountain	Suburb: Large	Large (85,979)
Jefferson County Public Schools	KY	East South Central	City: Large	Large (97,331)
Mercer Island School District	WA	Pacific	Suburb: Large	Medium (4,223)
Millburn Township Public Schools	NJ	Mid Atlantic	Suburb: Large	Medium (4,937)
Queen Anne's County Public Schools	MD	South Atlantic	Town: Fringe	Medium (7,781)

With respect to special school functions, outsourcing appeared more commonly among medium size suburban districts. The following table shows the distribution of those districts with special school function agreements:

District Name	State	Census Region	Locale	Size (Students)
Jefferson City Public Schools	MO	West North Central	City: Small	Medium (8,891)
Maricopa Unified School District #20	AZ	Mountain	Rural: Distant	Medium (5,966)
Mercer Island School District	WA	Pacific	Suburb: Large	Medium (4,223)
Millburn Township Public Schools	NJ	Mid Atlantic	Suburb: Large	Medium (4,937)
Pennsbury School District	PA	Mid Atlantic	Suburb: Large	Medium (10,850)

Hosting, maintenance, and backup services appear more commonly adopted by medium size districts in all parts of the country. The following table shows the distribution of those districts reporting these types of arrangements for student information.

District Name	State	Census Region	Locale	Size (Students)
Jefferson City Public Schools	MO	West North Central	City: Small	Medium (8,891)
Jefferson County Public Schools	KY	East South Central	City: Large	Large (97,331)
London City Schools	OH	East North Central	Town: Distant	Medium (2,059)
Maricopa Unified School District #20	AZ	Mountain	Rural: Distant	Medium (5,966)
Mercer Island School District	WA	Pacific	Suburb: Large	Medium (4,223)
Millburn Township Public Schools	NJ	Mid Atlantic	Suburb: Large	Medium (4,937)
Omaha Public Schools	NE	West North Central	City: Large	Large (49,405)
Peoria Public Schools District 150	IL	East North Central	City: Mid-size	Medium (14,254)
Queen Anne's County Public Schools	MD	South Atlantic	Town: Fringe	Medium (7,781)
Sublette County School District #9	WY	Mountain	Rural: Remote	Small (672)

For classroom functions, the responding districts represent large and medium districts spread across the country and across locale types. The following table shows the distribution for the use of cloud services to perform classroom functions:

District Name	State	Census Region	Locale	Size (Students)
Jefferson City Public Schools	MO	West North Central	City: Small	Medium (8,891)
Jefferson County Public Schools	CO	Mountain	Suburb: Large	Large (85,979)
Jefferson County Public Schools	KY	East South Central	City: Large	Large (97,331)
London City Schools	OH	East North Central	Town: Distant	Medium (2,059)
Maricopa Unified School District #20	AZ	Mountain	Rural: Distant	Medium (5,966)
Mercer Island School District	WA	Pacific	Suburb: Large	Medium (4,223)
Millburn Township Public Schools	NJ	Mid Atlantic	Suburb: Large	Medium (4,937)
Omaha Public Schools	NE	West North Central	City: Large	Large (49,405)
Queen Anne's County Public Schools	MD	South Atlantic	Town: Fringe	Medium (7,781)
San Luis Coastal Unified School District	CA	Pacific	City: Small	Medium (7,234)

Ultimately, the reliance by public schools on third-party online services for processing student data means that the privacy protection for the student data is of critical importance.

2. Weak Transparency of Practices

The relevant federal privacy laws (FERPA, COPPA and PPRA) require that parents be informed of data practices.[96] As a general observation, Fordham CLIP found that the practices associated with the transfer of student data were opaque. The lack of transparency for the agreements themselves and for the kinds of student data at stake in the agreements makes effective public oversight of school districts' privacy practices extremely difficult—if not impossible.

As a starting point, thirty-one districts—more than half—did not respond satisfactorily to a public records request. Many failed to answer in violation of state laws, others delayed extensively, and some of the responding districts erroneously denied the existence of agreements. This suggests that many school districts are unwilling or unable to disclose how they use and protect student data.

District websites were of widely variable quality with respect to disclosures regarding the transfer of student data to cloud service providers. For example, the web sweeps enabled Fordham CLIP to document some use of third party computing services of the largest districts that had not provided any documents in response to the public records requests, including the Los Angeles Unified School District, the City of Chicago School District 299, and the New York City Department of Education. The sweeps, however, yielded insufficient data to include the districts in the comprehensive analysis. By way of illustration, the City of Chicago School District 299 website made available product FAQs and information sheets, but the actual agreements were missing or too well hidden for the sweep to locate. The New York City Department of Education made available its contract for data analytics through the Shared Learning Collaborative (known by its product name, inBloom) as well as various social media and Internet use policies. But, locating these documents required multiple searches through a myriad of web pages and required extensive research time. This indicates that parents, students,

[96] *See generally supra* Part II.

and other interested parties would likely have great difficulty obtaining information on school district practices.

Beyond the difficulty of obtaining documentation, district data often had significant gaps. In many instances, when documentation was provided, the Fordham CLIP team was unable to discern the precise terms of an agreement between a district and a vendor because key pieces of information regarding the district-vendor relationship were missing from the agreements or from other documentation. Similarly, of the ninety-three agreements received from responding districts, twenty-six—nearly a third—represented a service or function that was not identifiable from terms of the agreement.[97]

3. Obstacles to Public Disclosure

While state open public record laws require, and fair information practice principles insist, that public schools' data processing arrangements be transparent, some districts responded to Fordham CLIP's public records requests with clear hostility. For example, the superintendent of one district wrote:

> "I have real problem [sic] with you using this law to complete a research project you are doing. That is not what the law was intended for nor do we have the time [to] pull information and send it to you so you can do your job…. so thank you for your abuse of the system and wasting our time."[98]

Similarly, another district initially said it would charge an administrative fee of $1,100 to provide the requested documents.[99] And, a large enrollment school in the northeast region initially refused to release a major agreement because the contract contained a confidentiality

---

[97] *See supra* Part IV.A.7.

[98] Email from Superintendent in West Region School District to Professor Reidenberg, dated July 23, 2013. In response to the following answer from Professor Reidenberg, the district provided materials:

> "I must respectfully disagree with your objection to our use of the public records law. Our project is a national examination of the way privacy is addressed by public schools when data involving students is outsourced to the Internet. We selected 54 school districts across the country for our data set. They were chosen from each census region and were based on enrollment size (2 large, 2 medium and 2 small per census region). We began our study calling many of these school districts and were invariably told that we should make a formal request for the materials. For the research methodology to be consistent, we need to approach all school districts in the same fashion. The public records laws were adopted precisely for the purpose of providing transparency to government and providing access to government documents for public review. This is exactly the purpose of our work. Our last national study in the field, "A Study of Elementary and Secondary School State Reporting Systems" <http://law.fordham.edu/center-on-law-and-information-policy/14769.htm> resulted in congressional hearings that addressed privacy issues in state longitudinal databases and was referenced in testimony this past winter to [your state's Senate]. While we are not looking to report on any individual school district which might reflect the more frequent uses of the open records in your district, we are seeking to identify national trends and practices and to offer recommendations on privacy issues including those related to FERPA that we identify from the trends and practices. We believe this use falls squarely within the purposes of [your state's] public records act." Email dated July 24, 2013.

[99] Letter from Superintendent of South District to Professor Reidenberg, dated July 3, 2013 . Following discussions with the superintendent and another district administrator, the district provided the materials without charge once the senior staff better understood the project.

clause.[100] The confidentiality clause was clearly in violation of the state's open public records act.[101]

Aside from the cases where a district may have misunderstood the scope of the public record request, these reactions and the obstacles to the disclosure of public records that some districts created suggest that districts do not want the public to know about their practices surrounding their stewardship of student data.

4. Low Quality of Documentation

The proper documentation of online service contracts is essential for public school districts to be able to demonstrate compliance with FERPA. Many school districts, however, appear to use services for which they do not seem to have adequate contract documentation.[102] For example, a number of districts appear to use services provided by the same vendor,[103] yet only one district was able to produce a copy of the agreement with the vendor.[104] Another district provided unsigned documents for a different set of agreements suggesting that the originals were unavailable.[105] Without available signed documentation, districts invite confusion and misunderstanding of their legal obligations. While the vendors of some services may simply require a district to accept web-based terms and conditions, districts should maintain contemporaneous copies of those web-based terms. Districts also might have failed to account for some services when responding to Fordham CLIP's request for documents. Although this may be the result of inadvertent oversight, it may also suggest that districts do not fully comprehend the nature and scope of the services they use.

Beyond the missing and unsigned agreements, more than 25% of the documents provided by the school districts failed to adequately describe the services covered by the relevant agreement.[106] Some districts provided purchase orders rather than complete contracts and many of the agreements lacked any description of the services to be furnished or contained general terms that could be applied to any number of services. Without clearly-described services in the vendor agreements, districts will not be able to demonstrate that they comply with FERPA and

[100] Letter from Public Records Officer of Northeast District to Professor Reidenberg, dated July 9, 2013.
[101] *See* Appeal by Fordham CLIP from Denial of Public Record submitted to District Superintendent, dated July 10, 2013 (demonstrating that the exception from public disclosure contained in the state statute does not apply to this contract).
[102] Western Region School District website has an Infinite Campus login portal but provided no agreement with that vendor. *See Campus Parent Portal Login*, URL on file with Fordham CLIP, (last visited Oct. 22, 2013). Additionally, a Northeast district provided an Infinite Campus information letter to parents, URL on file with Fordham CLIP, but the district provided no documents suggesting that it uses this service. Another South district informed the Fordham CLIP team that there are several hosted applications that are used by students for instructional purposes for which the district has no supporting documentation, including: iReady; First in Math; Edoptions; Voyager Ticket to Ride; Voyager VMath Live; Envisions Math; Understanding Numerations; and Read Naturally.
[103] For example, seven districts appear to have agreements with Infinite Campus.
[104] A Midwest district provided an Infinite Campus End User License Agreement.
[105] For example, Agreement Document No. 26 was missing a signature page. *See generally* Agreement Document No. 26. Agreement Document No. 36 included an unsigned signature page. *See* Agreement Document No. 36 at 5. Similarly, Agreement Document No. 12 included a signature page that was signed by only the district and not the vendor. *See* Agreement Document No. 12.
[106] Of the ninety-three agreements we received from responding districts, twenty-six—nearly a third—represented a service or function that was not identifiable based on the language of the agreement. *See supra* Part IV.A.7 (describing agreements with unidentifiable functions).

COPPA obligations, and parents and other interested parties will not be able to determine how schools are sharing student information. The lack of adequate contractual descriptions may also indicate that senior district personnel are insufficiently informed or unaware of the nature of the student information that the district outsources to third parties.

In addition, many of the vendor agreements provided to Fordham CLIP incorporated by reference separate documents to supplement or supplant terms and conditions, privacy policies, or provisions. Often, however, the districts failed to provide those separate documents, possibly because such were not on hand or were not otherwise immediately available. In other cases, districts provided versions of documents that, according to date stamps, appeared to have been printed from the Internet subsequent to the receipt of Fordham CLIP's public records requests. One district created a spreadsheet listing all of the vendors with which it had agreements for the purpose of responding to the public records request, rather than provide actual copies of the agreements.[107] Additionally, some districts provided agreements or policies that appeared to apply only to a vendor's website; it was not clear from these documents whether the terms also governed the actual service provided to the district.[108] Based on these examples, it seems unlikely that districts keep adequate records with original file copies of their vendor agreements; these examples also suggest that districts may not even have full sets of terms and conditions when committing to a specific contract.

The poor documentation and the probable lack of district access to some terms is of significant consequence. In such circumstances, districts would have neither a way of knowing or demonstrating the contract version applicable to the student data, nor a way to determine if a vendor altered its terms without notice to the district.

5. Weak Data Governance and Contracting Practices

Fordham CLIP's research revealed a number of data governance and contracting practices that suggest school districts are ill-equipped to adequately address privacy concerns when they outsource to vendors school functions that implicate student information. As an initial observation, many districts did not seem to understand the nature of the services that they outsourced to third party providers. This was reflected in both the difficulty Fordham CLIP encountered in identifying school district personnel who were aware of the district's technology outsourcing arrangements as well as in the difficulty some districts seemed to have in responding to the request for documents.

As a governance matter, approximately 20% of the responding districts had no policies addressing teacher use of information resources.[109] The central administration of these districts would, as a result, have neither knowledge nor oversight of classroom or school use of third-party services involving the transfer of student information. For example, if a school principal or teacher decided to use a service such as Dropbox for students to share family photos, the central administration would not have the opportunity to vet the terms and conditions of the service and would not have the ability to ensure COPPA compliance.

Many contracting practices reflected that districts were rarely in control of the terms and conditions of data transfers. Vendors typically presented the school districts with standard form

[107] *See* Midwest District Excel Spreadsheet.
[108] *See, e.g.*, Midwest District submission of links to terms of use and privacy policies that were to be printed directly from various vendors' websites and which were stated to govern use of the vendors' websites generally .
[109] *See infra* Part IV.D (discussing district policies regarding staff use of computer services).

contracts that would often contain misleading or inappropriate provisions. For example, vendors sometimes include a term specifying that the vendor would not cause the district to fall out of compliance with FERPA.[110] Because FERPA obligations attach to the school district—and because the vendor may not even be aware of those obligations with respect to the transferred data—such a clause inappropriately gives the district the impression that FERPA requirements are satisfied. In effect, this type of clause seems to reflect a fundamental misunderstanding of the applicable federal statutes on the part of the vendor and of the contracting district.

Additionally, vendors sometimes include clauses allowing the vendor to share data with affiliates without committing those affiliates to any privacy protections. Another contracting practice also illustrated that districts appeared to lack adequate control over the conditions of transfers of student data: vendor agreements would often grant the vendor the right to modify the terms and conditions at the vendor's discretion—and often without direct notice to end users and district-based system administrators.[111] In other words, districts legally relinquished the ability to comply with FERPA, since the vendor can unilaterally amend or alter the terms of service to enable the vendor to use student data for purposes other than those stipulated in the original agreement with the district.

Finally, in some instances, school districts outsourced their statutory compliance functions to state departments of education. In these cases, state departments of education contracted with vendors to provide services to school districts within the state. Sometimes, state departments of education required that districts use the department-acquired services; other times use was optional. When the state contracts with the vendor, the school district may not be able to retain control to assure that data is used only for permissible purposes. For example, the New York City Department of Education participates in the inBloom data analytics project but does not have a contract with inBloom. Rather, the vendor's agreement is with New York State and designates a state official—not a New York City Department of Education official—as the "super administrator" who determines both the purposes for processing the district's student data and who can gain access to that data.[112] FERPA, however, only allows the New York City Department of Education to transfer the data to a vendor for functions the school would otherwise perform (such as analytics) when the district has "direct control" over the recipient vendor.[113] The district's arrangement is not consistent with this requirement. By contrast, in Colorado, the arrangement for inBloom with Jefferson County Public Schools designates a district official as the super administrator and ensures that the district retain control over its data.

These governance and contracting practices indicate that school districts are not well-equipped to deal with the privacy implications of their use of cloud computing. School districts seem to lack personnel who fully understand the cloud arrangements and who have the privacy expertise to address both compliance and fairness issues. Similarly, districts generally did not appear to negotiate the terms of cloud agreements and, even if they sought to modify terms, it is unclear whether vendors would have permitted deviations from their standard boilerplate contracts.

---

[110] For example, one agreement provided that the vendor will not cause the customer to be out of compliance with FERPA. *See* Agreement Document No. 6 at 1.
[111] *See infra* Parts IV.C.1.d, IV.C.2.d, IV.C.3.d, IV.C.4.d, IV.C.5.d, and IV.C.6.d.
[112] *See* Service Agreement between Shared Learning Collaborative, LLC and New York State Education Department, dated Oct. 11, 2012, Exhibit G (*available at* http://usny.nysed.gov/rttt/docs/slc-service-agreement.pdf) (designating a state official) (last visited Nov. 29, 2013).
[113] 34 C.F.R. § 99.31(a)(1)(i)(B)(2).

C. Analysis of District Agreements by Type of Cloud Computing Service

Fordham CLIP examined in detail each of the responding districts' agreements according to the type of cloud computing service under contract. The agreements were categorized solely on the basis of the service descriptions found in the contracts. This Section provides the results of that analysis for each of the seven functional categories: 1) data analytic functions; 2) student reporting system functions; 3) guidance functions; 4) hosting, maintenance, and backup functions; 5) special school functions; 6) classroom functions; and 7) the agreements representing unidentifiable functions. The discussions for each of the categories report on the prevalence of contracts for the category and the content of the agreements with respect to the key elements identified in the document coding checklist. The discussion does not address practices that vendors and districts may have outside the actual terms of the agreements.

1. Data Analytics Functions

a. Prevalence

Of the twenty responding districts, only six (30%) produced documents representing agreements with third party service providers to perform data analytics.[114] These six districts provided a combined total of nine data analytics service agreements from a variety of service providers.[115] The limited use of cloud services for data analytic purposes was somewhat surprising in light of the policy emphasis placed on learning assessments. This may reflect several possible trends that would not be revealed from our data set. For example, school districts may not have yet considered any analytic options. Others may have considered, but were unsure of the value to the district of various analytic offerings. Or, districts may have rejected outsourcing student data for analytic purposes. Another possibility is that agreements to perform data analytics functions were in fact provided by responding districts, but such agreements did not make clear that they were for data analytics services and were thus categorized as having an unidentifiable function.[116] Lastly, some districts may not have understood their information technology infrastructure and simply failed to account for all of the third party services they use in responding to the documents request.

b. Contracts

FERPA regulations require that all districts have written agreements in place prior to the disclosure of data from student educational records to vendors for "audit and evaluation" purposes[117] or that they have "direct control" when releasing student information to vendors

[114] The six districts are: Echo School District, Jefferson County Public Schools (CO), Jefferson County Public Schools (KY), Omaha Public Schools, Providence Public School District, and Sublette County School District #9.
[115] While some districts employed more than one vendor for data analytics services, no one vendor has an agreement with more than one school district. The nine service providers are on file with Fordham CLIP.
[116] *See supra* Part IV.A.7.
[117] 34 C.F.R. § 99.35(a)(3).

under the "school official" exception.[118] All the responding districts had fully executed agreements with the vendors. However, 22% of the agreements were missing elements.[119]

As a compliance safeguard, only thirty-three percent (33%) of the agreements gave districts the right to audit and inspect the vendor's practices with respect to the transferred data.[120] This means that the overwhelming majority of school districts do not reserve the legal authority to verify that vendors are treating student data in accordance with their agreements.

c. Types of Student Identifying Data Transferred from Districts to Vendors

The use of information that identifies students is central to establish any privacy compliance obligations. FERPA regulations require that districts releasing student information to authorized representatives, such as analytic service providers, specify the personal information that is transferred.[121] However, agreements for data analytics services infrequently specified the types of identifying data that districts transfer to vendors. In fact, three of the nine agreements (33%) did not specify whether any identifying data was transferred at all.[122] The other six agreements specified the transfer of only some types of data. The contract specifications by type of identifying information are illustrated in the following table:

TYPE OF DATA TRANSFERRED		
Type of Data Specified	**Total (out of 9)**	**Percentage**
Name	1	11.1%
Address	2	22.2%
Sex	3	33.3%
ID	2	22.2%
Age/Grade	4	44.4%
Biometric	1	11.1%
Medical/Health	2	22.2%
Socio-Economic	2	22.2%
Transaction Data	2	22.2%

The most notable observation from this data is that only one type of student information—age/grade—was frequently specified as being transferred; almost all other types of student identifying data were specified as being transferred with only low or moderate frequency. Since the services performed under these contracts are designed to provide detailed analysis of student performance, it appears very likely that, at best, the agreements provided incomplete descriptions of the student's identifying data. If this is the case, such vagueness is a problematic contracting practice. The failure to include a complete description of all identifying data that is being transferred means the contract is silent on the key element triggering FERPA obligations,

[118] 34 C.F.R. § 99.31(a)(1)(i)(B)(2). *See also* Part II.A.3.
[119] Agreement Document No. 1 was missing the user manuals incorporated by reference in the agreement. *See* Agreement Document No. 1 at 3. Similarly, Agreement Document No. 4 was missing a page. *See generally* Agreement Document No. 4.
[120] *See, e.g.*, Agreement Document No. 3. Agreement Document No. 9 specifies that the school district retains complete control over its data, which could be construed as providing a right of audit or inspection. *See* Agreement Document No. 9 at 7.
[121] *See* 34 C.F.R. § 99.35(a)(3)(A).
[122] *See* Agreement Document No. 1; Agreement Document No. 5; Agreement Document No. 9.

as FERPA obligations attach to personally identifiable information drawn from educational records.[123]

d. Data Control: Sharing, Mining, and Redisclosure

Data sharing, mining and redisclosure of student information without parental consent is restricted under FERPA for specific purposes including "audit and evaluation" of district programs.[124] FERPA requires that districts specify the audit and evaluation purpose in a written agreement for disclosures related to that permissible purpose[125] and requires that districts retain control of the data in the event the transfer to the vendor qualifies as a disclosure to a "school official."[126] Parental consent is, nonetheless, required by the PPRA for "analysis or evaluation" of student information in the context of data that reveals certain types of characteristics (such as behavior tendencies that might be profiled for guidance purposes).[127] Districts' control over their student's transferred information is, thus, particularly important to assure that transferred data will only be used in accordance with permissible purposes. The following table shows the frequency that data analytic contracts contained clauses addressing these key data control issues.

[123] *See* 34 C.F.R. § 99.3 (Authority: 20 U.S.C. § 1232g) (defining "Personally Identifiable Information" as "includ[ing], but [ ] not limited to—(a) The [s]tudent's name; (b) The name of the student's parent or other family members; (c) The address of the student or the student's family; (d) A personal identifier, such as the student's social security number, student number, or biometric record; (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) Other information that, alone or in combination, 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; or (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates." *See also supra* Part II.A (discussion of FERPA).

[124] *See* 20 U.S.C. § 1232g(b)(1) (describing the requirement that parental consent be obtained before a district may disclose personally identifiable student information); 20 U.S.C. § 1232g(b)(3) (specifying that data may be shared without parental consent for audit and evaluation of school programs). *See also* 20 U.S.C. § 1232g(b)(1)(F) (specifying an exception for studies, which Fordham CLIP also analyzed under this exception when coding documents).

[125] 35 C.F.R. § 99.35(a)(3)(B).

[126] 35 C.F.R. § 99.31(a)(1)(i)(B)(2).

[127] The Protection of Pupil Rights Amendment ("PPRA") (20 U.S.C. § 1232h; 34 CFR Part 98) "applies to programs that receive funding from the U.S. Department of Education (ED) [and] is intended to protect the rights of parents and students in two ways: [By] seek[ing] to ensure that schools and contractors make instructional materials available for inspection by parents if those materials will be used in connection with an ED-funded survey, analysis, or evaluation in which their children participate; and [by] seek[ing] to ensure that schools and contractors obtain written parental consent before minor students are required to participate in any ED-funded survey, analysis, or evaluation that reveals [certain privileged or private information]." *See Protection of Pupil Rights Amendment (PPRA)*, Feb. 17 2005, http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html. *See* 20 U.S.C. § 1232h(c)(1)(E) (requiring that "a local educational agency that receives funds under any applicable program shall develop and adopt policies, in consultation with parents, regarding the following: [t]he collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose), including arrangements to protect student privacy that are provided by the agency in the event of such collection, disclosure, or use.").

DATA CONTROL: LIMITS ON SHARING, MINING, REDISCLOSURE		
	Total (out of 9)	**Percentage**
Document Prohibits or Limits Redisclosure	8	88.8%
District Retains Exclusive Control of Data	2	22.2%
District Retains Audit and Inspection Rights Respecting Vendor	3	33.3%
District Retains Right to Determine Data Access Based on User Role	1	11.1%
Document Specifies Audit/Evaluation Purpose for Disclosure	2	22.2%
Data Used for: Sale/Marketing of Instructional Materials, Student Recognition, College, Military, or Low-Cost Literary Materials	0	0.0%
Disclosure Allowed for Heath, Safety, or Emergency Purpose	0	0.0%
Document Prohibits Sale and Marketing of Data	0	0.0%
Foreign Storage Prohibited	0	0.0%
Access by Other Government Agencies Prohibited	0	0.0%

As a threshold observation, only two (22%) of the agreements contained a clause indicating that data was transferred for an audit or evaluation purpose.[128] Only two of the agreements (22%) stipulated that the district retains exclusive control of transferred data,[129] and only one of the agreements (11%) provided for districts to set user access controls.[130] While eighty-nine percent (89%) of the agreements prohibited or limited the redisclosure of student data or other confidential information,[131] the remaining eleven percent (11%) failed to incorporate this critical contract provision. None of the contracts specifically prohibited the sale and marketing of children's information.[132] Additionally, none specifically authorized access for health, safety or emergency purposes.[133] None included provisions limiting access by government departments—access that would not generally be permitted by FERPA. Although not restricted by any legal obligation, none of the agreements contemplated the issue of foreign storage of US student data that might jeopardize the privacy of such information.

For the 89% of the districts that did include contractual clauses prohibiting or limiting redisclosure, the contractual language is often ambiguous[134] or allows for exceptions to the generally stated ban on redisclosure.[135] This means that vendors, without violating their

[128] Both agreements are with the same Eastern District. Agreement Document No. 4 provides that data is transferred "[f]or purposes of providing . . . evaluations…." *See* Agreement Document No. 4 at 2 . Agreement Document No. 6 allows for studies involving the collection, review, analysis, and de-identification of student data. *See* Agreement Document No. 6 at 1.

[129] Agreement Document No. 4 stipulates that the vendor remains under the "direct control" of the district with respect to use or maintenance of student data. *See* Agreement Document No. 4 at 2. Agreement Document No. 9 provides that the school district retains complete control over its data. *See* Agreement Document No. 9 at 7.

[130] Agreement Document No. 9 specifies that the district is the ultimate arbiter of who can view its data. *See* Agreement Document No. 9 at 2.

[131] Agreement Documents Nos. 1, 2, 3, 4, 6, 7, 8, and 9 contain such provisions.

[132] Under the PPRA, parental consent would be required if related to the regulated information. *See* 12 U.S.C. § 1232h(c).

[133] All of which are purposes permissible under FERPA. *See* 20 U.S.C. 1232g(b)(1)(I).

[134] For example, Agreement Document No. 2 limits the dissemination of information to parties with a need to know and to contractors who have signed written agreements obliging themselves to protect data in accordance with law. *See* Agreement Document No. 2 at 9 . Agreement Document No. 6 stipulates that the vendor will not cause the customer to be out of compliance with FERPA. *See* Agreement Document No. 6 at 1. Similarly, Agreement Document No. 7 stipulates that personally identifiable information is not provided to any non-approved third parties under the contract. *See* Agreement Document No. 7 at 2.

[135] For example, Agreement Document No 7 stipulates that confidential information is not disclosed "except as required by law." *See* Agreement Document No. 7 at 4.

agreements, may engage in data mining and data sales without district approval or parental consent.

Lastly, a majority of the agreements prohibited the vendor from unilaterally amending terms in the agreement.[136] These provisions are significant, as they prevent the vendor from altering the terms applicable to the district's data. However, one agreement contained a provision allowing the vendor to change the terms without providing notice to the district.[137] In effect, this clause means that the district cannot retain control over the data as required by the FERPA regulations. Similarly, two other agreements were silent on modifications.[138] In other words, one-third of the agreements did not prohibit vendors from changing the terms.

In short, with respect to data control, the districts' agreements did not generally assure compliance with FERPA[139] and thus fail to protect the districts and their students from vendors' mining and using transferred student data for purposes beyond those intended by the district.

e. Parental Notice, Consent, and Access to Collected Data

FERPA generally requires that a district provide notice to and obtain consent from parents before student information may be disclosed to vendors for analytic purposes other than program audit and evaluation.[140] The data analytics agreements, however, did not typically address the responsibility of notice to parents and the obtention of parental consent. More than three-quarters (78%) of the data analytics agreements were silent with respect to parental notification; only 22% required districts to assure notification.[141] Similarly, only one of the nine agreements (11%) required that the district obtain parental consent before it transferred data to the vendor.[142] This means that the contractual relationships between the districts and the vendors generally fail to establish or assure mechanisms that will enable compliance with FERPA obligations.

In addition, FERPA requires districts to offer parents access to their children's educational records, and additionally provides for correction rights.[143] The data analytics agreements did not contemplate this requirement and this, in effect, creates obstacles for districts to satisfy the parental access and correction obligation. The overwhelming majority of agreements were also silent with respect to parental access and correction of data. Only one agreement (11%) permitted a district to provide parents with the ability to access and correct data

[136] The six agreements are: Agreement Document No. 1, Agreement Document No. 3, Agreement Document No. 4, Agreement Document No. 6, Agreement Document No. 7, and Agreement Document No. 9.
[137] Agreement Document No. 2 contains a provision implying that the vendor's Terms of Service may be modified without notice provided to end users. *See* Agreement Document No. 2 at 8.
[138] Agreement Documents Nos. 5 and 6 were silent regarding data security obligations.
[139] *See* 20 U.S.C. § 1232g(b)(4)(B) ("[P]ersonal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student.").
[140] *See* 12 U.S.C. § 1232g(b).
[141] One such is the Agreement Document No. 3; another is Agreement Document No. 4 (including a condition that the "[the district] has specified at least annually in a FERPA notification to parents/guardians that it uses outside contractors or consultants as school officials…."). *See* Agreement Document No. 4 at 1.
[142] That agreement is Agreement Document No. 3.
[143] *See* 20 U.S.C. § 1232g(a)(2).

that was transferred to the vendor.[144] These findings with respect to parent notice, consent, and access are shown below:

NOTICE, CONSENT, ACCESS, AND TRANSPARENCY		
	Total (out of 9)	**Percentage**
Document Provides (for) Parental Notice	2	22.2%
Document Provides (for) Parental Consent	1	11.1%
District Can Provide Parental Access to, Correction of Data	1	11.1%
Parents Activate Account with Vendor Directly	0	0.0%

f. COPPA Obligations

To the extent that data analytics services collect information directly from school children or enable the tracking of school children based on their interactions with the cloud service, COPPA obligations would apply.[145] Only one of the data analytics agreements (11%) contemplated gathering information directly from children and anticipated tracking the children's online activity.[146] This reflects that data analytic contracts are essentially service agreements with school districts and not systems designed for children to engage directly with the vendor.

g. Data Security

As a data security measure, FERPA requires the destruction or deletion of data after it is no longer needed for the purposes for which it was transferred.[147] The two-thirds of the data analytics agreements (67%) did provide for the deletion of student data at the conclusion of the contract. Yet, one-third of the agreements failed to meet this requirement. Seventy-eight percent

---

[144] Agreement Document No. 7 provides that subscribers or their parents/guardians are restricted to accessing their own data materials. *See* Agreement Document No. 7 at 1.

[145] *See supra* Part II.C for a discussion of COPPA and districts' responsibilities and obligations with respect to the Act.

[146] The agreement stipulates that the product may be used to collect personally identifiable information from children under the age of 13, which triggers COPPA obligations. *See* Agreement Document No. 7 at 4 . A contract summary form accompanying the agreement stipulates that the vendor provides a "comprehensive online solution that will track all student data . . . and consists of the following components: 1. Progress Tracking," which includes tracking student attendance, test scores, course grades, credits, schedule, contact info, behavior, PBGR components, and "2. Individual Learning Plans," which include goal setting, course map, activities, career roadmap, resumes, questionnaires, parental review, and additional links. *See id.* at 1.

[147] *See, e.g.*, 20 U.S.C. § 1232g(b)(1)(F) (making data destruction a condition of disclosure for the purpose of "conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction…"); 20 U.S.C. § 1232g(b)(K)(ii) (making data destruction a condition of disclosure to "the Secretary of Agriculture, or authorized representative from the Food and Nutrition Service or contractors acting on behalf of the Food and Nutrition Service, for the purposes of conducting program monitoring, evaluations, and performance measurements of State and local educational and other agencies and institutions receiving funding or providing benefits of 1 or more programs authorized under the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq.) or the Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.) . . . ."); 20 U.S.C. § 1232g(b)(3) (requiring that personally identifiable data be destroyed when no longer needed after use by the "Comptroller General of the United States, [ ] the Secretary, or [ ] State educational authorities [ ] having access to student or other records . . . necessary in connection with the audit and evaluation of Federally-supported education programs, or in connection with the enforcement of the Federal legal requirements which relate to such programs"). *See also* Part II.A (discussion of FERPA).

(78%) of the agreements contained a clause providing for data security, but only one specified any type or minimum level of encryption.[148] Only one agreement (11.1%) required the vendor to notify the district in the event of a data security breach.[149] These findings are shown in the following table:

DATA SECURITY		
	Total (out of 9)	**Percentage**
Data Deleted or Destroyed at End of Contract Period	6	66.6%
Non-Specified Security Obligation	7	77.8%
Encryption Level Specified	1	11.1%
NIST Level Specified	0	0.0%
Data Breach Notification Specified	1	11.1%

2. Student Reporting Functions

a. Prevalence

Of the twenty responding districts, only four (20%) produced agreements suggesting that they outsource student reporting functions to third party vendors.[150] These four districts produced a combined total of five agreements from multiple vendors.[151] The limited use of cloud services for student reporting functions suggests that districts continue to prefer that these services be performed internally. It is also possible that such agreements were provided, but because of their ambiguity or vagueness were included below as an unidentified function.[152] A final possibility is that some districts simply failed to account for all of the third party services that they use when responding to our document request or did not understand their information technology infrastructure.

[148] For example, Agreement Document No. 1 provides that the vendor will take "[r]easonable steps to safeguard . . . confidential information." *See* Agreement Document No. 1 at 5. Agreement Document No. 2 provides that vendor will protect data in accordance with its own policies regarding confidential information. *See* Agreement Document No. 2 at 8. Agreement Document No. 4 imposes security measures that are "consistent with industry standards." *See* Agreement Document No. 4 at 4. Interestingly, specific security measures were listed in an Exhibit of the agreement but were redacted by the district. *See id.* at 10–11. Similarly, Agreement Document No. 7 with the same district specifies that "commercially reasonable precautions" are taken to protect data. *See* Agreement Document No. 7 at 3. One agreement—Agreement Document No. 8—contains a data security provision that seems to protect only the vendor's confidential information by specifying that the "[c]ustomer will use commercially reasonable efforts to prevent unauthorized access to or use of the [service]." *See* Agreement Document No. 8 at 2. Agreement Document No. 9 provides for numerous security requirements and guidelines, including "[k]ey baseline security requirements and that 'all sensitive data [be] sent over SSL when travelling over external networks.'" *See* Agreement Document No. 9 at 9–14.

[149] Agreement Document No. 7 stipulates that the service provider "immediately advises the licensee in writing upon reasonable suspicion or actual knowledge of a security threat." *See* Agreement Document No. 7 at 3.

[150] The four districts are: Jefferson County Public Schools (CO), Mercer Island School District, Providence Public School District, and Sublette County School District #9.

[151] The agreements are on file with Fordham CLIP.

[152] *See supra* Part IV.A.7.

b. Contracts

All of the districts had fully executed contracts with the vendors; but, of the five student reporting agreements, one was incomplete.[153] Only one of the agreements (20%) contained provisions giving the district a contractual right to audit and inspect the vendor's compliance with the agreement transferring student information.[154] This means that districts are handicapped in assuring the fair treatment of their student data.

c. Types of Student Identifying Data Transferred from Districts to Vendors

The agreements for student reporting functions infrequently identified the student data being transferred to vendors. The findings are shown in the following table:

TYPE OF DATA TRANSFERRED		
Type of Data Specified	**Total (out of 5)**	**Percentage**
Name	0	0.0%
Address	0	0.0%
Sex	0	0.0%
ID	0	0.0%
Age/Grade	0	0.0%
Biometric	0	0.0%
Medical/Health	0	0.0%
Socio-Economic	0	0.0%
Transaction Data	1	20%

Of the five student reporting agreements, only one (20%) specified that identifying data was transferred between the district and the vendor.[155] In their specifications, this agreement referenced only one type of data—transaction data—as transferred.

This failure to specify the types of student data transferred presents a significant transparency issue and is inconsistent with the FERPA mandate.[156] This cannot be an accurate reflection of the actual data transferred because the purpose of these agreements is reporting on individual students.

d. Data Control: Sharing, Mining, and Redisclosure

School districts may disclose some student personally identifiable information without first obtaining parental consent on the basis of FERPA's exceptions to its general consent requirement.[157] Because student reporting functions are services that school districts historically

---

[153] The incomplete document was Agreement Document No. 14. Neither the service's Privacy Policy nor its Terms of Use—both integrated with the agreement by reference—were provided. Fordham CLIP was able to retrieve these documents (both on file with Fordham CLIP) online on July 31, 2013, at 12:05 PM.
[154] Agreement Document No. 12 provides that all data remains the property of the school district, which could also be construed as providing a right of audit or inspection. *See* Agreement Document No. 12 at 3.
[155] Agreement Document No. 15 at 1, 3 (specifying that vendor has license "to use, reproduce, extract and otherwise process…Customer Data" [subject to certain limitations] and defining "Customer Data" as any education-related data that is inputted or submitted by the district or users of the service).
[156] *See* 34 C.F.R. 99.35(a)(3)(A).
[157] *See generally* 20 U.S.C. § 1232g(b).

performed internally, districts would most likely not need parental consent under FERPA to transfer data to vendors who would perform those services.[158] None of the student reporting agreements, however, referenced such qualifying functions for the disclosure of student information to the vendor. Districts would, though, still have to retain control over the student data. These findings with respect to key attributes of data control are illustrated in the following table:

DATA CONTROL: LIMITS ON SHARING, MINING, AND REDISCLOSURE		
	Total (out of 5)	**Percentage**
Document Prohibits or Limits Redisclosure	4	80%
District Retains Exclusive Control of Data	1	20%
District Retains Audit and Inspection Rights Respecting Vendor	1	20%
District Retains Right to Determine Data Access Based on User Role	3	60%
Document Specifies Audit/Evaluation Purpose for Disclosure	0	0.0%
Data Used for: Sale/Marketing of Instructional Materials, Student Recognition, College, Military, or Low-Cost Literary Materials	0	0.0%
Disclosure Allowed for Heath, Safety, or Emergency Purpose	0	0.0%
Document Prohibits Sale and Marketing of Data	0	0.0%
Foreign Storage Prohibited	0	0.0%
Access by Other Government Agencies Prohibited	0	0.0%

Overall, the student reporting agreements did a poor job of stipulating that the contracting district retains exclusive control of the data that it transfers to the vendor. Of the five agreements, only one (20%) stipulated that the district would retain exclusive control of the transferred data.[159] A majority of the agreements (60%) did, though, give the district a right to control the access to transferred data based on the user's role.[160] More positively, four of the agreements (80%) contained provisions prohibiting or limiting the redisclosure of student data or other confidential information.[161] This is significant because redisclosure of student data is prohibited by FERPA without additional parental consent,[162] and these express prohibitions seek to bar vendors from leveraging data for multiple purposes. Nevertheless, the contractual

[158] *See* 20 U.S.C. §1232g(b)(1) (describing the requirement that parental consent be obtained before a district may disclose personally identifiable student information, and carving out exceptions to this general rule).
[159] Agreement Document No. 12 specifies that all data transferred remains the property of the district. *See* Agreement Document No. 12 at 3.
[160] Agreement Document No. 10 specifies that the subscriber designates an employee subscriber administrator who is responsible for assigning passwords and authorizing others' access to the service; the agreement is silent, however, on whether the district has the authority to determine the vendor's use of and access to data based on role. *See* Agreement Document No. 10 at 4. Similarly, Agreement Document No. 14 provides that the subscriber "set[s] and maintain[s] access and permission rights for authorized users," and it too is silent as to whether the district has the authority to determine the vendor's use of and access to data based on role. *See* Agreement Document No. 14 at 1. Agreement Document No. 12 provides for access limits and prohibits any unauthorized uses of data beyond those limits. *See* Agreement Document No. 12 at 2.
[161] The agreements containing such provisions are: Agreement Document No. 11, Agreement Document No. 12, Agreement Document No. 14, and Agreement Document No. 15 (all on file with Fordham CLIP).
[162] *See* 20 U.S.C. § 1232g(b)(4)(B) ("[P]ersonal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student.").

language in the districts' agreements is often ambiguous[163] or allows for exceptions to the generally stated no-redisclosure policy.[164] This means that vendors could take advantage of the ambiguous terms to use data for multiple purposes. None of the agreements contained a provision expressly prohibiting the vendor from selling or using the student data for marketing purposes. And, none of the agreements included protections with respect to foreign data storage and government agency access.

Finally, 40% of the student reporting agreements contained a provision prohibiting the vendor from unilaterally amending the agreement.[165] This is a positive contracting practice, as it prevents a vendor from altering the terms of the agreement. However, one of the agreements allowed the vendor to unilaterally modify the contractual terms without notice to the district.[166] Where the vendor can unilaterally alter the terms of the contract, the district has, in effect, relinquished control over the data in contradiction to FERPA. The remaining two agreements were silent with regard to modification.

e. Parental Notice, Consent, and Access to Collected Data

The student reporting agreements fared poorly in addressing the responsibility for providing notice to parents of outsourcing arrangements. Similarly, the agreements did not establish mechanisms for districts to comply with the requirements for parental access and correction. The findings are shown in the following table:

NOTICE, CONSENT, ACCESS, AND TRANSPARENCY		
	Total (out of 5)	**Percentage**
Document Provides (for) Parental Notice	0	0.0%
Document Provides (for) Parental Consent	0	0.0%
District Can Provide Parental Access to, Correction of Data	0	0.0%
Parents Activate Account with Vendor Directly	0	0.0%

Of the five student reporting agreements, none stipulated that the district must notify parents that the service is used or that student data is transferred. Similarly, none required that the district obtain parental consent before it transfers data to the vendor.

163 For example, Agreement Document No. 11 stipulates that "[the vendor] agrees not to use, disclose or distribute any student information directly or indirectly without Subscriber's prior written consent," and that "[the vendor] agrees to respect such confidentiality and shall use [it's] best efforts to keep such data confidential." *See* Agreement Document No. 11 at 2. Similarly, Agreement Document No. 12 stipulates that neither party shall disclose directly, indirectly, or allow to be disclosed any confidential data, and that the parties will only use confidential data to perform their obligations under the contract. *See* Agreement Document No. 12 at 3. Finally, Agreement Document No. 15 seems to oblige only the district with respect to the vendor's confidential information: "Customer will use commercially reasonable efforts to prevent unauthorized access to or use of the [service]." *See* Agreement Document No. 15 at 2.

164 For example, Agreement Document No. 12 stipulates the parties will only use confidential data to perform their obligations under the contract. *See* Agreement Document No. 12 at 3. Similarly, Agreement Document No. 14 stipulates that data will not be redisclosed unless required by law, to protect property rights, or to protect personal safety in an emergency. *See* Agreement Document No. 14 at 2.

165 These agreements are Agreement Document No. 11 and Agreement Document No. 12.

166 Agreement Document No. 14 provides that the service's Terms of Use are amendable with notice posted only to the terms as found on the web. *See* Agreement Document No. 14 at 1.

Additionally, all of the student reporting agreements were silent with respect to parental access and correction of data. None indicated whether parents could activate accounts to access their children's data. This means that the districts have not contractually assured that they can comply with the access and correction provisions of FERPA.[167]

f. COPPA Obligations

None of the student reporting agreements indicated that the service allowed a child to supply personally identifiable information or enabled a child to be tracked. These findings are illustrated in the following table:

COPPA OBLIGATIONS		
	Total (out of 5)	**Percentage**
Service Enables Child to Supply PII	0	0.0%
Service Enables Child to Be Tracked	0	0.0%

This is surprising, because half of the agreements seem to involve data collection directly from students. To the extent that student reporting systems would be open to middle school students to consult class grades, then COPPA would be relevant and applicable to those under 13.

g. Data Security

As previously noted, FERPA imposes obligations on districts for data security in many circumstances when they transfer data.[168] A strong majority of student reporting agreements (60%) provided for data deletion at the end of the contract period, and three of the five (60%) student reporting agreements specified some type of security obligation on the part of the vendor.[169] One agreement went further to specify the encryption level used by the vendor,[170] but none referred to a specific NIST level. And lastly, none of the agreements required vendors to notify districts of any data security breach. These findings are summarized below:

DATA SECURITY		
	Total (out of 5)	**Percentage**
Data Deleted or Destroyed at End of Contract Period	3	60%
Non-Specified Security Obligation	3	60%
Encryption Level Specified	1	20%
NIST Level Specified	0	0.0%
Data Breach Notification Specified	0	0.0%

[167] *See* 20 U.S.C. § 1232g(a)(2).
[168] *See, e.g., supra* notes 139 and 147.
[169] Agreement Document No. 11 provides that "[the vendor] agrees to respect [ ] confidentiality and shall use [it's] best efforts to keep [ ] data confidential." *See* Agreement Document No. 11 at 2. Agreement Document No. 12 simply provides that "information will be transferred and maintained in a secure manner." *See* Agreement Document No. 12 at 4. Finally—and contrary to the apparent trend obliging *vendors* to maintain a security obligation—Agreement Document No. 15 provides that "*Customer* will[ ] use commercially reasonable efforts to prevent unauthorized access to or use of the [service]" (emphasis added). *See* Agreement Document No. 15 at 2.
[170] Agreement Document No. 15 specifies that the vendor uses "SSL encryption" to protect data. *See* Agreement Document No. 15 at 2.

3. Guidance Functions

a. Prevalence

Of the twenty responding districts, only five (25%) produced agreements suggesting that they outsource guidance functions to third party vendors.[171] The five districts produced a combined total of six agreements from three different vendors.[172] While this suggests a concentration of vendors, the limited number of agreements also indicates that districts do not widely use cloud services to fulfill school guidance functions. Like the findings in the other contract categories, this may reflect a district preference to rely on internal systems or may reflect that other agreements provided were too vague to determine a guidance purpose and were thus classified as "unidentifiable function" agreements. It is also possible that districts omitted relevant agreements in their responses.

b. Contracts

Of the six guidance agreements, only three (50%) represented fully executed contracts between the district and the vendor.[173] One of the six agreements was also incomplete.[174] Of the half of the agreements that were not executed, the guidance functions seemed to involve "click-through" agreements that require users or students to accept service terms of use and/or privacy policies. This means that districts may be imposing whatever terms vendors offer on students or their parents without negotiation. These findings are illustrated in the following table:

CONTRACTING		
	Total (out of 6)	**Percentage**
Direct Contract Between District and Vendor	3	50.0%
Vendor May Unilaterally Amend (With Direct Notice)	1	16.7%
Vendor May Unilaterally Amend (Without Notice)	2	33.3%
Vendor May Not Unilaterally Amend	2	33.3%

Three of the five districts also used the same vendor's services but with different terms and conditions in their agreements.[175] This may reflect negotiations between districts and the vendor or may reflect different services under contract. The texts of the agreements did not provide a basis to determine why the terms are slightly different.

Lastly, none of the agreements provided districts with a right to audit and inspect vendors' compliance with the contract obligations. As a result, none of the districts have the legal right to verify how their data is treated by the vendors.

[171] The five districts are: Jefferson County Public Schools (CO), Jefferson County Public Schools (KY), Mercer Island School District, Millburn Township Public Schools, and Queen Anne's County Public Schools.
[172] The six agreements are: Agreement Document No. 16, Agreement Document No. 17, Agreement Document No. 18, Agreement Document No. 19, Agreement Document No. 20, and Agreement Document No. 21.
[173] These agreements are by West District, South District, and Northeast District.
[174] The incomplete document was Agreement Document No. 20, which referenced a Privacy Policy that was not supplied to Fordham CLIP.
[175] *See* Agreement Document No. 16; Agreement Document No. 17; Agreement Document No. 20.

c. Types of Student Identifying Data Transferred from Districts to Vendors

Unlike the agreements in the previous categories, the contracts for guidance functions frequently specified the types of student data being transferred to vendors. The findings are illustrated by the following table:

TYPE OF DATA TRANSFERRED		
Type of Data Specified	**Total (out of 6)**	**Percentage**
Name	5	83.3%
Address	5	83.3%
Sex	4	66.7%
ID	1	16.7%
Age/Grade	4	66.7%
Biometric	0	0.0%
Medical/Health	0	0.0%
Socio-Economic	1	16.7%
Transaction Data	3	50.0%

An overwhelming majority of the six agreements detailed whether student name, address, sex, age/grade, and transaction data were transferred. On the other hand, very few of the agreements specified whether student ID numbers, biometric, or medical/health data were transferred.

d. Data Control: Sharing, Mining, and Redisclosure

Guidance functions involve the processing of student information to counsel students in their academic, personal/social and career development.[176] Guidance data will often be part of a student's educational record and subject to FERPA's restrictions on disclosures and use. Similarly, where the information relates to personal and social development, the PPRA may also apply by requiring parental consent for the collection and use of the data.[177] Thus, as with the other categories of agreements, district control over outsourced data in the context of guidance functions is quite important. The content of the contracts that outsource student data for guidance functions is summarized in the following table:

[176] *See, e.g.*, Va. Dept. of Educ., Student and School Support: Student Counseling and Guidance, http://www.doe.virginia.gov/support/school_counseling/index.shtml (last visited Nov. 15, 2013).
[177] *See supra* Part II.B.

DATA CONTROL: LIMITS ON SHARING, MINING, AND REDISCLOSURE		
	Total (out of 6)	**Percentage**
Document Prohibits or Limits Redisclosure	4	66.7%
District Retains Exclusive Control of Data	0	0.0%
District Retains Audit and Inspection Rights Respecting Vendor	0	0.0%
District Retains Right to Determine Data Access Based on User Role	0	0.0%
Document Specifies Audit/Evaluation Purpose for Disclosure	1	16.7%
Data Used for: Sale/Marketing of Instructional Materials, Student Recognition, College, Military, or Low-Cost Literary Materials	1	16.7%
Disclosure Allowed for Heath, Safety, or Emergency Purpose	0	0.0%
Document Prohibits Sale and Marketing of Data	0	0.0%
Foreign Storage Prohibited	0	0.0%
Access by Other Government Agencies Prohibited	0	0.0%

As a starting point, the table shows that only one agreement specified that student data was transferred for an audit or evaluation purpose.[178] Another agreement (16.7%) specified that data was transferred for the sale and marketing of products for college recruitment.[179] None of the agreements specified that disclosure was for a health or emergency purpose. Similarly, none of the agreements specified that data was transferred for health, safety, or emergency purposes.[180] This means that parental consent would be required in all the other guidance arrangements for the transfer of all data subject to FERPA.

The table also shows that none of the guidance agreements provided districts with exclusive control over their data. Similarly, none of the agreements allowed districts to set user access or controls. Nor did any agreements grant the districts a right to audit or inspect the vendor for compliance with the terms of the agreement.

Additionally, none of the agreements prohibited foreign storage of student data or prohibited access to transferred student data by other government agencies. In essence, the districts cannot assure compliance with FERPA's obligations for direct control over third parties processing student data as a result.

FERPA also requires a ban on redisclosure without parental consent.[181] If the data is not subject to FERPA, limitations on redisclosure are still important fair information practices to protect student privacy. While two-thirds of the guidance agreements contained provisions limiting or prohibiting data redisclosure, one-third did not.[182] For those that did impose contractual limitations, the contractual language was often ambiguous[183] or allowed exceptions

[178] *See* Agreement Document No. 21 at 5 (providing that the vendor uses aggregate information to generate statistical studies and to conduct research related to "[their] professional work").
[179] The vendor uses aggregate information to "identify, develop, and offer products and services that help in the transition from high school to college." *See* Agreement Document No. 21 at 5. This is a permissible use under FERPA. *See* 20 U.S.C. §§ 1232h(c)(1)(E)-(c)(4)(A).
[180] *See* 20 U.S.C. § 1232g(b)(1)(I).
[181] *See* 20 U.S.C. § 1232g(b)(4)(B) ("[P]ersonal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student.").
[182] Those four agreements are: Agreement Document No. 16, Agreement Document No. 18, Agreement Document No. 20, and Agreement Document No. 21.
[183] For example, Agreement Document No. 20 provides that the vendor will not disclose information to its partners without consent. *See* Agreement Document No. 20 at 1. The same vendor's agreement with one Central district provides for a clearer limitation, however: it stipulates that if the client is subject to FERPA, the vendor will not disclose personally identifiable information without obtaining signed and dated written consent of the student, or if

to the generally stated bar to redisclosure.[184] None of the guidance agreements expressly prohibited the vendor from selling or using guidance data for marketing purposes.

In terms of contract modification, only one of the six guidance agreements prohibited the vendor from unilaterally amending the agreement.[185] By contrast, one-third of the agreements allowed the vendors to unilaterally modify the contractual terms without notice to the district.[186] Two agreements, however, allowed the vendor to unilaterally amend the agreement with notice to the district.[187] The last agreement was silent on the matter.[188]

In effect, the majority of the vendors may alter the terms of the agreement without the district's explicit consent. This means that the districts do not have any effective control over their data once it is transferred to the vendors for guidance functions.

e. Parental Notice, Consent, and Access to Data Collected

The guidance function agreements do not generally address the need to provide notice to parents or to obtain parental consent. Of the six guidance agreements, none required parental notification. One stipulated that if the vendor were to redisclose student data, the district must notify parents about the district's use of the service and that student data was transferred.[189] Only one of the six agreements (17%) required the availability (without any notification) of an opt-out for parents who did not want their child's data collected by the vendor.[190] This is problematic, as the parental rights to notice of and consent to the transfer of student information are central tenets of FERPA, and have only limited exemptions.[191] The agreements also failed to reserve to the district a right to allow for parental access to and correction of the data that is transferred to vendors; only one of the guidance agreements enabled the district to provide such a

---

the student is under eighteen years of age, the student's parents/guardians. *See* Agreement Document No. 17 at 8. Agreement Document No. 18 however, provides that limitations on the redisclosure of confidential information affect only the subscriber and not the service provider. *See* Agreement Document No. 18 at 6.

[184] For example, Agreement Document No. 21 provides that redisclosure of information to third parties is not permitted except as required by law, or to "relevant suppliers to complete purchases or transactions." *See* Agreement Document No. 21 at 2, 5. Additionally, Agreement Document No. 20 provides that the vendor will not disclose information to its partners without consent; however, the agreement also provides that use of the vendor's website amounts to consent to the collection, use, and maintenance of information. *See* Agreement Document No. 20 at 1.

[185] Agreement Document No. 18 provides that neither party may modify the contract without written agreement. *See* Agreement Document No. 18 at 6.

[186] Agreement Document No. 20 provides that changes to the service's Privacy Policy are made only online, and thus without direct notice to subscribers or end users. *See* Agreement Document No. 20 at 3. Agreement Document No. 21 provides that the vendor reserves the right to change or amend its Privacy Policy or Terms and Conditions without notice. *See* Agreement Document No. 21 at 1, 2, 4.

[187] Agreement Document No. 17 provides that the vendor give 60 days of written notice and that contract changes are effective upon renewal. *See* Agreement Document No. 17 at 12. Agreement Document No. 19 provides that vendor must give "appropriate online notice" before making any material modification. *See* Agreement Document No. 19 at 5.

[188] Agreement Document No. 16 contained no provision addressing amendment.

[189] Agreement Document No. 17 provides that if the client is subject to FERPA, the vendor will not disclose personally identifiable information without obtaining signed and dated written consent of the student, or if the student is under eighteen years of age, the student's parents/guardians. *See* Agreement Document No. 17 at 8.

[190] Agreement Document No. 16 provides that parents may email the vendor to opt their child out of its practice of collecting personally identifiable information, which implies that if the parents decline to do so, they provide their consent to the collection of such information. *See* Agreement Document No. 16 at 2.

[191] *See* 34 C.F.R. 99.35(a)(3).

right.[192] Without retaining this right, districts do not have the legal ability to satisfy FERPA's access and correction mandate. These findings are summarized in the following table:

NOTICE, CONSENT, ACCESS, AND TRANSPARENCY		
	Total (out of 6)	**Percentage**
Document Provides (for) Parental Notice	0	16.7%
Document Provides (for) Parental Consent	1	16.6%
District Can Provide Parental Access to, Correction of Data	1	16.7%
Parents Activate Account with Vendor Directly	0	0.0%

f. COPPA Obligations

None of the guidance agreements provided that the service allows a child to supply personally identifiable information or enables a child to be tracked. This is surprising, as half of the agreements seemed to contemplate users' agreeing to privacy terms. And, none of the agreements indicated that parents would have to activate an account directly with the vendor. The lack of contractual provisions does not assure that the service bans children from supplying personally identifiable information or being tracked. While one agreement, for example, was silent on the matter altogether,[193] other agreements expressly provided that the service does not allow students to supply personally identifiable information.[194] Nevertheless, if the services are provided via a website allowing children under 13 to input data, then COPPA's obligations will apply.

g. Data Security

Data security is only partially addressed in the guidance function agreements. Two-thirds of the agreements did not require that vendors delete or destroy data upon termination of the agreement, even though FERPA generally requires the destruction or deletion of data after it is no longer needed for the purpose for which the data was originally transferred.[195] Further, one-third of the agreements failed to require any data security obligation on the part of the vendor.[196] Only one agreement included a specific level of security.[197] None of the agreements contained a provision requiring the vendor to notify the district in the event that the vendor's security measures are breached or data is otherwise compromised. These findings are illustrated in the following table:

---

[192] Agreement Document No. 20 provides for access to and correction of student information. *See* Agreement Document No. 20 at 2.

[193] The Agreement Document No. 18 Terms of Use do not make clear whether a child under the age of 13 may supply personally identifiable information through the service or be tracked by the services. *See generally* Agreement Document No. 18.

[194] For example, Agreement Document No. 20 provides that the service is not directed toward use by children. *See* Agreement Document No. 20 at 3. Agreement Document No. 21 provides that the vendor does not knowingly collect information from users under 13 years of age. *See* Agreement Document No. 21 at 1.

[195] *See, e.g., supra* note 147.

[196] Those agreements are Agreement Document No. 16 and Agreement Document No. 20. Four agreements did provide for data security. *See* Agreement Document No. 17; Agreement Document No. 18; Agreement Document No. 19; Agreement Document No. 21.

[197] Agreement Document No. 17 provided that the vendor uses SSL encryption. *See* Agreement Document No. 17 at 8.

DATA SECURITY		
	Total (out of 6)	**Percentage**
Data Deleted or Destroyed at End of Contract Period	2	33.3%
Non-Specified Security Obligation	4	66.7%
Encryption Level Specified	1	16.7%
NIST Level Specified	0	0.0%
Data Breach Notification Specified	0	0.0%

4. Special School Functions

a. Prevalence

Of the twenty responding districts, five (25%) produced agreements representing the outsourcing of various special school functions to third party vendors.[198] These districts produced a combined total of nine agreements for seven different services.[199] These services related to payment for student cafeteria purchases, planning and managing bus transportation, managing student health and fitness data, testing memory for student interventions, and managing mass notifications to members of the school community including students and parents.[200] There may be additional functions outsourced to the cloud that were not clearly described in the agreements and were thus treated as having an unidentifiable function.[201] Similarly, because these functions are not related to instruction, districts may not have recognized that other district agreements involved student data and cloud services.

---

[198] The five are: Jefferson City Public Schools, Maricopa Unified School District #20, Mercer Island School District, Millburn Township Public Schools, and Pennsbury School District.

[199] The vendors' information is on file with Fordham CLIP.

[200] The seven different services for which we received agreements are summarized as follows:

- Agreement Documents Nos. 22 and 29 (from the same vendor) represent an online service that allows parents to track and finance their child's school meals. *See generally* Agreement Documents Nos. 22 and 29.
- Agreement Document No. 23 represents a service that offers student transportation services to school districts. *See* Agreement Document No. 23 at 1.
- Agreement Document No. 24 represents a service that "enable[s] [the district] to communicate with parents/guardians about attendance, school events, emergency situations, and important issues impacting [the parent's] child." *See* Agreement Document No. 24 at 1.
- Agreement Documents Nos. 25 and 27 (from the same vendor) represent a service that enables the district to "send unlimited any-time messages to parents of enrolled students, administrators, faculty, staff, and board members." *See generally* Agreement Documents No. 25; Agreement Document No. 27.
- Agreement Document No. 26 represents a service that that provides a "computer-based solution for attention problems caused by poor working memory." *See Vendor's website, URL on file with Fordham CLIP* (last visited Oct. 9 2013).
- Agreement Document No. 28 represents a service providing a "bus routing and scheduling system." *See* Agreement Document No. 28 at 1.
- Agreement Document No. 30 represents a service that provides a "web-based school health information system . . . designed to monitor student health and fitness parameters, help schools meet wellness mandates, and support a culture of wellness . . . by harness[ing] technology with best practices to provide online resources that help the entire school community create a healthier learning environment." *See Vendor's website, URL on file with Fordham CLIP* (last visited Oct. 9 2013).

[201] *See supra* Part IV.A.7.

Because the special school function agreements do not appear to involve educational records,[202] no privacy law is likely to apply to the student data that is transferred by districts under these contracts despite the sensitivity of the data. For example, school cafeteria purchase records reveal what each student eats every day at the cafeteria, and school transportation data reveals the street corners where students will be standing early in the morning and after school.

b. Contracts

Of the nine special school functions agreements, more than 75% represented fully executed contracts between the district and the vendor,[203] and one provided that the service was available to the district free of charge.[204] This suggests that some districts have attenuated relationships with the entities processing their students' data, either due to a lack of contractual privity or due to a lack of a financial consideration. None of the special school functions agreements specified that disclosure was for an audit or evaluation purpose. None of the agreements indicated that disclosure was for the sale or marketing of instructional materials, student recognition, college or military recruitment, or low-cost literary materials. The lack of such disclosures re-enforces that the data implicated by these agreements is outside the scope of FERPA. One of the agreements did, however, stipulate that the transfer of student information was for health, safety, or emergency purposes.[205] This agreement was for a system designed to track student health and well-being.[206]

In terms of compliance mechanisms, none of the special school functions agreements provided the district with a contractual right to audit and inspect the vendor's practices with respect to the transferred data. As a result, districts will have difficulty effectively monitoring that vendors treat the student data appropriately.

The special school functions agreements were also frequently incomplete, with two-thirds missing critical elements in the documentation.[207] This presents a serious transparency issue, as

---

[202] 20 U.S.C. § 1232g(a)(4)(A). The Supreme Court has held that educational records are those records maintained as institutional records about students rather than other information about students generated in the course of a student's day. *See* Owasso Indep. School District v. Falvo, 534 U.S. 426 (2002) (holding peer-grade assignments are not educational records under FERPA).

[203] Those agreements are Agreement Document No. 23, Agreement Document No. 24, Agreement Document No. 26, Agreement Document No. 27, Agreement Document No. 28, Agreement Document No. 29, and Agreement Document No. 30.

[204] Agreement Document No. 29 provides that the service is free to districts, but that the service collects a $1.75 convenience fee for every deposit made by parents. *See* Agreement Document No. 29 at 2. Note that there is no similar provision in Agreement Document No. 22 (between the same vendor and a different district) because that district supplied an incomplete agreement. *See infra* note 207.

[205] *See generally* Agreement Document No. 24 and Agreement Document No. 30.

[206] *See supra* note 200 (providing a brief description of the service represented by Agreement Document No. 30).

[207] Of the nine special school functions agreements, only four were complete: Agreement Document No. 26, Agreement Document No. 28, Agreement Document No. 29, and Agreement Document No. 30. The five incomplete agreements are as follows:

- Agreement Document No. 22: The terms and conditions and software license agreement provided were unsigned, but were stated to be agreed upon through acceptance of a separate referenced proposal; this proposal was not supplied to Fordham CLIP.
- Agreement Document No. 23: The original agreement between the vendor and the district was not supplied to Fordham CLIP.
- Agreement Document No. 24: The original agreement between the vendor and the district was not supplied to Fordham CLIP.

it indicates that the districts either did not have the missing documents or did not fully respond to the public records request. These findings are illustrated by the following table:

DOCUMENT COMPLETENESS		
	Total (out of 9)	**Percentage**
Complete Documents Provided	4	44.4%
Document Was Obtained Post-Open Records Request	0	0.0%

c. Types of Student Identifying Data Transferred from Districts to Vendors

The agreements for special school functions rarely specified the types of student data being transferred. The indications of student identifying data are shown in the table below:

TYPE OF DATA TRANSFERRED		
Type of Data Specified	**Total (out of 9)**	**Percentage**
Name	1	11.1%
Address	1	11.1%
Sex	0	0.0%
ID	1	11.1%
Age/Grade	1	11.1%
Biometric	0	0.0%
Medical/Health	0	0.0%
Socio-Economic	0	0.0%
Transaction Data	0	0.0%

Only one of the special school functions agreements specified that student name, address, and age/grade were transferred under the agreement.[208] One other agreement specified that student ID numbers were transferred to the vendor.[209] The seven other agreements did not specify the types of student data transferred at all.

Notwithstanding the silence of the agreements with respect to data types, each agreement is likely to involve the transfer of one or more identifying data points. This is especially true considering the types of services these vendors provide.[210] For example, it seems probable that data types such as name, address, and age would be transferred to a vendor providing student transportation services. Additionally, one might expect that student health information would be transferred in connection with a "web-based school health information system."[211] Indeed, that arrangement might also be subject to COPPA if students are asked to provide information directly on the vendor's website.

- Agreement Document No. 25: The vendor's Acceptable Use Policy and Privacy Policy were not supplied to Fordham CLIP.
- Agreement Document No. 27: The vendor's Privacy Statement was not supplied to Fordham CLIP.

208 *See* Agreement Document No. 27 at 1.
209 *See* Agreement Document No. 29 at 1.
210 *See supra* note 200.
211 *See supra* note 200.

d. Data Control: Sharing, Mining, and Redisclosure

The special school functions agreements generally contained few provisions assuring district control over student data once transferred to vendors. Given the sensitivity of the data, this is surprising. The attributes of data control included in the agreements are illustrated in the following table:

DATA CONTROL: LIMITS ON SHARING, MINING, AND REDISCLOSURE		
	Total (out of 9)	**Percentage**
Document Prohibits or Limits Redisclosure	3	33.3%
District Retains Exclusive Control of Data	0	0.0%
District Retains Audit and Inspection Rights Respecting Vendor	0	0.0%
District Retains Right to Determine Data Access Based on User Role	1	11.1%
Document Specifies Audit/Evaluation Purpose for Disclosure	0	0.0%
Data Used for: Sale/Marketing of Instructional Materials, Student Recognition, College, Military, or Low-Cost Literary Materials	0	0.0%
Disclosure Allowed for Heath, Safety, or Emergency Purpose	1	11.1%
Document Prohibits Sale and Marketing of Data	0	0.0%
Foreign Storage Prohibited	0	0.0%
Access by Other Government Agencies Prohibited	0	0.0%

Of the nine special school functions agreements, only one-third contained provisions that prohibit or limit the re-disclosure of student data or other confidential information.[212] This is a discouragingly low figure. Furthermore, the three agreements that do prohibit or limit redisclosure are ambiguous or subject to important exceptions to non-disclosure.[213] Consequently, vendors can take advantage of the terms in the agreements to use and redisclose the data beyond the original purposes of the special function agreement.

Only one of the agreements gave the district a right to determine access to the data it transfers based on a user's role.[214] None of the agreements expressly prohibited vendors from selling or using student data for marketing purposes. This is problematic; the absence of a provision expressly prohibiting the sale or marketing use of data implies that it may be permissible for the vendor to do so even though some of the agreements contain provisions that prohibit or limit redisclosure of data.

More troubling is the inability of districts to preserve the continued validity of the terms of their agreements. Fewer than 50% of the agreements prohibited vendors from unilaterally amending the terms and conditions.[215] One agreement expressly permitted the vendor to

---

[212] Those three agreements are Agreement Document No. 25, Agreement Document No. 27, and Agreement Document No. 29.

[213] For example, Agreement Document No. 25 provides that data is not rented, traded, or sold to third parties, but that it is disclosed if necessary to comply with law or to operate or maintain the service. *See* Agreement Document No. 25 at 1. Additionally, Agreement Document No. 29 provides that the vendor is not required to disclose student data in violation of FERPA. *See* Agreement Document No. 29 at 3.

[214] Agreement Document No. 29 provides that the district maintains student data and furnishes it to the vendor, subject to its responsibilities under FERPA. *See* Agreement Document No. 29 at 3.

[215] Those agreements are Agreement Document No. 22, Agreement Document No. 25, Agreement Document No. 28, and Agreement Document No. 30.

unilaterally modify the contractual terms without notice to the district,[216] another allowed unilateral modifications with notice to the district,[217] and one was silent on the matter.[218] These findings are illustrated in the following table:

CONTRACTING		
	Total (out of 9)	**Percentage**
Fully Executed Between District and Vendor	7	77.8%
Vendor May Unilaterally Amend (With Direct Notice)	1	11.1%
Vendor May Unilaterally Amend (Without Notice)	1	11.1%
Vendor May Not Unilaterally Amend	4	44.4%

e. Parental Notice, Consent, and Access to Data Collected

The special school functions agreements fared poorly with respect to parental notice and consent considerations. Only one agreement provided that parents should be notified[219] and their consent be obtained for data to be transferred under the agreement.[220] The agreements also generally failed to reserve to the district a right to allow for parental access to and correction of the data that was transferred to the vendor; only one of the agreements contained a provision enabling the district to provide parents and eligible students with such a right.[221] These findings are illustrated by the following table:

NOTICE, CONSENT, ACCESS, AND TRANSPARENCY		
	Total (out of 9)	**Percentage**
Document Provides (for) Parental Notice	1	11.1%
Document Provides (for) Parental Consent	1	11.1%
District Can Provide Parental Access to, Correction of Data	1	11.1%
Parents Activate Account with Vendor Directly	1	11.1%

Finally, one of the special school functions agreements indicated that parents must activate an account directly with the vendor.[222] The dearth of parent-activated accounts is slightly surprising, as it would seem that special school services might be more student- and parent-interactive than other functions that do not require student or parent interaction.[223] This

[216] Agreement Document No. 29 provides that the vendor reserves the right to change security providers and payment services without notice. *See* Agreement Document No. 29 at 1. Note that this provision allows for seemingly immaterial modifications.
[217] Agreement Document No. 27 provides that continued use of the services following the posting of changes to Privacy Policy terms constitutes acceptance of the revised terms. *See* Agreement Document No. 27 at 2.
[218] Agreement Document No. 24 contained no provision addressing amendment.
[219] In light of Agreement Document No. 24, the district provides a parent information letter to notify parents of the district's use of the service. *See* Agreement Document No. 24 at 1.
[220] In light of Agreement Document No. 24, the district provides a parent information letter to notify parents that their provision of their contact information to the district meets the consent requirement mandated by the district. *See* Agreement Document No. 24 at 1, 3.
[221] Agreement Document No. 27 provides: "[the vendor] offers users the ability to correct or change the information collected during registration." *See* Agreement Document No. 27 at 1.
[222] Agreement Document No. 29 provides that parents initiate and maintain their accounts with the vendor. *See* Agreement Document No. 29 at 1.
[223] *See, e.g.*, *supra* note 200.

also means that the parent activation may be used by the vendor to change the applicable privacy policies for the children's data from terms contractually agreed upon by the district.

f. COPPA Obligations

Of the nine special school functions agreements, one specified both that the service enables a child to supply personally identifiable information and enables a child to be tracked.[224] It would seem that at least some special school functions would be likely to require some level of student interaction. Of course, the lack of contractual provisions providing for such interaction does not imply that the service bars children from supplying personally identifiable information or from being tracked. The other eight agreements, for example, were silent on the matter altogether, and silence should not be construed as a prohibition. Furthermore, none of the agreements expressly provided that the service bans students from providing personally identifiable information. These findings suggest that special school function services rarely allow children to supply personally identifiable information, which is surprising considering the purposes for which some of such services are intended.[225] These findings are illustrated by the following table:

COPPA OBLIGATIONS		
	Total (out of 9)	**Percentage**
Service Enables Child to Supply PII	1	11.1%
Service Enables Child to Be Tracked	1	11.1%

g. Data Security

The special school functions agreements fared poorly with respect to how they addressed data security. None of the agreements specified that transferred data be deleted or destroyed at the end of the contract period, and less than a quarter contained a provision specifying some type of security obligation on the part of the vendor. Furthermore, none of the agreements contained a provision requiring the vendor to notify the district in the event that the vendor's security measures are breached or data is otherwise compromised. These findings are shown in the following table:

DATA SECURITY		
	Total (out of 9)	**Percentage**
Data Deleted or Destroyed at End of Contract Period	0	0.0%
Non-Specified Security Obligation	2	22.2%
Encryption Level Specified	1	11.1%
NIST Level Specified	0	0.0%
Data Breach Notification Specified	0	0.0%

[224] Agreement Document No. 27 provides that the service enables a child to supply information to chat rooms, message boards, and other similar interactive features, and also provides that such information may allow other users to track the child. *See* Agreement Document No. 27 at 1.
[225] *See, e.g.*, *supra* note 200.

Only three of the nine special school functions agreements specified some type of security obligation on the part of the vendor,[226] while the other six were silent on the matter. Two agreements contained a general security obligation.[227] One agreement also specified the encryption level used by the vendor.[228] None of the agreements, however, specified the level of security such as the NIST level. These findings are not encouraging, as they suggest that vendors of special school functions services—unlike the vendors of data analytics, student reporting, and guidance functions services—do not recognize data security as a concern and do not tailor their products and services accordingly.

Additionally, none of the nine special school functions agreements contained a provision requiring that the vendor notify the district in the event that the vendor's security measures are breached or data is otherwise compromised. Of course, it may be the case that vendors do, in fact, alert districts in the event of data breach without expressly contracting to do so. Nevertheless, the absence of express contractual provisions ensuring such is inconsistent with the inference that some vendors (of other types of services[229]) recognize data security as a legitimate concern. Accordingly, vendors of student reporting services should adopt data breach notification practices and include provisions for such in their agreements with districts.

5. Hosting, Maintenance, and Backup Functions

a. Prevalence

FERPA allows districts to outsource educational record information for institutional services without parental consent.[230] Hosting, maintenance and backup functions would fall within that authority. Of the twenty responding districts, 50% reported outsourcing hosting, maintenance, and backup functions to third party vendors.[231] Districts outsource these functions more frequently than other services within dataset.[232] Districts also use a wide variety of

---

[226] Those three agreements are Agreement Document No. 27, Agreement Document No. 29, and Agreement Document No. 30.

[227] Agreement Document No. 27 provides that all "personal information is stored on servers at a location designed specifically to ensure that no unauthorized individuals have access to the server or its data." *See* Agreement Document No. 27 at 1. Agreement Document No. 30 provides that the vendor uses "Cisco or other similar industry standard firewalls." *See* Agreement Document No. 30 at 5.

[228] Agreement Document No. 29 provides that the vendor uses SSL encryption and firewalls. *See* Agreement Document No. 29 at 6.

[229] *See, e.g.*, *supra* Parts IV.C.1.g and IV.C.2.g; *infra* Parts IV.C.5.g, IV.C.6.g., and IV.C.7.g (discussing vendors taking security obligations seriously). *But see supra* Part IV.C.3.g (describing a finding of weaker security obligations).

[230] *See supra* Part II.A.3.

[231] The ten districts are: Jefferson City Public Schools, Jefferson County Public Schools (KY), London City Schools, Maricopa Unified School District #20, Mercer Island School District, Millburn Township Public Schools, Omaha Public Schools, Peoria Public Schools District 150, Queen Anne's County Public Schools, and Sublette County School District #9.

[232] Compare: Data Analytics Functions (six districts) (*see supra* Part IV.C.1); Student Reporting Functions (four districts) (*see supra* Part IV.C.2); Guidance Functions (five districts) (*see supra* Part IV.C.3); and Special School Functions (five districts) (*see supra* Part IV.C.4). *See also infra* Part IV.C.6 (discussing Classroom Functions—also ten districts).

vendors: the ten districts used thirteen different vendors covering a total of fifteen agreements.[233] The classroom function category was the only group that had a wider range of service agreements.[234] There are two possible explanations for the increase in both responding districts and agreements produced by those districts in the context of hosting, maintenance, and backup outsourcing. One explanation is that districts outsource hosting, maintenance, and backup functions more frequently than they outsource data analytics, student reporting, guidance, or special school functions. A second related explanation is that hosting, maintenance, and backup functions are more readily identifiable with regard to the request for documents, and therefore districts were more apt and able to supply Fordham CLIP with agreements for these services.

b. Contracts

For districts to outsource educational record information for hosting, maintenance, and backup, FERPA requires that districts have written agreements with the vendors.[235] Of the fifteen hosting, maintenance, and backup agreements, almost all (86%) involved direct contracts between districts and vendors.[236] These agreements were more complete than those in the other categories: of the fifteen agreements, 80% were complete and only three were missing documentation.[237]

Districts, though, were not particularly vigilant in assuring means to verify that vendors comply with their contractual obligations. Only two of the agreements (13%) included a clause giving the district a contractual right to audit and inspect the vendor's practices with respect to the transferred data.[238]

c. Types of Student Identifying Data Transferred from Districts to Vendors

For hosting, maintenance, and backup services that include educational records protected by FERPA, the statute requires district contracts to specify the types of data being transferred.[239]

---

[233] The vendors are: Schoolwires, Inc.; esri; Gaggle; Interactive Educational Services, Inc.; Washington School Information Processing Cooperative; Northwest Educational Service; Enterprise Management Service; Edline, LLC; TIENET; Infinite Campus; Houghton Mifflin Harcourt; Performance Matters; and Scholastic, Inc.
[234] The largest set of agreements for the outsourcing of a particular function contains twenty-two, which represents agreements for the outsourcing of classroom functions. *See infra* Part IV.C.6. Compare: Data Analytics (nine agreements) (*see supra* Part IV.C.1); Student Reporting (five agreements) (*see supra* Part IV.C.2); Guidance (six agreements) (*see supra* Part IV.C.3); and Special School Functions (nine agreements) (*see supra* Part IV.C.4).
[235] 20 U.S.C. § 1232g(b)(1)(A).
[236] Those agreements are Agreement Documents Nos. 31, 32, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, and 44. Note that the two agreements that did not represent a direct contract between a district and the vendor— Agreement Document No. 33 and Agreement Document No. 45—were coded as such because those did not make clear the parties to each agreement.
[237] The full agreement terms of Agreement Document No. 31 were not supplied to Fordham CLIP. The Master Agreement referenced by Agreement Document No. 32 was not supplied to Fordham CLIP. Finally, the Standard Terms and Conditions, Additional Terms, Privacy Policy, and Terms of Use referenced by Agreement Document No. 38 were not supplied to Fordham CLIP.
[238] Agreement Document No. 36 provides that all data supplied remains the property of the school district, which could also be construed as providing a right of audit or inspection. *See* Agreement Document No. 36 at 3. Agreement Document No. 40 provides the district, "at all times…with the right to audit [the vendor's] compliance with [confidentiality obligations under the agreement]." *See* Agreement Document No. 40 at 7.
[239] *See, e.g.*, 34 C.F.R. § 99.35(a)(3)(A).

The agreements, however, rarely specified the types of identifying student data being transferred. The table below summarizes the contract descriptions:

TYPE OF DATA TRANSFERRED		
Type of Data Specified	**Total (out of 15)**	**Percentage**
Name	3	20.0%
Address	3	20.0%
Sex	0	0.0%
ID	0	0.0%
Age/Grade	1	6.7%
Biometric	0	0.0%
Medical/Health	0	0.0%
Socio-Economic	0	0.0%
Transaction Data	2	13.3%

Eleven of the agreements (more than 70%) did not specify the transfer of any student data at all. The four that did provide the required specifications only disclosed isolated elements.[240]

While it is unlikely that vendors providing system maintenance services require the collection and transfer of student information, vendors providing hosting and data backup services would, in fact, be likely to receive identifying data and be subject to stating the data needs in the agreements.

d. Data Control: Sharing, Mining, and Redisclosure

District control over data transferred in the context of hosting, maintenance, and backup services is critical for ensuring privacy and is required by FERPA when districts outsource to agents activities that the districts would otherwise perform in-house.[241] If vendors do not have contractual limits on sharing, mining, and redisclosure of hosted and backed-up data, then districts have relinquished control over their students' data. The contractual provisions preserving data control found in the various hosting, backup and maintenance agreements are summarized below:

[240] For example, Agreement Document No. 31 specified only the transfer of student name, address, and age/grade. *See* Agreement Document No. 31 at 1, 2. Agreement Document No. 33 specified only that transaction data was collected and analyzed. *See* Agreement Document No. 33 at 3. Similarly, Agreement Document No. 38 specified the collection of transaction data as well as student name and address. *See* Agreement Document No. 38 at 2. Finally, Agreement Document No. 42 specified only the transfer of student name and address. *See* Agreement Document No. 42 at 1.

[241] *See* 34 C.F.R. § 99.31(a)(1)(i)(B) (requiring that third-party vendors performing tasks as "school officials" be "under the direct control of the . . . institution with respect to the use and maintenance of educational records").

DATA CONTROL: LIMITS ON SHARING, DATA, AND REDISCLOSURE		
	Total (out of 15)	**Percentage**
Document Prohibits or Limits Redisclosure	8	53.3%
District Retains Exclusive Control of Data	2	13.3%
District Retains Audit and Inspection Rights Respecting Vendor	2	13.3%
District Retains Right to Determine Data Access Based on User Role	4	26.7%
Document Specifies Audit/Evaluation Purpose for Disclosure	0	0.0%
Data Used for: Sale/Marketing of Instructional Materials, Student Recognition, College, Military, or Low-Cost Literary Materials	0	0.0%
Disclosure Allowed for Heath, Safety, or Emergency Purpose	0	0.0%
Document Prohibits Sale and Marketing of Data	1	6.7%
Foreign Storage Prohibited	0	0.0%
Access by Other Government Agencies Prohibited	0	0.0%

As illustrated by the content of the agreements, districts do not effectively retain rights to control their data when the information is transferred for hosting, maintenance, and back up. Only two agreements (13%) appeared to give exclusive control to the district.[242] Approximately 25% of the agreements provided explicit rights for districts to determine access to the transferred data.[243] But, these provisions were often ambiguous as to the scope of the district's ability to determine access to and control of data.[244]

Barely half of the agreements (eight) prohibit or limit the redisclosure of student data.[245] Only one of the agreements (7%) expressly prohibited the vendor from selling or using the

[242] Agreement Document No. 36 provides that no district records shall be redisclosed without the district's written consent. *See* Agreement Document No. 36 at 3. Agreement Document No. 41 provides that the district is responsible for data content and controls on data access and use. *See* Agreement Document No. 41 at 23.

[243] Agreement Document No. 31 provides that the school may determine which web features may be used and which individuals or groups have particular levels of access privilege. *See* Agreement Document No. 31 at 3. Note that this statement is ambiguous with respect to the term "individuals or groups," as such could be interpreted to mean either only those individuals or groups acting on behalf of the school, or alternatively, all individuals or groups—including those employed by the vendor or acting on the vendor's behalf. Agreement Document No. 41 provides that the district is responsible for data content and controls on data access and use. *See* Agreement Document No. 41 at 23. Note that this statement, too, is ambiguous. On the other hand, Agreement Document No. 42 provides that the school has primary authority over who can register for, use, and gain access to personal information posted on the website. *See* Agreement Document No. 42 at 1. Finally, Agreement Document No. 43 provides for client selection and assignment based on access and security needs. *See* Agreement Document No. 43 at 2.

[244] *See, e.g.*, *supra* note 243 (describing select contractual provisions addressing the district's right to determine control access to collected data).

[245] Agreement Document No. 31 provides that data will not be disclosed to third parties without written consent, unless otherwise allowed by FERPA. *See* Agreement Document No. 31 at 3. It also provides that disclosure may be made if required by law, to those with administrative privilege, or to business transaction service providers as required. *See id.* at 5. Agreement Document No. 33 provides that disclosure of information is limited to only web site partners; alternatively, the vendor may disclose aggregated user data. *See* Agreement Document No. 33 at 3. Agreement Document No. 36 provides that disclosure will not be made without the written consent of the district. *See* Agreement Document No. 36 at 3. Agreement Document No. 38 provides that the vendor may disclose information to government agencies as required by law, as well as to the subscribing school. *See* Agreement Document No. 38 at 2. Agreement Document No. 40 provides that information received from the district—specifically student data—is confidential and shall not be made available to any third party. *See* Agreement Document No. 40 at 6. Agreement Document No. 41 provides that confidential information will not be made available to third parties for purposes other than the implementation of the agreement. *See* Agreement Document No. 41 at 15. Agreement Document No. 42 prohibits redisclosure to third parties without the consent of a parent, the school, or the eligible student unless otherwise permitted by FERPA. *See* Agreement Document No. 42 at 3.

received data for marketing purposes.[246] Approximately 45% of hosting, maintenance, and backup services are thus not prohibited from re-purposing and re-using data they receive from districts—including for marketing purposes. In essence, this means that many districts will not be able to comply with FERPA obligations in connection with their hosting, maintenance, and back up functions where their contracts do not bar data mining and re-use. In addition, for those agreements that do prohibit or limit redisclosure, the language is often ambiguous or subject to many exceptions.[247]

Lastly, districts further relinquish control when they allow vendors to change the terms of any privacy commitments. Approximately one-third of the agreements (five) contained a provision prohibiting vendors from unilaterally amending the agreement.[248] However, six of the remaining agreements (40%) explicitly allowed the vendors to unilaterally modify the contractual terms without notice to the district,[249] while four agreements were silent on the matter.[250] Where the vendor can modify the terms unilaterally, districts may lose control of any data that they have transferred under the agreement.

e. Parental Notice, Consent, and Access to Collected Data

The hosting, maintenance, and backup agreements fared poorly with respect to parental notice concerning the storage of student information. Most of the agreements also failed to reserve to the district a right to allow for parental access to and correction of the data transferred to and held by the vendor. These terms of the agreements are summarized in the following table:

Agreement Document No. 44 provides that the district's data remains its own property and that the vendor agrees not to use such data for purposes beyond those necessary to execute the obligations of the agreement. *See* Agreement Document No. 44 at 1.

[246] Agreement Document No. 40 provides that information received from the district, specifically including student data, is confidential and shall not be made available to any third party. It also provides that such information shall not be used for purposes other than to perform its obligations under the agreement. *See* Agreement Document No. 40 at 6.

[247] *See, e.g.*, *supra* note 243.

[248] Agreement Document No. 35 provides a unilateral right to amend, but only as to the amount of fees and not to other terms and conditions. Agreement Document No. 36 provides that it may only be modified or amended with the mutual consent of the parties. *See* Agreement Document No. 36 at 4. Agreement Document No. 40 provides that it "shall not be amended or modified except in writing by duly authorized representatives of the parties that specifically refer to [the agreement]." *See* Agreement Document No. 40 at 20. Agreement Document No. 41 provides that it may only be modified or amended with the mutual consent of the parties. *See* Agreement Document No. 41 at 2–3. Agreement Document No. 44 provides that it may only be modified by a written instrument executed by both parties. *See* Agreement Document No. 44 at 2.

[249] Agreement Document No. 31 provides that changes to the Privacy Policy are posted to the vendor's website only. *See* Agreement Document No. 31 at 6. Agreement Document No. 33 provides that the vendor may revise the agreement without notice and posts updated changes on the service's website only. *See* Agreement Document No. 33 at 3. Agreement Document No. 38 provides: "[the vendor] reserves the right to change this Service at any time, for any reason, and without notice, including the right to terminate these services." *See* Agreement Document No. 38 at 1. Agreement Document No. 42 provides that the Terms of Use may be changed without notice, but if a material change is made to the Privacy Policy, the school must obtain new consent from parents of students under 13 years of age. *See* Agreement Document No. 42 at 1, 6. Agreement Document No. 43 provides that vendor's the Terms of Service may be modified with notice posted online only. *See* Agreement Document No. 43 at 3. Agreement Document No. 45 provides that "it may be modified or updated by the [vendor]." *See* Agreement Document No. 45 at Para. 11.

[250] Agreement Document Nos. 32, 34, 37, and 39 contained no provision addressing amendment.

NOTICE, CONSENT, ACCESS, AND TRANSPARENCY		
	Total (out of 15)	**Percentage**
Document Provides (for) Parental Notice	1	6.7%
Document Provides (for) Parental Consent	2	13.3%
District Can Provide Parental Access to, Correction of Data	2	13.3%
Parents Activate Account with Vendor Directly	0	0.0%

Of the fifteen agreements, only one provided that district must notify parents that the service is used or that student data is transferred.[251] That same agreement provided that parents must consent to the district's use of the service as it pertains to their child.[252] Another agreement required that parents consent to the creation of a back-up account for their child, but did not address notice of the service.[253] In effect, these services are non-transparent for parents.

Additionally, only two of the agreements (13%) enabled the district to provide parents and eligible students with the right to access and correct student data.[254] This generalized absence of a provision assuring that parents will have access and an ability to correct erroneous student data is problematic because these rights are central components of FERPA.[255]

f. COPPA Obligations

The hosting, maintenance, and backup agreements provided that a child may supply personally identifiable information or be tracked more frequently than agreements for other types of services. These findings are illustrated by the following table:

COPPA OBLIGATIONS		
	Total (out of 15)	**Percentage**
Service Enables Child to Supply PII	3	20.0%
Service Enables Child to Be Tracked	2	13.3%

Of the fifteen agreements, three (20%) specified that the service allows children to supply personally identifiable information.[256] Two (13%) indicated that the service enables a child to be

---

[251] Agreement Document No. 42 provides that parents or guardians of minors using the service must read and agree to the Terms of Use before the minor may use the website. *See* Agreement Document No. 42 at 1.
[252] *See supra* note 251.
[253] Agreement Document No. 33 provides that schools must obtain parental consent before issuing accounts to students. *See* Agreement Document No. 33 at 4.
[254] Agreement Document No. 31 requires that the district give parents access to view the profiles of children under 13. *See* Agreement Document No. 31 at 2, 3. Agreement Document No. 42 allows the school to provide parents with access to their child's personally identifiable information and to permit parental correction and deletion of such data. *See* Agreement Document No. 42 at 2.
[255] *See supra* Part II.A.2.
[256] Agreement Document No. 38 provides that the service maintains bulletin boards, message forums, and similar features to which students may post content and cautions students to not share personally identifiable information in such places because it may be tracked by other users. *See* Agreement Document No. 38 at 4. Agreement Document No. 42 provides that the service allows users to post and share content on social media and message boards and that such information might be tracked by other users. *See* Agreement Document No. 42 at 2–7. However, registration for the service requires verification of birth date, which allows the vendor to filter out users who are under 13 unless such users have obtained appropriate parental consent. *See id.* at 1–2. Agreement Document No. 31 provides that the service allows users to post, download and upload content, and engage in "social media" only if appropriate parental consent is given. *See* Agreement Document No. 31 at 1–3.

tracked. At the same time, only two agreements required parental consent,[257] reflecting that satisfaction of COPPA requirements is not included in all the services that collect data from students and track them.

g. Data Security

The hosting, maintenance, and backup agreements addressed data security more frequently than the other types of contracts. Clauses that were included in the agreements are summarized in the following table:

DATA SECURITY		
	Total (out of 15)	**Percentage**
Data Deleted or Destroyed at End of Contract Period	2	13.3%
Non-Specified Security Obligation	9	60.0%
Encryption Level Specified	3	20.0%
NIST Level Specified	1	6.7%
Data Breach Notification Specified	2	13.3%

Two of the fifteen hosting, maintenance, and backup agreements contained a provision specifying that data be deleted or destroyed at the end of the contract period.[258] This is disappointing, as FERPA generally requires the destruction or deletion of data after it is no longer needed for the purpose for which the data was originally transferred.[259] One explanation for the lack of such provisions may be that these agreements require districts to simply "click-through" a terms of use, privacy policy, or other terms on the Internet. Regardless, districts should be wary of entering into agreements that do not require the vendor to delete, destroy, or return transferred data at the end of the contract term.

Of the fifteen agreements, ten (66%) specified some type of security obligation on the part of the vendor.[260] The remaining third of the contracts were silent and contained no security obligations. For those contracts that required data security, six (40%) contained a general security obligation[261] and four more (27%) required specific encryption levels or standards,[262] including one contract that specified a NIST level.[263]

---

[257] Agreement Document No. 42 provides that parents or guardians of minors using the service must read and agree to the Terms of Use before the minor may use the website. *See* Agreement Document No. 42 at 1.

[258] Agreement Document No. 31 provides that at the termination of the agreement, data is not retained except as necessary to comply with any legal obligations. *See* Agreement Document No. 31 at 4. Agreement Document No. 40 provides that at termination of the agreement, all data be returned or destroyed within ten days of contract termination and that a written certification be provided to confirm that such has been accomplished. *See* Agreement Document No. 40 at 7.

[259] *See supra* note 147.

[260] Those agreements are Agreement Documents Nos. 31, 33, 36, 37, 38, 40, 41, 42, 43, and 44.

[261] Agreement Document No. 31 provides that the vendor uses physically secure data storage locations, password controls, and limited access servers to protect data. *See* Agreement Document No. 31 at 6. Agreement Document No. 33 provides that the vendor uses a "variety of measures" to protect data. *See* Agreement Document No. 33 at 4, 6. Agreement Document No. 36 provides that the vendor will use reasonable security procedures to assure that district material is not disclosed. *See* Agreement Document No. 36 at 3. Agreement Document No. 37 provides that the vendor uses automated backup and recovery features. *See* Agreement Document No. 37 at 3. Agreement Document No. 40 provides that vendor will "implement and maintain administrative, physical, and technical safeguards to ensure" confidentiality and security. *See* Agreement Document No. 40 at 6. Agreement Document No. 41 provides that the vendor uses virus protection, backups and recovery, storage and security, and monitoring

Finally, only two of the agreements (13%) required the vendor to notify the district in the event that the vendor's security measures are breached or data is otherwise compromised.[264] This absence of express contractual provisions ensuring breach notification handicaps districts in the event of inadvertent disclosures or wrongful access to their children's data.

6. Classroom Functions

a. Prevalence

Of the twenty responding districts, half outsource classroom functions to third party vendors.[265] The ten districts produced a combined total of twenty-two agreements representing fifteen different vendors.[266] This represents the largest category of identified cloud service use by districts, both with respect to the number of districts and the total number of contracts. The frequency of districts reporting that they outsource classroom functions may be due to the nature of these services. Alternatively, these functions may have been more readily identifiable for the districts responding to the request for documents.

b. Contracts

FERPA permits districts to outsource information from educational records to service providers acting as "school officials" performing institutional services or functions on behalf of

---

procedures to ensure data security. *See* Agreement Document No. 41 at 11. Agreement Document No. 42 agreement provides that the vendor "takes security seriously and employs reasonable security measures and procedures" and that the information is maintained "in a physical environment that utilizes industry-standard security measures." *See* Agreement Document No. 42 at 6. Agreement Document No. 43 provides that the vendor offers communications back-up and spam/virus protection. *See* Agreement Document No. 43 at 3. Finally, Agreement Document No. 44 provides that the vendor uses "commercially reasonable security measures," including firewalls, encryption, passwords, and virus protection to protect data. *See* Agreement Document No. 44 at 1.

[262] Agreement Document No. 37 provides that the vendor uses three encryption levels: 448-bit Blowfish encryption, 256-bit AES encryption, and 128-bit online-banking encryption. *See* Agreement Document No. 37 at 3. Agreement Document No. 38, on the other hand, provides that the vendor uses "industry standard" SSL encryption. *See* Agreement Document No. 38 at 1. Similarly, Agreement Document No. 44 provides that the vendor uses "commercially reasonable security measures," including firewalls, encryption, passwords, and virus protection. *See* Agreement Document No. 44 at 1.

[263] In addition to establishing a general security obligation, Agreement Document No. 40 also provides that NIST security standards must be maintained. *See* Agreement Document No. 40 at 28.

[264] Agreement Document No. 40 provides that vendor immediately report any security incident, real or suspected, to the district involving its data. *See* Agreement Document No. 40 at 6. Agreement Document No. 43 provides that the vendor notifies the customer using "reasonable effort" in the event of a data breach. *See* Agreement Document No. 43 at 1.

[265] The ten districts are: Jefferson City Public Schools, Jefferson County Public Schools (CO), Jefferson County Public Schools (KY), London City Schools, Maricopa Unified School District #20, Mercer Island School District, Millburn Township Public Schools, Omaha Public Schools, Queen Anne's County Public Schools, and San Luis Coastal Unified School District.

[266] The services are: Edmodo; Google Apps for Education; Schoolmessenger Messaging Services; Schoology Learning Management System; Apex Learning, Inc.; Blackboard Learn; SuccessMaker (Pearson); mclanguage360 (Proximity Learning); Learning A–Z; Microsoft Office 2013; Rosetta Stone; Study Island (Edmentum); Opentext FirstClass Messaging Service; Schoolwires, Inc.; and My Big Campus.

the school.[267] In this situation, FERPA requires that the vendor be under the direct control of the district.[268] Student data collected in the context of classroom functions, however, may not qualify as "educational records."[269] For example, a cloud service that enables students to store class projects online or work collaboratively on the stored project will generate content and transactional data about the students. That data is not likely to meet the definition of an "educational record."

Fifty-five percent (12) of the classroom function agreements were fully executed contracts between districts and vendors.[270] Others required only that the district "click-through" online terms of use or service and did not indicate who executed the agreement or when the agreement was executed. Over three quarters of the agreements were complete as provided; four were incomplete.[271]

Six of the twenty-two agreements (27%) offered the service to districts free of charge.[272] This means that the personal information of students is likely being commercialized in some way to support the provision of the service to the district.

Like in the other categories, the overwhelming majority of agreements failed to include safeguards for vendor compliance. Only two (10%) of the classroom function agreements gave the district a contractual right to audit and inspect the vendor's practices with respect to the transferred data.[273]

c. Types of Student Identifying Data Transferred from Districts to Vendors

The agreements for classroom functions infrequently specified the type of identifying data being transferred for the services. FERPA, however, requires the specification of data being transferred to authorized representatives.[274] Further, without a specification of the identifying information at issue, the agreement leaves vendors vulnerable to unrealized COPPA issues, as

[267] *See* 34 C.F.R. § 99.31(a)(1)(i)(B) (authorizing contractors to be considered as "school officials" under specified conditions).
[268] 34 C.F.R. § 99.33(a)(1)(i)(B)(2).
[269] *See supra* Part II.A.1 for a discussion of "educational record."
[270] Those agreements are Agreement Documents Nos. 47, 48, 49, 50, 51, 53, 55, 57, 59, 60, 61, and 62.
[271] The Terms of Service, Privacy Policy, and Acceptable Use Policy referenced by Agreement Document No. 46 were not supplied to Fordham CLIP. The Privacy Policy referenced by Agreement Document No. 59 was not supplied to Fordham CLIP. The Standard Purchase and License Terms and Privacy Policy referenced by Agreement Document No. 60 were not supplied to Fordham CLIP. Finally, the Privacy Policy referenced by Agreement Document No. 61 was not supplied to Fordham CLIP.
[272] Agreement Document No. 46 provides that the basic services are provided free of charge. *See* Agreement Document No. 46 at 7. Agreement Document No. 54 provides that the initial term is provided free of charge. *See* Agreement Document No. 54 at 12–13. Agreement Document No. 55 provides that the service is free during its initial term. *See* Agreement Document No. 55 at 8. Similarly, Agreement Document No. 63 (from the same vendor) provides that the service is provided free of charge for the initial term. *See* Agreement Document No. 63 at 2. Finally, Agreement Document No. 64 provides that the basic service is provided free of charge. *See* Agreement Document No. 64 at 6.
[273] Agreement Document No. 50 provides that the board of education retains the right to inspect or audit all accounting reports, books, or records concerning the vendor's performance of the service. *See* Agreement Document No. 50 at 5. Agreement Document No. 59 provides that one may request a copy or send a correction of the personal information held by the vendor through email or mail. *See* Agreement Document No. 59 at 3.
[274] *See* 34 C.F.R. § 99.35(a)(3)(A).

COPPA may apply to some of the functions.[275] The findings are illustrated in the following table:

TYPE OF DATA TRANSFERRED		
Type of Data Specified	**Total (out of 22)**	**Percentage**
Name	6	27.3%
Address	6	27.3%
Sex	1	4.5%
ID	0	0.0%
Age/Grade	3	13.6%
Biometric	0	0.0%
Medical/Health	0	0.0%
Socio-Economic	0	0.0%
Transaction Data	3	13.6%

Sixty-three percent of the agreements did not specify at all what identifying student data was transferred. The remaining 37% specified some types of identifying information, with name and address specified most frequently.[276] In light of the nature of these services, it seems likely that vendors of services intended for student-interactive, classroom, or at home use might require more student data than what is reflected in these agreements. Indeed, almost 14% of the agreements do include mention of student transaction data.

d. Data Control: Sharing, Mining, and Redisclosure

As indicated previously, districts must retain control over data mining and redisclosure when they share student information for compliance with FERPA in the case of "educational records" and for fair information practice in the case of data not covered by FERPA.[277] Without control over the data, districts cannot assure that student information will be handled properly and in accordance with permissible uses. To the extent that data for classroom functions qualifies as educational record information, districts will be required to have direct control over the vendors. The following table presents a summary of the contractual clauses addressing data control:

[275] COPPA applies to websites that collect personal information directly from children under 13. Consequently, if an online service provider collects identifying information directly from children under that age, parental notice and consent are required. *See supra* Part II.C.

[276] For example, Agreement Document No. 46 specifies the transfer of only student name and address. *See* Agreement Document No. 46 at 2–3. Agreement Document No. 52 specifies the transfer of only student name and address. *See* Agreement Document No. 52 at 1. Agreement Document No. 56, on the other hand, specifies the transfer of student name, address, age/grade, and transaction data—though the provision of such information is completely voluntary with respect to this vendor. *See* Agreement Document No. 56 at 2. Agreement Document No. 59 specifies the transfer of only transaction data. *See* Agreement Document No. 59 at 3. Agreement Document No. 60 specifies that student name, age/grade, and transaction data was to be transferred. *See* Agreement Document No. 60 at 1. Agreement Document No. 64 agreement specifies the transfer of student name, address, and sex—a type of student data not specified as being transferred in the vendor's agreement with another district. *See* Agreement Document No. 64 at 2; *see also* Agreement Document No. 46 (representing an agreement between the same vendor and a different district). Finally, Agreement Document No. 67 specifies the transfer of only the student's name. *See* Agreement Document No. 67 at Para. 2(a).

[277] *See generally* Appendix B.

DATA CONTROL: LIMITS ON SHARING, MINING, AND REDISCLOSURE		
	Total (out of 22)	**Percentage**
Document Prohibits or Limits Redisclosure	16	72.7%
District Retains Exclusive Control of Data	1	4.5%
District Retains Audit and Inspection Rights Respecting Vendor	2	9.1%
District Retains Right to Determine Data Access Based on User Role	4	18.2%
Document Specifies Audit/Evaluation Purpose for Disclosure	0	0.0%
Data Used for: Sale/Marketing of Instructional Materials, Student Recognition, College, Military, or Low-Cost Literary Materials	0	0.0%
Disclosure Allowed for Heath, Safety, or Emergency Purpose	0	0.0%
Document Prohibits Sale and Marketing of Data	1	4.5%
Foreign Storage Prohibited	0	0.0%
Access by Other Government Agencies Prohibited	0	0.0%

As a threshold, close to 75% of the agreements for classroom functions prohibited or limited the redisclosure of student data or other confidential information.[278] This matches

[278] Agreement Document No. 46 provides that personal information is not rented or sold, but is shared with affiliate businesses as necessary to fulfill business transactions with the vendor, the vendor's agents (only to the extent necessary for them to assist the vendor), and as required by law. *See* Agreement Document No. 46 at 6, 7. Agreement Document No. 47 provides that the vendor will not disclose confidential information except to affiliates, employees, or agents with a need to know and who are bound by confidentiality agreements. *See* Agreement Document No. 47 at 3. Disclosure is made only for the purpose of exercising the rights and obligations of the agreement, or as otherwise required by law. *See id.*. Agreement Document No. 49 provides that student data is confidential and the vendor will use it only as necessary to render its services. *See* Agreement Document No. 49 at 6. Agreement Document No. 50 provides that the vendor agrees to not disclose information to third parties except as required by law. *See* Agreement Document No. 50 at 3. Agreement Document No. 51 provides that redisclosure of confidential information is made only to employees or agents who have signed a nondisclosure agreement and who have a need to know in connection with the original agreement. *See* Agreement Document No. 51 at 1. Agreement Document No. 52 provides that personal information will not be disclosed to third parties, but that it will be disclosed to other companies within the company, or as required by law. *See* Agreement Document No. 52 at 1. Agreement Document No. 54 provides that the vendor will not redisclose confidential information except to "authorized personnel" (as described in the agreement) who are bound by a nondisclosure agreement, or otherwise as required by law. *See* Agreement Document No. 54 at 6–7, 14. Agreement Document No. 55 provides that confidential information will not be disclosed except to employees or affiliates with a need to know and who have signed a confidentiality agreement, or otherwise as required by law; the vendor also agrees to function as a "school official," per FERPA. *See* Agreement Document No. 55 at 7. Agreement Document No. 56 only provides that aggregate demographic information is not shared. *See* Agreement Document No. 56 at 2. Agreement Document No. 60 provides that the vendor will not redisclose confidential information without prior written consent unless it is required to do so by law. *See* Agreement Document No. 60 at 3. Agreement Document No. 61 provides that the vendor will not redisclose confidential information unless required by law. *See* Agreement Document No. 61 at 3. Agreement Document No. 63 provides that the vendor will not disclose confidential information except to affiliates, employees, or agents with a need to know and who are bound by confidentiality agreements, and even then only for the purpose of exercising the rights and obligations of the agreement, or as otherwise required by law. *See* Agreement Document No. 63 at 3. Agreement Document No. 64 provides that the vendor shares aggregate information with its partners. *See* Agreement Document No. 64 at 3. That agreement also provides that data is not rented or sold. *See id.* at 3. According to the agreement, data is shared with other businesses, but only to the extent that it relates to user activity with that business. *See id.* at 4. Data is also shared as required by law under the agreement. *See id.* at 5. Agreement Document No. 65 provides that the vendor rediscloses information according to FERPA or as required by law. *See* Agreement Document No. 65 at 4, 7. Disclosure is also made to users who have been assigned "administrative privileges" by the school and to "trusted businesses and contractors [who] provide certain services which support [the vendor's] provision and hosting of the Website or otherwise support the operation of the associated online services." *See id.* at 6–7. The vendor also discloses aggregate, de-identified

FERPA's required ban on redisclosure of student data absent parental consent.[279] However, provisions in many of these classroom function agreements were often ambiguous or subject to exceptions permitting redisclosure.[280] Only one of the twenty-two agreements (4.5%) expressly prohibited the vendor from selling or using for marketing purposes the student data it receives.[281] And, fewer than 5% of the classroom function agreements stipulated that districts retain ownership control of transferred data.[282]

With respect to determinations of access to data transferred for classroom functions, fewer than 20% of the agreements vested the district with the right to determine access to the data based on a user's role.[283] For those agreements that did reserve the right to districts, the provisions were often ambiguous as to the scope of the district's ability to determine access and control.[284] None of the classroom functions agreements prohibited foreign storage of student data or prohibited access to transferred student data by other government agencies.

Lastly, and particularly troubling, the majority—twelve of the twenty-two classroom functions agreements—expressly permitted vendors to unilaterally modify the contractual terms without notice to the district.[285] Only seven of the agreements (32%) contained a provision

---

information for use "in any way." *See id.* at 9. Agreement Document No. 66 provides that the parties agree not to disclose each other's confidential data except to affiliates, employees, and agents with a need to know and who have agreed in writing to keep such data confidential. *See* Agreement Document No. 66 at 3. Finally, Agreement Document No. 67 provides that the vendor never promotes, sells, or discloses personally identifiable information to third parties. *See* Agreement Document No. 67 at 1.

[279] *See* 20 U.S.C. § 1232g(b)(4)(B) ("[P]ersonal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student.").

[280] *See supra* note 278.

[281] Agreement Document No. 67 provides that the vendor will never promote, sell, or disclose personally identifiable information to third parties. *See* Agreement Document No. 67 at 1.

[282] Agreement Document No. 50 provides that the board of education retains ownership in any reports, data, or information prepared or assembled by the vendor. *See* Agreement Document No. 50 at 4.

[283] Agreement Document No. 46 provides that different levels of user access can be created using access codes. *See* Agreement Document No. 46 at 3. Note that this provision is unclear as to whether it applies to only district personnel or to the vendor's employees as well. Similarly, Agreement Document No. 55 vaguely provides that the customer is empowered to designate administrators (though this likely is meant to refer to administrators of the service within the district). *See* Agreement Document No. 55 at 5. Agreement Document No. 57 provides that advanced user management allows control over a user's access and privileges on a granular level. *See* Agreement Document No. 57 at 2. Finally, Agreement Document No. 65 provides that the site administrator assigns roles and access after registration. *See* Agreement Document No. 65 at 2–3. This, too, likely refers to an administrator of the service as it is used by the district.

[284] *See, e.g.*, *supra* note 283.

[285] Agreement Document No. 46 provides that changes to the Terms of Service are posted on the website and are only possibly delivered by email. *See* Agreement Document No. 46 at 1, 7. Additionally, the Privacy Policy may change with email notification or web posting. *See id*. at 10. Agreement Document No. 47 provides that the vendor reserves the right to make commercially reasonable modifications either with or without notice. *See* Agreement Document No. 47 at 1. Agreement Document No. 52 provides that the Privacy Statement and Terms of Use may be modified from time to time, with notice of modification posted on the vendor's website. *See* Agreement Document No. 52 at 1. Agreement Document No. 54 provides that the vendor reserves the right to make commercially reasonable modifications either with or without notice. *See* Agreement Document No. 54 at 12. Agreement Document No. 56 provides that changes to the Privacy Statement will be posted on the vendor's homepage. *See* Agreement Document No. 56 at 3. Agreement Document No. 58 provides that vendor "might occasionally update" its Privacy Statement. *See* Agreement Document No. 58 at 11. Agreement Document No. 60 provides that the Privacy Policy may change "from time to time" and such changes will be posted on the vendor's website. *See* Agreement Document No. 60 at 3. Agreement Document No. 61 provides that the vendor reserves the right to change its privacy terms by posting notification of such changes online. *See* Agreement Document No. 61 at 8.

prohibiting the vendor from unilaterally amending the agreement.[286] Of the remaining 20% of the classroom function agreements, two still allowed the vendor to unilaterally amend the agreement as long as notice is provided to the district,[287] and two agreements were silent on the matter.[288] In effect, the overwhelming ability of vendors to unilaterally change the terms of their contracts with the districts means that districts cannot contractually retain control over their classroom function data.

e. Parental Notice, Consent, and Access to Data Collected

The classroom function agreements did not clearly address parental notice or consent. Most of the agreements failed to reserve to the district a right to allow for parental access to and correction of the data that is transferred to vendors. None of the agreements stipulated that the services require parents to activate an account with the vendor directly. These findings are illustrated by the following table:

NOTICE, CONSENT, ACCESS, AND TRANSPARENCY		
	Total (out of 22)	**Percentage**
Document Provides (for) Parental Notice	8	36.4%
Document Provides (for) Parental Consent	9	40.9%
District Can Provide Parental Access to, Correction of Data	2	9.1%
Parents Activate Account with Vendor Directly	0	0.0%

Thirty-six percent of the agreements included clauses allocating responsibility to districts to notify parents that the service is used or that student data is transferred.[289] Those same

---

Agreement Document No. 63 provides that material changes may be made with email notice to the system administrator or by a notification on the service's admin console. *See* Agreement Document No. 63 at 1. Agreement Document No. 64 provides that notice of changes or amendments is posted on the vendor's website and is also possibly emailed to the customer's system administrator. *See* Agreement Document No. 64 at 1, 6. Agreement Document No. 65 provides that notice of changes to the Privacy Policy is not provided to the end user, but is provided on the school's website. *See* Agreement Document No. 65 at 1, 8. Agreement Document No. 67 provides that the vendor reserves the right to alter the Terms of Use at its discretion. *See* Agreement Document No. 67 at 4–5.

[286] Those agreements are Agreement Documents Nos. 49, 50, 51, 53, 55, 62, and 66.

[287] Agreement Document No. 55 provides that URL terms and services are amendable with notice to the customer via email or via notification on the admin console. *See* Agreement Document No. 55 at 3. Agreement Document No. 59 merely "encourage[s] . . . periodic[ ] review" of the privacy statement "as it may change at any time." *See* Agreement Document No. 59 at 1.

[288] Agreement Documents Nos. 48 and 57 did not address amendment.

[289] Agreement Document No. 46 provides that parents must read and agree to the Terms of Service and give consent for use by students under the age of 18. *See* Agreement Document No. 46 at 1, 2. Agreement Document No. 50 requires that the district obtain any "necessary parental consent for each Client User student to access and use the [vendor's] [c]ourses." *See* Agreement Document No. 50 at 2 . Agreement Document No. 52 provides that students under the age of 18 must read the Online Privacy Statement with a parent or guardian. *See* Agreement Document No. 52 at 1. The Privacy Policy referenced by Agreement Document No. 60 provides general notice of the vendor's policies to parents. *See generally* Agreement Document No. 60 . Agreement Document No. 61 includes a parent/guardian notification letter that informs parents/guardians that the district implements the service. *See* Agreement Document No. 61 at 1. Agreement Document No. 63 (between the same vendor and a different district) provides that parental consent is required for use of the service when "necessary." *See* Agreement Document No. 63 at 2, 4 . The Parent Notification letter referenced by Agreement Document No. 64 provides parents with notice that the school uses the service. *See* Agreement Document No. 64 at 1. The agreement provides that parents of students

agreements provided that the district also obtain parental consent, as did one additional agreement.[290] It is surprising that so few classroom functions agreements required parental notice and consent, as these services are intended for direct student interaction. The lack of contractual provisions requiring or providing for parental notice and consent in classroom functions agreements is problematic, as the parental rights to notice of and consent to the transfer of student information are central tenets of FERPA, and are excepted only in limited circumstances.[291] Similarly, to the extent that classroom function services will collect information directly from school children under 13 years old, COPPA may require vendors to obtain parental consent. In fact, none of the agreements indicated that parents would have to activate an account with the vendor for children's access.

With respect to data access, only two the agreements (9%) gave districts rights that would enable the districts to provide parents and eligible students with the right to access and correct student data.[292] In the context of classroom functions agreements, it is surprising that so few of the agreements allow for a parental right to access and correct student data, as such is also a central component of FERPA.[293]

f. COPPA Obligations

COPPA may apply to vendors collecting personal information directly from children under 13 through classroom function services. The classroom function agreements, though, typically did not indicate if children would provide information online to the vendor. Approximately 18% of the agreements specify that children could supply personally identifiable information.[294] Similarly, approximately13% included clauses indicating that the services would track children's activities. These findings are shown in the table below:

---

under the age of 18 must be notified before such students use the service. *See id.* at 1–3. Agreement Document No. 65 requires that parents of students under the age of 18 read and agree to the Terms of Use. *See* Agreement Document No. 65 at 1, 4.

[290] Agreement Document No. 55 provides that the customer must obtain parental consent for use by end users to comply with COPPA. *See* Agreement Document No. 55 at 8.

[291] *See supra* note 124.

[292] Agreement Document No. 60 provides that a request to access data must be made through the school district. *See* Agreement Document No. 60 at 3. Agreement Document No. 64 allows for parental access to student information and also provides that the service has a student edit function. *See* Agreement Document No. 64 at 1.

[293] *See supra* note 143.

[294] Agreement Document No. 52 provides that the service allows user to submit information that "include[s], but [is] not limited to: name, email, address, social security number," and others. *See* Agreement Document No. 52 at 1. Such submissions may take the form of public postings. *See id.* at 2. The service also tracks cookies. *Id*. Agreement Document No. 64 provides that parental consent is required for children to supply personally identifiable information; otherwise, such data submitted by children under 13 years of age is deleted. *See* Agreement Document No. 64 at 1. The vendor disclaims that it cannot control the actions of other users with whom a user shares information. *See id*.. Furthermore, the website captures users' IP addresses and uses cookies. *Id.* at 2–3. Agreement Document No. 65 provides that children may supply personally identifiable only after parental consent to use. *See* Agreement Document No. 65 at 2. Users, including those under 13 years of age, may post or share information while using the service and "[the vendor] has no practical ability to restrict the information, conduct, communications, or content which might be posted or exchanged through the use of its technology . . . ." *See id.* at 2–3. Agreement Document No. 46 provides that children under the age of 13 may supply personally identifiable information only when parental consent has been given for use of the service; if it is discovered that a student under that age has used the service without the required consent, the vendor will delete the student's information and data. *See* Agreement Document No. 46 at 2.

COPPA OBLIGATIONS		
	Total (out of 22)	**Percentage**
Service Enables Child to Supply PII	4	18.2%
Service Enables Child to Be Tracked	3	13.6%

g. Data Security

For basic data security, more than 50% of the agreements required that vendors use some type of security to protect the student data;[295] however, 45% were silent on the matter. Agreements that addressed security provisions generally did not require a precise security obligation.[296] Only one agreement specified an encryption level used by the vendor.[297]

---

295 Agreement Document No. 46 provides that the vendor uses passwords, coding, and permission checks to protect data security. *See* Agreement Document No. 46 at 8. Agreement Document No. 47 provides that vendor will adhere to reasonable security standards that are "no less than the security standards at facilities where [the vendor] stores and processes its own information of a similar type," and also that the vendor has implemented at least "industry standard systems" for security. *See* Agreement Document No. 47 at 1. Agreement Document No. 49 provides that vendor will provide a "secure academic social network." *See* Agreement Document No. 49 at 5. Agreement Document No. 54 provides that the vendor uses a "reasonable degree of care" to protect confidential information. *See* Agreement Document No. 54 at 7. Agreement Document No. 55 provides that the vendor uses "[i]ndustry standard systems and procedures" to secure data. *See* Agreement Document No. 55 at 3. Agreement Document No. 56 provides that the vendor takes "every precaution to protect users' information," that sensitive information is protected both online and offline, and that sensitive information online is encrypted. *See* Agreement Document No. 56 at 2–3. Agreement Document No. 59 provides that the vendor has "appropriate measures in place" to "make reasonable efforts" to protect personal information security. *See* Agreement Document No. 59 at 3. Agreement Document No. 60 provides: "All user information and coursework data are encoded and transmitted through session keys . . . ." *See* Agreement Document No. 60 at 2. Agreement Document No. 61 provides that the vendor uses "reasonable security standards" where it stores and processes customer data. *See* Agreement Document No. 61 at 1. Similarly, Agreement Document No. 63 provides that the vendor uses "industry standard [security] procedures." *See* Agreement Document No. 63 at 1. Agreement Document No. 65 provides that the vendor uses "industry standard" security practices that are "reasonable." *See* Agreement Document No. 65 at 8. Finally, Agreement Document No. 66 provides that the vendor uses "[i]ndustry standard systems and procedures to ensure the security and confidentiality of customer data." *See* Agreement Document No. 66 at 1.

296 Agreement Document No. 46 provides that the vendor uses passwords, coding, and permission checks to protect data security. *See* Agreement Document No. 46 at 8. Agreement Document No. 47 provides that vendor will adhere to reasonable security standards "no less than the security standards at facilities where [the vendor] stores and processes its own information of a similar type" and that vendor has implemented at least "industry standard systems" for security. *See* Agreement Document No. 47 at 1. Agreement Document No. 49 provides that vendor will provide a "secure academic social network." *See* Agreement Document No. 49 at 5. Agreement Document No. 54 provides that the vendor agrees to use a "reasonable degree of care" to protect confidential information. *See* Agreement Document No. 54 at 7. Agreement Document No. 55 (from the same vendor) provides that the vendor implements "[i]ndustry standard systems and procedures." *See* Agreement Document No. 55 at 3. Agreement Document No. 56 provides that vendor takes "every precaution to protect users' information," that sensitive information is protected both online and offline, and that sensitive information online is encrypted. *See* Agreement Document No. 56 at 2–3. Agreement Document No. 59 provides that the vendor has "appropriate measures in place" to "make reasonable efforts" to protect personal information security. *See* Agreement Document No. 59 at 3. Agreement Document No. 60 provides that "[a]ll user information and coursework data are encoded and transmitted through session keys . . . ." *See* Agreement Document No. 60 at 2. Agreement Document No. 61 provides that the vendor uses "reasonable security standards" where it stores and processes customer data. *See* Agreement Document No. 61 at 1. Agreement Document No. 63 provides that the vendor uses "industry standard [security] procedures." *See* Agreement Document No. 63 at 1. Agreement Document No. 65 provides that the vendor uses "industry standard" security practices that are "reasonable." *See* Agreement Document No. 65 at 8. Agreement Document No. 66 provides that the vendor implements "[i]ndustry standard systems and procedures to ensure the security and

As another important data security measure, the destruction or deletion of data transferred for classroom functions is critical once the functions are completed or the contract terminates. Yet, only 32% of the agreements required the deletion or destruction of transferred data by the end of the contract period.[298]

Finally, only one of the twenty-two classroom functions agreements contained a provision requiring that the vendor notify the district in the event that the vendor's security measures are breached or data is otherwise compromised.[299] These findings are illustrated by the following table:

DATA SECURITY		
	Total (out of 22)	**Percentage**
Data Deleted or Destroyed at End of Contract Period	7	31.8%
Non-Specified Security Obligation	12	54.5%
Encryption Level Specified	1	4.5%
NIST Level Specified	0	0.0%
Data Breach Notification Specified	1	4.5%

7. Unidentifiable Functions

This category represents the largest grouping of agreements—more than 25% of all the agreements provided in response to the document request. For these agreements, it was not possible for Fordham CLIP, based on the contractual language, to discern why the district was contracting with the vendor. Because the functions of these agreements are unknown, any analysis of their contents will have limited meaning. As a result, this section will only address their prevalence, the contracts themselves, and several of the privacy protections found in these unidentified agreements.

confidentiality of customer data." *See* Agreement Document No. 66 at 1. Note the variations between Agreement Documents Nos. 54, 55, 61, 63, and 66—all of which are from the same vendor.

[297] Agreement Document No. 61 provides that the vendor uses SSL encryption. *See* Agreement Document No. 61 at 7.

[298] Agreement Document No. 46 provides that account termination may lead to the destruction of associated content. *See* Agreement Document No. 46 at 8. Users may request data deletion, though some information may remain visible if it were copied or stored by other users; additionally, aggregated data may still be used by the vendor. *See id*. at 9. Agreement Document No. 47 provides that the vendor will overwrite data over time after the termination of the agreement. *See* Agreement Document No. 47 at 5. On the other hand, Agreement Document No. 54 (between the same vendor and a different district) provides that the vendor will return or destroy confidential information at the expiration of the agreement. *See* Agreement Document No. 54 at 12. In yet another iteration by the same vendor with a different district, Agreement Document No. 55 provides that the customer may access and export its data at the termination of the agreement and that the vendor will delete or overwrite any un-exported data over time. *See* Agreement Document No. 55 at 9. Similar to another agreement from still the same vendor, Agreement Document No. 61 provides that the vendor will delete and overwrite data over time after termination. *See* Agreement Document No. 61 at 5. Finally, Agreement Document No. 65 provides that users *may* delete information after termination. *See* Agreement Document No. 65 at 7.

[299] Agreement Document No. 51 provides that the vendor promptly notifies the customer of any unauthorized use or disclosure of confidential information. *See* Agreement Document No. 51 at 1.

a. Prevalence

Of the twenty responding districts, more than half produced agreements with third party vendors that did not make clear the service the vendor would provide to the district.[300] The eleven districts produced a combined total of twenty-six agreements representing twenty-five different services or vendors.[301] Although these districts provided other agreements that were unclassifiable—including agreements from the same vendors—this group of twenty-six agreements did not make evident any clearly identified purposes.

b. Contracts

Of the twenty-five agreements for an unidentifiable function, only ten were complete.[302] The high frequency of incomplete documentation may explain why it was not possible to determine the function or purpose of the services; it is likely that language contained in the

---

[300] The eleven districts are Jefferson City Public Schools, Jefferson County Public Schools (CO), Jefferson County Public Schools (KY), London City Schools, Mercer Island School District, Millburn Township Public Schools, Peoria Public School District 150, Providence Public School District, Queen Anne's County Public Schools, San Luis Coastal Unified School District, and Sublette County School District #9.

[301] The services are: Tyler Pulse; Microsoft Online Services; Technology Partners; ANGEL Learning, Inc.; Certiport.com; Edgenuity; Edmentum; Edmodo; Google Chrome OS for Enterprise; Information Design, Inc./SPS EZ PAY; Microsoft Office 2013 Outlook; Project Lead the Way, Inc.; Scholastic.com; Scientific Learning Corp.; Education Only Enterprise Software Reseller; Metropolitan Educational Council; Mercer Island School District Founding Member Agreement for Services; TIENET; FIRM Solutions Data Solutions; SchoolMessenger; Mutual Nondisclosure Agreement; NCS Pearson Product License Agreement; Houghton Mifflin Harcourt; and Northwest Evaluation Association.

[302] The incomplete documents were as follows:

- The Service Agreement referenced by Agreement Document No. 69 was not supplied to Fordham CLIP.
- The Terms and Conditions referenced by Agreement Document No. 71 were not supplied to Fordham CLIP.
- Agreement Document No. 72: Although a Privacy Statement was provided, no direct contract was supplied to Fordham CLIP.
- The fee quote referenced by Agreement Document No. 73 was not supplied to Fordham CLIP.
- The Master Services Agreement referenced by Agreement Document No. 74 was not supplied to Fordham CLIP.
- Agreement Document No. 75: Only order forms and "Standard Purchase and License Terms" were provided to Fordham CLIP.
- The Acceptable Use Policy referenced by Agreement Document No. 76 was not supplied to Fordham CLIP.
- The Agreement Document No. 77 order form was not supplied to Fordham CLIP.
- The End-User License Agreement referenced by Agreement Document No. 80 was not supplied to Fordham CLIP.
- Agreement Document No. 85 was missing at least one page.
- Agreement Document No. 86 was missing all even-numbered pages.
- The Data Processing Agreement referenced by Agreement Document No. 87 was not supplied to Fordham CLIP.
- The Student Information System & Support Services Proposal accompanying Agreement Document No. 88 referenced three services already in use by the district, agreements for which were not supplied to Fordham CLIP.
- The contract governing Agreement Document No. 93 was not supplied to Fordham CLIP.

Agreement Document No. 83 did not apply to the analysis.

elements missing from these agreements would have helped to make clear the service's purpose or function.

c. *Privacy Protections*

A majority of the agreements with an unidentifiable function either prohibited or limited redisclosure of collected data. Generally, however, the agreements did a poor job of reserving to the contracting district rights preserving access to the data and the vendor. Additionally, very few of the agreements specified that disclosure to the vendor was for a purpose that would exempt the disclosure from FERPA's parental consent requirement.[303] Similarly, few contained a provision prohibiting the sale or marketing of collected data. On the other hand, it is encouraging that almost half of the agreements required some form of data security on the part of the vendor. Additionally, fourteen of the agreements (53%) prohibited the vendor from unilaterally amending the agreement. This was the strongest showing among the various categories of agreements.

D. District Policies on Staff Use of Computer Services

District adherence to statutory obligations and fair information practices can be circumvented if the district's staff uses cloud services unbeknownst to the central administration. For example, if a teacher signs up for a "free" account so that the teacher's students can share photographs online as part of a class project, the district will not have had an opportunity to vet the service's privacy protections, and the teacher's activities may not comply with the district's legal obligations. Furthermore, for services that may involve the subsequent sale or marketing of student information, the PPRA requires districts to have policies adopted in consultation with parents.[304] The existence of a district policy establishing teachers' responsibilities for online activity involving students' information is, thus, critical, especially in an environment where teachers are excited and prone to adopt new technologies that can enhance their teaching.

Eighty percent of the districts reported policies that prohibit teachers from using services without district approval.[305] Consequently, twenty percent of the districts do not have internal

---

[303] *See* 20 U.S.C. § 1232g(b)(1) (describing the requirement that parental consent be obtained before a district may disclose personally identifiable student information, and carving out exceptions to this general rule).
[304] *See* 20 U.S.C. § 1232h(c).
[305] District Policy Document No. 1 provides that external software must be registered with the system administrator before installation or use, and also forbids the use of home software on the district server. *See* District Policy Document No. 1 at 1. District Policy Document No. 2 provides: "Users may only install and use properly licensed software, audio or video media purchased by the district or approved for use by the district." *See* District Policy Document No. 2 at 4. It also provides: "Web pages by teachers shall be hosted on servers maintained by the district or on an approved site." *Id.* at 5. District Policy Document No. 3 provides: "Users shall receive or transmit communications using only district-approved and district-managed communications systems. For example, users may not use web-based e-mail, messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the district." *See* District Policy Document No. 3 at 17. District Policy Document No. 4 provides: "Employees will NOT . . . Use unauthorized software products which adversely affect network performance." *See* District Policy Document No. 4 at 1. District Policy Document No. 5 stipulates that the school board regulates for a limited educational purpose and disallows social media use by staff. *See* District Policy Document No. 5. District Policy Document No. 6 provides that employees must obtain the district's permission to install software. *See* District Policy Document No. 6 at 2, 4. District Policy Document No. 7 provides: "Unacceptable network use by district students and staff includes . . . Downloading, installation and use of applications (including shareware or freeware) without permission or approval from their Site Technology Specialist

governance rules that can assure the safeguarding of student information.[306] And, even in districts with policies, the degree of compliance is not known.

E. Notices to Parents Regarding Student Data Privacy

Fewer than half the districts provided notices to parents about data privacy. Only nine of the twenty districts (45%) sent parents notifications about student data privacy[307] and only five districts (25%) directly addressed their cloud computing services in those notices.[308] This means that districts are not providing the required transparency to parents.

---

and Technology Teacher on Special Assignment." *See* District Policy Document No. 7 at 1. District Policy Document No. 8 provides that staff cannot purchase and use software not approved by the director of technology. *See* District Policy Document No. 8 at 2. District Policy Document No. 9 provides that users may only download, install and use district approved software. *See* District Policy Document No. 9 at Para. 3. District Policy Document No. 10 provides that system administrators as well as the superintendent will deem what is appropriate use. *See* District Policy Document No. 10 at 3–4, 5. District Policy Document No. 11 provides: "A district employee who wishes to utilize any technology for electronic communication other than district-approved or district-hosted electronic accounts to communicate with current [district] students must both; notify his/her building principal, and obtain written or electronic consent from the student's parent(s) before utilizing the technology." *See* District Policy Document No. 11 at 1. District Policy Document No. 12 provides that downloading and loading of software without permission from CTS through building technology coordination is prohibited. *See* District Policy Document No. 12 at 3–4. District Policy Document No. 13 provides that the use of unauthorized programs violates the district's Acceptable Use Policy. *See* District Policy Document No. 13 at 5, 10. District Policy Document No. 14 provides that employees may not download or install any software without the approval of DIS, and also prohibits personal file storage. *See* District Policy Document No. 14 at 6.. District Policy Document No. 15 provides: "Any software installation on district computers must have prior approval of the building administrator and the Technology department." *See* District Policy Document No. 15 at 2. District Policy Document No. 16 provides that non-district-approved software use requires permission by the chief technology officer. *See* District Policy Document No. 16 at 2. The document also provides that the district network cannot be used for downloading software or files not related to the district's mission. *See id*. at 2.

[306] Some districts provided employee use policies that did not contain such a provision. For example, neither District Policy Document No. 17, District Policy Document No. 18, nor District Policy Document No. 19 contained such a provision.

[307] Fordham CLIP received the parental notifications from the following districts: West Region Districts (Parental Notification Document No. 1; Parental Notification Document No. 2; Parental Notification Document No. 4; Parental Notification Document No. 5; Parental Notification Document No. 6; Parental Notification Document No. 7; Parental Notification Document No. 8; Parental Notification Document No. 14; Parental Notification Document No. 18; Parental Notification Document No. 19; Parental Notification Document No. 23; Parental Notification Document No. 25); South Region School District (Parental Notification Document No. 3); Northeast Region School Districts (Parental Notification Document No. 9; Parental Notification Document No. 10; Parental Notification Document No. 15; Parental Notification Document No. 16; Parental Notification Document No. 17; Parental Notification Document No. 24); Midwest Region School Districts (Parental Notification Document No. 11; Parental Notification Document No. 12; Parental Notification Document No. 13); South Region Districts (Parental Notification Document No. 20; Parental Notification Document No. 21; Parental Notification Document No. 22; Parental Notification Document No. 26; Parental Notification Document No. 27; Parental Notification Document No. 28).

[308] Parental Notification Document No. 5; Parental Notification Document No. 23; Parental Notification Document No. 24; Parental Notification Document No. 25; Parental Notification Document No. 26; Parental Notification Document No. 27; Parental Notification Document No. 28.

V. RECOMMENDATIONS

The findings demonstrate substantial deficiencies in the privacy protections afforded to student data when public schools outsource functions to the cloud. Fordham CLIP's analysis reveals an overwhelming need for public schools and vendors to improve their information practices so that student data can be adequately protected and so that public schools can comply with FERPA, PPRA, and COPPA and more generally with their community norms and expectations surrounding the privacy of student information.

This Part of the study sets out a series of recommendations for school districts, policy-makers, and vendors to consider. These recommendations address transparency, contract terms, contracting practices and data governance. In addition, they propose the establishment of a research and clearing center to provide assistance in effecting public policy and contracting.

A. Recommendations on Transparency

Fordham CLIP's findings suggest that district agreements often do not meet basic transparency standards. Two practices, in particular, would improve transparency surrounding district agreements with cloud service providers:

1. The Existence and Identity of Cloud Service Providers Should Be Available on District Websites

Districts should be transparent with their parents and communities about their reliance on cloud services. These services can and should be identified on district websites and the privacy protections in place for student data should be readily visible. Most of the documents Fordham CLIP received in response to the public records request were provided electronically and could readily be placed on a district's website to provide full transparency.

2. Notice to Parents

Districts must provide parents with adequate notice of the transfer of their children's information to cloud service providers. Where consent to transfer or use is required by FERPA or PPRA, districts must assure a mechanism to obtain such consent. In cases where COPPA requires cloud service providers to obtain parental consent, districts should assist those providers in complying with COPPA.

B. Recommendations on Contract Terms

Based on the findings, it seems that cloud service agreements frequently lack basic protections on student data. Fordham CLIP's research suggests that, more often than not, districts are passive parties to cloud service contracts; service providers draft terms and conditions and districts have neither the expertise nor the ability to negotiate over those terms. It is the responsibility of service providers and districts to pay closer attention to privacy issues and obligations; it is likewise the responsibility of state and federal education officials to advance privacy protection.

The checklist developed for this study to analyze the agreements provides a framework to improve the terms, conditions, and contracting practices regarding cloud service agreements.

Because vendors typically draft the cloud computing contracts and control the terms of those agreements, vendors have a responsibility to treat districts fairly and to effectively safeguard student information. Specifically, the checklist provides a framework that can be applied to agreements to: 1) improve the protection of student privacy and 2) assure statutory compliance. Vendors should use this framework in the preparation of contracts with school districts. Additionally, state and federal education officials, as well as state and federal legislatures, can advance this agenda by requiring that all publicly funded agreements contain a specific set of terms. The recommendations for these terms and conditions are:

1. Specification of the Purpose of and the Authority to Enter into the Agreement

The purpose of the agreement—including the service functions to be performed—should be transparent and specified explicitly. Similarly, the justification or authority to outsource the service function should be explicitly stated. When FERPA applies, these statements are required for audit and evaluation purposes, research studies, and cases when contractors are performing school functions as agent for a district.[309] When FERPA does not apply, this is an important contractual representation.

2. Specification of the Types of Data Transferred or Collected

There should be no ambiguity in the agreement regarding the data that is transferred or collected online (e.g., transaction data). The contract terms should include an appendix or exhibit listing the data elements that are transferred and collected. In particular, the agreements should indicate exactly what identifying information is used by the vendor.

In addition, the contract terms should explicitly address the collection of data directly from children and whether cloud service providers will track children's use of the services.

3. Prohibition or Limitation on Redisclosure of Student Data

FERPA contains restrictions on the redisclosure of student information.[310] Accordingly, cloud service agreements should explicitly prohibit or, where appropriate, limit redisclosure.

4. Prohibition or Limitation on the Sale or Marketing of Student Information Without Express Parental Consent

Because of legal restrictions[311] and fairness concerns, cloud service agreements should include a clause explicitly addressing the sale and marketing of transferred data or the use of that data by the vendor itself for sale and marketing purposes without parental consent.

5. Assurance that Districts Have Exclusive Control over Data Access and Mining

Districts should be in control of their student data. This means that agreements must ensure that district personnel may determine who accesses student information and how such information may be mined for legitimate, authorized purposes. To the extent that vendors seek

---

[309] *See* 34 C.F.R. § 99.31(a)(6)(i)(C)(1).
[310] *See* 20 U.S.C. § 1232g(b)(4)(B); 34 C.F.R. § 99.33.
[311] *See id.*

to use student data for any commercial purposes in addition to providing the specified services, those uses must be clearly disclosed in the principal contract document.

6. Prohibition on the Imposition of New or Conflicting Privacy Terms when Parents are Required to Activate an Account for the School's Cloud Services

When cloud services require parents to activate an account so that their children can participate in school activity, the activation process should not be a means to force parents to consent to weaker privacy protections in circumvention of the privacy protections included in the district's contract. Agreements should stipulate that the activation process will be consistent with the privacy terms of the district's agreement and will not override those terms.

7. Allocation of Responsibilities for Granting Parental Access and Correction Capabilities

Cloud service arrangements may diffuse or complicate how parents can exercise their rights of access and correction under FERPA.[312] The cloud service agreements should, thus, specify the responsibilities as between the district and the service provider to assure that the exercise of the parental rights can be satisfied.

8. Specification of Whether Foreign Storage and Processing Is Permitted

While not a legal requirement, the ability of a district to assure control over student information may be affected by the jurisdiction where the data might be stored. Districts should be made aware of this risk through a contract specification.

9. Specification of Whether Other Government Agencies May Have Access Without Parental Consent

FERPA limits the ability of sharing student information across different government agencies (e.g. sharing between the state education agency and state labor department).[313] Cloud service agreements—particularly data analytic agreements—should specify what, if any, sharing is contemplated.

10. Specification of Data Security and Breach Notification

Data security is essential in the context of student data. The cloud service agreements should specify requirements for the types and levels of security to be deployed. In addition, a data breach notification clause is important for districts to ensure that they remain informed about the status of their data.

[312] *See* 20 U.S.C. § 1232g(a)(1) (providing a right of access to educational records); 20 U.S.C. § 1232g(a)(2) (providing a right to challenge inaccuracies).
[313] FERPA does not authorize disclosure of educational records without parental consent for general purposes by government agencies. *See, e.g.*, 20 U.S.C. § 1232g(b).

11. Prohibition on Unilateral Modifications

Districts cannot accept agreements that allow unilateral modifications by cloud service providers and still comply with FERPA, PPRA and basic privacy protections. Accordingly, agreements must ban unilateral modifications.

12. Inclusion of a Right for the District to Audit and Inspect Vendors' Compliance

Districts need a means of verifying that vendors are fulfilling their contractual commitments, as districts are subject to the FERPA and PPRA obligations independent from the vendors.

C. Recommendations on Contracting Practices

Based on many of the poor contracting practices revealed in this report, districts must properly document contractual commitments and obligations. Unlike many business contexts in which organizations may accept the risk of inadequately documented partnerships, schools are stewards of students' information and have public responsibilities that require more careful attention. This recommendation thus consists of two components:

1. Districts Need Executed Agreements.

Districts must have original, dated agreements executed by both parties. In the case of services with online "click-through" agreements, districts must preserve a copy of the agreement that is executed online, which should include date of acceptance and identification of the authorized signing officers. Without properly executed agreements, districts' legal rights and obligations are not properly established.

2. Districts Need Complete Documentation.

Districts must have original, dated agreements that are complete and that include all documents incorporated by reference by the agreement (e.g., privacy policies, terms of use, additional terms and conditions). Without complete documentation, districts can neither demonstrate their compliance with legal obligations nor establish their rights with respect to vendors.

D. Recommendations on Data Governance

The study findings indicate that data governance should be strengthened at the district level.

1. Districts Must Establish Policies and Implementation Plans for the Adoption of Cloud Services by Teachers and Staff.

All districts should have policies in place that require consideration of privacy issues and obligations as part of the vetting of any cloud service agreement. Districts should also have employee computer use policies that bar employees from using cloud services not approved by the district. Without such policies, teachers are likely to inadvertently compromise student privacy. At the same time, districts need to have an easy means such as a web portal for teachers to identify approved services or to request approval to use new tools. Lastly, districts need to include the review of district policies on employee computer use as part of in-service training. Teachers need to have data literacy and an understanding of the implications of technologies that use student information.

To assist in developing sound and effective policies, districts may wish to create a data governance advisory council that would include members of the local community. The council's role would be to provide advice in connection with policies for the district's use of online services that would assure information privacy and the transparency of the online services in use by the school system.

Industry and others may also wish to assist districts by developing certification criteria and mechanisms to vet cloud services that effectively protect student privacy. Organizations can, for example, offer schools portals to certified "privacy safe" products and services.

2. Districts Must Address Directly and Publicly Their Policies on Allowing the Use of Student Data for Advertiser Supported Services when Not Prohibited by FERPA.

The findings illustrate that "freemium" services are being made available to schools. For these services, student data is likely being used in some way to support the provision of the service to the district. The choice to use "freemium" services at the cost of student privacy should be clear, transparent and subject to public discussion. Vendors have a responsibility and must ensure that districts and their communities have sufficient information for such public discussions. Vendors should provide and districts should require clear information about how student data may be used for commercial purposes beyond the provision of contracted cloud services.

3. States and Larger Districts Must Have Chief Privacy Officers.

The findings show that districts need assistance to address the privacy issues associated with the treatment of their students' information. In a prior study, Fordham CLIP strongly recommended that states establish Chief Privacy Officers within the state's Department of Education.[314] Now, this function is ever more essential to be able to provide advice to smaller districts and districts without the resources to handle privacy issues on their own. For larger districts and those with extensive cloud networks and intensive data transfers, the designation of a chief privacy officer with responsibility for data governance, privacy compliance, and teacher training is necessary to assure proper stewardship of student data and to enable those districts to more effectively assure the protection of their students' information.

E. Recommendation for the Creation of a National Research Center and Clearinghouse

The findings indicate that in addition to the school districts, both cloud service providers and policy-makers have a tremendous need for assistance in addressing student data privacy. A

[314] *See* Joel R. Reidenberg, Jamela Debelak et al., *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems*, at 56 (Fordham CLIP Research Report: 2009), *available at* http://law.fordham.edu/assets/CLIP/CLIP_Report_Childrens_Privacy_Final.pdf.

national research center and clearinghouse would be able to provide critical guidance. Such a center should be independent of commercial interests to assure objectivity, and could be created through a variety of vehicles including state or federal legislation, private support for a non-profit, or grant support. The center's role could consist of the following responsibilities:

- Preparing academic and policy research to provide insight on privacy issues related to student data and schools
- Convening workshops for stakeholders
- Drafting model contract clauses, privacy notices, and consent forms for common cloud service functions
- Creating a repository for research, model contracts, and policies

APPENDIX A

Open Records Act Request Letter

FORDHAM **University**
School of Law

PROFESSOR JOEL R. REIDENBERG
Stanley D. and Nikki Waxberg Chair in Law
Academic Director, Center on Law and Information Policy

FORDHAM CENTER ON INFORMATION LAW AND POLICY
Research Project:

Privacy and Cloud Computing in K-12 Public Schools

The Fordham Center on Law and Information Policy ("Fordham CLIP") is researching the use of "cloud," web-based, or third-party computer services by public school districts across the country. Fordham CLIP is inviting approximately 50 districts to participate in this study chosen from the Department of Education's NCES database to reflect large, mid-size and small enrollment districts across each of the nine U.S. Census geographic regions. The project's goal is to analyze how public school districts address student privacy when using online services to identify compliance practices and trends. The final published report, which will be made available to all participating school districts and the public, will seek to make policy recommendations to help educational leaders and policy-makers understand how these services and service providers comply with legal requirements. Your participation in this project will help to ensure that our final report is a useful tool for understanding this increasingly important issue.

On behalf of Fordham CLIP, I request copies of the following information:

1. All contracts or user agreements the District might have for free or paid computing services with outside service providers/vendors involving data about students (e.g. hosting services for school work or projects, student information systems, student demographic databases, web services, course/grade management services, document management services, email services for students/teachers/administrators).

2. All District computer use policies with respect to staff and teachers' use of free or paid third-party services that might host or process student information.

3. All notices circulated by the District to parents about student data privacy.

4. All notices circulated by the District to parents about the use of free or paid third-party computing services that receive student data.

Please send copies to:

Professor Joel R. Reidenberg
Fordham University School of Law
140 West 62nd Street
New York, NY 10023

Or by email to: jreidenberg@law.fordham.edu

For any questions concerning this request, I may be reached by email or by phone at: 212-636-6843.

---

140 WEST 62nd STREET * NEW YORK, N.Y. 10023-7485 (USA) * TEL. 212-636-6843 *FAX 212-930-8833
Email: <jreidenberg@law.fordham.edu> Web: <http://faculty.fordham.edu/reidenberg>

APPENDIX B

Document Coding Checklist

DOCUMENT CODING CHECKLIST

Question	Rationale	Category
Does the document specify transfer of student name?	FERPA 20 U.S.C. § 1232g(b)(1)	Types of Data Transferred
Does the document specify transfer of student address?	FERPA 20 U.S.C. § 1232g(b)(1)	
Does the document specify transfer of student sex?	FERPA 20 U.S.C. § 1232g(b)(1)	
Does the document specify transfer of student ID?	FERPA 20 U.S.C. § 1232g(b)(1)	
Does the document specify transfer of student age/grade?	FERPA 20 U.S.C. § 1232g(b)(1)	
Does the document specify transfer of biometric data?	FERPA 20 U.S.C. § 1232g(b)(1)	
Does the document specify transfer of medical/health data?	FERPA 20 U.S.C. § 1232g(b)(1)	
Does the document specify transfer of socio-economic data?	FERPA 20 U.S.C. § 1232g(b)(1)	
Does the document specify collection of transaction data?	Transparency	
Does the document prohibit or limit redisclosure?	FERPA 20 U.S.C. §§ 1232g(b)(1)(F) & (4)(B); 34 C.F.R. § 99.33(b)	Sharing, Data Mining, Redisclosure Limits, and Data Control
Does the contract give the district exclusive control over its data?	FERPA 20 U.S.C. § 1232g(b)(1)(A); 34 C.F.R. § 99.31(a)(1)(i)(B)	
Does the district have audit and inspection rights over the vendor?[315]	FERPA 20 U.S.C. §§ 1232g(b)(1)(A) & (b)(4)(A); 34 C.F.R. §§ 99.32(c)(3) & 99.31(a)(1)(i)(B); Good Contract Practice	
Does the district have exclusive control to determine access to data based on the user's role?	Data security	
Does the contract specify an audit or evaluation purpose for disclosure to vendor?	FERPA 20 U.S.C. §§ 1232g(b)(1)(F), (b)(5) & (b)(3); 34 C.F.R. 99.31(a)(6)(iii); PPRA 20 U.S.C. 1232h(c)(4)(A)	
Is data being used for sale or marketing of instructional materials, student recognition, college or military recruitment, or to provide low-cost literary materials?	PPRA 20 U.S.C. § 1232h(c)(4)(A)	
Does the agreement provide that information may be disclosed for a health, safety, or emergency purpose?	FERPA 20 U.S.C. § 1232g(b)(1)(H)-(I); 34 C.F.R. §99.31(a)(6)(iii)	
Does contract prohibit the sale and marketing use of student data (including transaction data)?	Secondary Use	
Does the contract prohibit foreign storage?	Data Security	
Does the contract prohibit access by other gov't agencies?	Secondary Use	
Does the document provide (for) parental notice?[316]	FERPA 20 U.S.C. §§ 1232g(a)(5)(A), (b), (h), and (j); 34 C.F.R. §§ 99.31(a) & (b); FERPA 20 U.S.C. § 1232g(e); 34 C.F.R. § 99.7(a)(1); FERPA 20 U.S.C. § 1232g(e); COPPA 15 U.S.C. §§ 6502(b)(1) and 16 C.F.R. §§ 312.3(b) & (c); PPRA 20 U.S.C. § 1232h(c)(1); PPRA 20 U.S.C. §§ 1232h(c)(2)(A)(i), h(c)(2)(8), h(c)(2)(C) & 1232(h)(d); PPRA 20 U.S.C. § 1232h(c)(2)(A)(ii)	Notice, Consent, Access, and Transparency
Does the document provide (for) parental consent?[317]	FERPA 20 U.S.C. §§ 1232g(a)(5)(A), (b), (h), and (j); 34 C.F.R. §§ 99.31(a) & (b); FERPA 20 U.S.C. § 1232g(e); 34 C.F.R. § 99.7(a)(1); COPPA 16 C.F.R. § 312.4; PPRA 20 U.S.C. § 1232h(c)(1)	
Does the contract give the district a right enabling it to provide parental access and correction to student data?	FERPA 20 U.S.C. §§ 1232g(a)(1)(A) & (a)(2); COPPA 15 U.S.C. § 6502(b)(1) and 16 C.F.R. § 312.4	
Must parents activate an account directly with the vendor?	COPPA 16 C.F.R. § 312.4	

[315] The Fordham CLIP team interpreted a district's retention of complete control and/or ownership of the data to imply audit/inspection rights.

[316] This question seeks to answer whether the document either: 1) provides actual notice or 2) provides that the district must give parents notice of its use of a particular service.

[317] This question seeks to answer whether the document either: 1) is used to obtain parental consent or 2) provides that the district must obtain parental consent before a student may use a particular service.

Does the service enable a child to supply PII?	COPPA; 16 CFR § 312.2	COPPA
Does the service enable a child to be tracked?	COPPA; 16 CFR § 312.2	
Does the contract provide for the destruction/deletion of student data at end of contract period?	20 U.S.C. §§ 1232(b)(1)(F) & (b)(3)	Data Security
Does the document include a non-specified security obligation?[318]	Data Security	
Does the document specify an encryption level?	Data Security	
Does the document specify a NIST level?	Data Security	
Does the contract address data breach notification?	Data Security	
Is there a direct contract between the district and data recipient/vendor?[319]	FCPO Guidance	Contracting
Does the contract provide a unilateral right to amend by vendor: YES (w/notice[320])?	Contract Validity	
Does the contract provide a unilateral right to amend by vendor: YES (w/out notice)?	Contract Validity	
Does the contract provide a unilateral right to amend by vendor: NO?	Contract Validity	
Is the document complete?	Contract Practice	Document Completeness
Was the document obtained post-open records request?	Contract Practice	
Does the district have a policy on employee's use of Internet-based services that limits employees to services approved by the district?	Data Governance	Misc.
Are the services provided without financial charge to the district?	Secondary Use	

[318] This question seeks to answer whether the document contains a generally-stated security obligation.
[319] This question seeks to answer whether the document represents a fully executed agreement between the vendor and district personnel.
[320] Fordham CLIP interprets this to mean “direct” or “actual” notice. Constructive notice is insufficient to satisfy this question.

APPENDIX C

Results by Category

DATA ANALYTICS

		CATEGORY	Data Analytics	
		AGGREGATE RESULTS	**Total (out of 9)**	**Percentage**
DOCUMENT CONTENTS	Type of Data Transferred	Does the document specify transfer of **type of student data: NAME?**	1	11.1%
		Does the document specify transfer of **type of student data: ADDRESS?**	2	22.2%
		Does the document specify transfer of **type of student data: SEX?**	3	33.3%
		Does the document specify transfer of **type of student data: ID?**	2	22.2%
		Does the document specify transfer of **type of student data: AGE/GRADE?**	4	44.4%
		Does the document specify transfer of **type of student data: BIOMETRIC?**	1	11.1%
		Does the document specify transfer of **type of student data: MEDICAL/HEALTH?**	2	22.2%
		Does the document specify transfer of **type of student data: SOCIO-ECONOMIC?**	2	22.2%
		Does the contract clearly indicate if **transaction data is collected and analyzed**?	2	22.2%
	Sharing, Data Mining, Redisclosure Limits, and Data Control	Does the document provide **prohibitions or limitations on redisclosure**?	8	88.9%
		Does the contract include **a contractual provision giving exclusive control** of **all** data analytics to the school district?	2	22.2%
		Does the District have **audit and inspection** rights with respect to the vendor?	3	33.3%
		Does the contract give the District **exclusive control to determine access** to data based on the user's role?	1	11.1%
		Does the contract specify an **Audit/evaluation purpose** for disclosure to vendor?	2	22.2%
		Is data being used for sale or marketing of **instructional materials, student recognition, colleges, the military, or low-cost literary materials?**	0	0.0%
		Does the agreement provide that information may be disclosed for a **health, safety, or emergency purpose?**	0	0.0%
		Does contract prohibit the **sale and marketing use** of student data including transaction data?	0	0.0%
		Does the contract prohibit: **FOREIGN STORAGE**?	0	0.0%
		Does the contract prohibit: **ACCESS BY OTHER GOV'T AGENCIES**?	0	0.0%
	Notice, Consent, Access, and Transparency	Does the document provide **Parental Notice**?	2	22.2%
		Does the document provide **Parental Consent**?	1	11.1%
		Does the contract give the District a contractual right that enables the District to provide **parental access and correction** to student data?	1	11.1%
		Does the arrangement provide that **parents must activate account** directly with vendor?	0	0.0%
	COPPA Obligations	Does the service **enable a child to supply PII**?	1	11.1%
		Does the service **enable a child** to be **tracked**?	1	11.1%
	Data Security	Does the contract provide for the **Destruction/Deletion of student data** at the end of the contract period?	6	66.7%
		Does the document include any of the following **Data security requirement: NON-SPECIFIED SECURITY OBLIGATION?**	7	77.8%
		Does the document include any of the following **Data security requirement: ENCRYPTION LEVEL?**	1	11.1%
		Does the document include any of the following **Data security requirement: NIST LEVEL?**	0	0.0%
		Does the contract address **data breach notification**?	1	11.1%
	Contracting	Is there a **direct contract** between the District and data recipient/vendor?	9	100.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/notice)**?	0	0.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/out notice)**?	1	11.1%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **NO**?	6	66.7%
	Document Completeness	Is the document complete?	7	77.8%
		Was the document obtained post-Open Records request?	0	0.0%
	Miscellaneous	Does the District have a **policy on employee's use of Internet-based services** that limits employees to services approved by the District?	0	0.0%
		Are the services provided **without financial charge** to the district?	1	11.1%

STUDENT REPORTING

			CATEGORY	Student Reporting	
			AGGREGATE RESULTS	*Total (out of 5)*	*Percentage*
DOCUMENT CONTENTS	Type of Data Transferred	Does the document specify transfer of **type of student data: NAME?**		0	0.0%
		Does the document specify transfer of **type of student data: ADDRESS?**		0	0.0%
		Does the document specify transfer of **type of student data: SEX?**		0	0.0%
		Does the document specify transfer of **type of student data: ID?**		0	0.0%
		Does the document specify transfer of **type of student data: AGE/GRADE?**		0	0.0%
		Does the document specify transfer of **type of student data: BIOMETRIC?**		0	0.0%
		Does the document specify transfer of **type of student data: MEDICAL/HEALTH?**		0	0.0%
		Does the document specify transfer of **type of student data: SOCIO-ECONOMIC?**		0	0.0%
		Does the contract clearly indicate if **transaction data is collected and analyzed**?		1	20.0%
	Sharing, Data Mining, Redisclosure Limits, and Data Control	Does the document provide **prohibitions or limitations on redisclosure**?		4	80.0%
		Does the contract include **a contractual provision giving exclusive control** of **all** data analytics to the school district?		1	20.0%
		Does the District have **audit and inspection** rights with respect to the vendor?		1	20.0%
		Does the contract give the District **exclusive control to determine access** to data based on the user's role?		3	60.0%
		Does the contract specify an **Audit/evaluation purpose** for disclosure to vendor?		0	0.0%
		Is data being used for sale or marketing of **instructional materials, student recognition, colleges, the military, or low-cost literary materials?**		0	0.0%
		Does the agreement provide that information may be disclosed for a **health, safety, or emergency purpose?**		0	0.0%
		Does contract prohibit the **sale and marketing use** of student data including transaction data?		0	0.0%
		Does the contract prohibit: **FOREIGN STORAGE**?		0	0.0%
		Does the contract prohibit: **ACCESS BY OTHER GOV'T AGENCIES**?		0	0.0%
	Notice, Consent, Access, and Transparency	Does the document provide **Parental Notice**?		0	0.0%
		Does the document provide **Parental Consent**?		0	0.0%
		Does the contract give the District a contractual right that enables the District to provide **parental access and correction** to student data?		0	0.0%
		Does the arrangement provide that **parents must activate account** directly with vendor?		0	0.0%
	COPPA Obligations	Does the service **enable a child to supply PII**?		0	0.0%
		Does the service **enable a child** to be **tracked**?		0	0.0%
	Data Security	Does the contract provide for the **Destruction/Deletion of student data** at the end of the contract period?		3	60.0%
		Does the document include any of the following **Data security requirement: NON-SPECIFIED SECURITY OBLIGATION?**		3	60.0%
		Does the document include any of the following **Data security requirement: ENCRYPTION LEVEL?**		1	20.0%
		Does the document include any of the following **Data security requirement: NIST LEVEL?**		0	0.0%
		Does the contract address **data breach notification**?		0	0.0%
	Contracting	Is there a **direct contract** between the District and data recipient/vendor?		5	100.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/notice)**?		0	0.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/out notice)**?		1	20.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **NO**?		2	40.0%
	Document Completeness	Is the document complete?		4	80.0%
		Was the document obtained post-Open Records request?		0	0.0%
	Miscellaneous	Does the District have a **policy on employee's use of Internet-based services** that limits employees to services approved by the District?		0	0.0%
		Are the services provided **without financial charge** to the district?		0	0.0%

GUIDANCE

		CATEGORY	Guidance	
		AGGREGATE RESULTS	*Total (out of 6)*	*Percentage*
DOCUMENT CONTENTS	Type of Data Transferred	Does the document specify transfer of **type of student data: NAME?**	5	83.3%
		Does the document specify transfer of **type of student data: ADDRESS?**	5	83.3%
		Does the document specify transfer of **type of student data: SEX?**	4	66.7%
		Does the document specify transfer of **type of student data: ID?**	1	16.7%
		Does the document specify transfer of **type of student data: AGE/GRADE?**	4	66.7%
		Does the document specify transfer of **type of student data: BIOMETRIC?**	0	0.0%
		Does the document specify transfer of **type of student data: MEDICAL/HEALTH?**	0	0.0%
		Does the document specify transfer of **type of student data: SOCIO-ECONOMIC?**	1	16.7%
		Does the contract clearly indicate if **transaction data is collected and analyzed**?	3	50.0%
	Sharing, Data Mining, Redisclosure Limits, and Data Control	Does the document provide **prohibitions or limitations on redisclosure**?	4	66.7%
		Does the contract include **a contractual provision giving exclusive control** of **all** data analytics to the school district?	0	0.0%
		Does the District have **audit and inspection** rights with respect to the vendor?	0	0.0%
		Does the contract give the District **exclusive control to determine access** to data based on the user's role?	0	0.0%
		Does the contract specify an **Audit/evaluation purpose** for disclosure to vendor?	1	16.7%
		Is data being used for sale or marketing of **instructional materials, student recognition, colleges, the military, or low-cost literary materials?**	1	16.7%
		Does the agreement provide that information may be disclosed for a **health, safety, or emergency purpose?**	0	0.0%
		Does contract prohibit the **sale and marketing use** of student data including transaction data?	0	0.0%
		Does the contract prohibit: **FOREIGN STORAGE**?	0	0.0%
		Does the contract prohibit: **ACCESS BY OTHER GOV'T AGENCIES**?	0	0.0%
	Notice, Consent, Access, and Transparency	Does the document provide **Parental Notice**?	0	0.0%
		Does the document provide **Parental Consent**?	1	16.7%
		Does the contract give the District a contractual right that enables the District to provide **parental access and correction** to student data?	1	16.7%
		Does the arrangement provide that **parents must activate account** directly with vendor?	0	0.0%
	COPPA Obligations	Does the service **enable a child to supply PII**?	0	0.0%
		Does the service **enable a child** to be **tracked**?	0	0.0%
	Data Security	Does the contract provide for the **Destruction/Deletion of student data** at the end of the contract period?	2	33.3%
		Does the document include any of the following **Data security requirement: NON-SPECIFIED SECURITY OBLIGATION?**	4	66.7%
		Does the document include any of the following **Data security requirement: ENCRYPTION LEVEL?**	1	16.7%
		Does the document include any of the following **Data security requirement: NIST LEVEL?**	0	0.0%
		Does the contract address **data breach notification**?	0	0.0%
	Contracting	Is there a **direct contract** between the District and data recipient/vendor?	3	50.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/notice)**?	2	33.3%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/out notice)**?	2	33.3%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **NO**?	1	16.7%
	Document Completeness	Is the document complete?	5	83.3%
		Was the document obtained post-Open Records request?	0	0.0%
	Miscellaneous	Does the District have a **policy on employee's use of Internet-based services** that limits employees to services approved by the District?	0	0.0%
		Are the services provided **without financial charge** to the district?	0	0.0%

SPECIAL SCHOOL FUNCTIONS

		CATEGORY	Special School Functions	
		AGGREGATE RESULTS	***Total (out of 9)***	***Percentage***
DOCUMENT CONTENTS	**Type of Data Transferred**	Does the document specify transfer of **type of student data: NAME?**	1	11.1%
		Does the document specify transfer of **type of student data: ADDRESS?**	1	11.1%
		Does the document specify transfer of **type of student data: SEX?**	0	0.0%
		Does the document specify transfer of **type of student data: ID?**	1	11.1%
		Does the document specify transfer of **type of student data: AGE/GRADE?**	1	11.1%
		Does the document specify transfer of **type of student data: BIOMETRIC?**	0	0.0%
		Does the document specify transfer of **type of student data: MEDICAL/HEALTH?**	0	0.0%
		Does the document specify transfer of **type of student data: SOCIO-ECONOMIC?**	0	0.0%
		Does the contract clearly indicate if **transaction data is collected and analyzed**?	0	0.0%
	Sharing, Data Mining, Redisclosure Limits, and Data Control	Does the document provide **prohibitions or limitations on redisclosure**?	3	33.3%
		Does the contract include **a contractual provision giving exclusive control** of **all** data analytics to the school district?	0	0.0%
		Does the District have **audit and inspection** rights with respect to the vendor?	0	0.0%
		Does the contract give the District **exclusive control to determine access** to data based on the user's role?	1	11.1%
		Does the contract specify an **Audit/evaluation purpose** for disclosure to vendor?	0	0.0%
		Is data being used for sale or marketing of **instructional materials, student recognition, colleges, the military, or low-cost literary materials?**	0	0.0%
		Does the agreement provide that information may be disclosed for a **health, safety, or emergency purpose?**	1	11.1%
		Does contract prohibit the **sale and marketing use** of student data including transaction data?	0	0.0%
		Does the contract prohibit: **FOREIGN STORAGE**?	0	0.0%
		Does the contract prohibit: **ACCESS BY OTHER GOV'T AGENCIES**?	0	0.0%
	Notice, Consent, Access, and Transparency	Does the document provide **Parental Notice**?	1	11.1%
		Does the document provide **Parental Consent**?	1	11.1%
		Does the contract give the District a contractual right that enables the District to provide **parental access and correction** to student data?	1	11.1%
		Does the arrangement provide that **parents must activate account** directly with vendor?	1	11.1%
	COPPA Obligations	Does the service **enable a child to supply PII**?	1	11.1%
		Does the service **enable a child** to be **tracked**?	1	11.1%
	Data Security	Does the contract provide for the **Destruction/Deletion of student data** at the end of the contract period?	0	0.0%
		Does the document include any of the following **Data security requirement: NON-SPECIFIED SECURITY OBLIGATION?**	2	22.2%
		Does the document include any of the following **Data security requirement: ENCRYPTION LEVEL?**	1	11.1%
		Does the document include any of the following **Data security requirement: NIST LEVEL?**	0	0.0%
		Does the contract address **data breach notification**?	0	0.0%
	Contracting	Is there a **direct contract** between the District and data recipient/vendor?	7	77.8%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/notice)**?	1	11.1%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/out notice)**?	1	11.1%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **NO**?	4	44.4%
	Document Completeness	Is the document complete?	4	44.4%
		Was the document obtained post-Open Records request?	0	0.0%
	Miscellaneous	Does the District have a **policy on employee's use of Internet-based services** that limits employees to services approved by the District?	0	0.0%
		Are the services provided **without financial charge** to the district?	1	11.1%

HOSTING, MAINTENANCE, AND BACKUP FUNCTIONS

			CATEGORY	Hosting/Maintenance/Backup	
			AGGREGATE RESULTS	*Total (out of 15)*	*Percentage*
DOCUMENT CONTENTS	Type of Data Transferred	Does the document specify transfer of **type of student data: NAME?**		3	20.0%
		Does the document specify transfer of **type of student data: ADDRESS?**		3	20.0%
		Does the document specify transfer of **type of student data: SEX?**		0	0.0%
		Does the document specify transfer of **type of student data: ID?**		0	0.0%
		Does the document specify transfer of **type of student data: AGE/GRADE?**		1	6.7%
		Does the document specify transfer of **type of student data: BIOMETRIC?**		0	0.0%
		Does the document specify transfer of **type of student data: MEDICAL/HEALTH?**		0	0.0%
		Does the document specify transfer of **type of student data: SOCIO-ECONOMIC?**		0	0.0%
		Does the contract clearly indicate if **transaction data is collected and analyzed**?		2	13.3%
	Sharing, Data Mining, Redisclosure Limits, and Data Control	Does the document provide **prohibitions or limitations on redisclosure**?		8	53.3%
		Does the contract include **a contractual provision giving exclusive control** of **all** data analytics to the school district?		2	13.3%
		Does the District have **audit and inspection** rights with respect to the vendor?		2	13.3%
		Does the contract give the District **exclusive control to determine access** to data based on the user's role?		4	26.7%
		Does the contract specify an **Audit/evaluation purpose** for disclosure to vendor?		0	0.0%
		Is data being used for sale or marketing of **instructional materials, student recognition, colleges, the military, or low-cost literary materials?**		0	0.0%
		Does the agreement provide that information may be disclosed for a **health, safety, or emergency purpose?**		0	0.0%
		Does contract prohibit the **sale and marketing use** of student data including transaction data?		1	6.7%
		Does the contract prohibit: **FOREIGN STORAGE**?		0	0.0%
		Does the contract prohibit: **ACCESS BY OTHER GOV'T AGENCIES**?		0	0.0%
	Notice, Consent, Access, and Transparency	Does the document provide **Parental Notice**?		1	6.7%
		Does the document provide **Parental Consent**?		2	13.3%
		Does the contract give the District a contractual right that enables the District to provide **parental access and correction** to student data?		2	13.3%
		Does the arrangement provide that **parents must activate account** directly with vendor?		0	0.0%
	COPPA Obligations	Does the service **enable a child to supply PII**?		3	20.0%
		Does the service **enable a child** to be **tracked**?		2	13.3%
	Data Security	Does the contract provide for the **Destruction/Deletion of student data** at the end of the contract period?		2	13.3%
		Does the document include any of the following **Data security requirement: NON-SPECIFIED SECURITY OBLIGATION?**		9	60.0%
		Does the document include any of the following **Data security requirement: ENCRYPTION LEVEL?**		3	20.0%
		Does the document include any of the following **Data security requirement: NIST LEVEL?**		1	6.7%
		Does the contract address **data breach notification**?		2	13.3%
	Contracting	Is there a **direct contract** between the District and data recipient/vendor?		13	86.7%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/notice)**?		0	0.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/out notice)**?		6	40.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **NO**?		5	33.3%
	Document Completeness	Is the document complete?		12	80.0%
		Was the document obtained post-Open Records request?		0	0.0%
	Miscellaneous	Does the District have a **policy on employee's use of Internet-based services** that limits employees to services approved by the District?		0	0.0%
		Are the services provided **without financial charge** to the district?		0	0.0%

CLASSROOM FUNCTIONS

			CATEGORY	Classroom Functions	
			AGGREGATE RESULTS	*Total (out of 22)*	*Percentage*
DOCUMENT CONTENTS	Type of Data Transferred	Does the document specify transfer of **type of student data: NAME?**		6	27.3%
		Does the document specify transfer of **type of student data: ADDRESS?**		6	27.3%
		Does the document specify transfer of **type of student data: SEX?**		1	4.5%
		Does the document specify transfer of **type of student data: ID?**		0	0.0%
		Does the document specify transfer of **type of student data: AGE/GRADE?**		3	13.6%
		Does the document specify transfer of **type of student data: BIOMETRIC?**		0	0.0%
		Does the document specify transfer of **type of student data: MEDICAL/HEALTH?**		0	0.0%
		Does the document specify transfer of **type of student data: SOCIO-ECONOMIC?**		0	0.0%
		Does the contract clearly indicate if **transaction data is collected and analyzed**?		3	13.6%
	Sharing, Data Mining, Redisclosure Limits, and Data Control	Does the document provide **prohibitions or limitations on redisclosure**?		16	72.7%
		Does the contract include **a contractual provision giving exclusive control** of **all** data analytics to the school district?		1	4.5%
		Does the District have **audit and inspection** rights with respect to the vendor?		2	9.1%
		Does the contract give the District **exclusive control to determine access** to data based on the user's role?		4	18.2%
		Does the contract specify an **Audit/evaluation purpose** for disclosure to vendor?		0	0.0%
		Is data being used for sale or marketing of **instructional materials, student recognition, colleges, the military, or low-cost literary materials?**		0	0.0%
		Does the agreement provide that information may be disclosed for a **health, safety, or emergency purpose?**		0	0.0%
		Does contract prohibit the **sale and marketing use** of student data including transaction data?		1	4.5%
		Does the contract prohibit: **FOREIGN STORAGE**?		0	0.0%
		Does the contract prohibit: **ACCESS BY OTHER GOV'T AGENCIES**?		0	0.0%
	Notice, Consent, Access, and Transparency	Does the document provide **Parental Notice**?		8	36.4%
		Does the document provide **Parental Consent**?		9	40.9%
		Does the contract give the District a contractual right that enables the District to provide **parental access and correction** to student data?		2	9.1%
		Does the arrangement provide that **parents must activate account** directly with vendor?		0	0.0%
	COPPA Obligations	Does the service **enable a child to supply PII**?		4	18.2%
		Does the service **enable a child** to be **tracked**?		3	13.6%
	Data Security	Does the contract provide for the **Destruction/Deletion of student data** at the end of the contract period?		7	31.8%
		Does the document include any of the following **Data security requirement: NON-SPECIFIED SECURITY OBLIGATION?**		12	54.5%
		Does the document include any of the following **Data security requirement: ENCRYPTION LEVEL?**		1	4.5%
		Does the document include any of the following **Data security requirement: NIST LEVEL?**		0	0.0%
		Does the contract address **data breach notification**?		1	4.5%
	Contracting	Is there a **direct contract** between the District and data recipient/vendor?		12	54.5%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/notice)**?		2	9.1%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/out notice)**?		12	54.5%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **NO**?		7	31.8%
	Document Completeness	Is the document complete?		18	81.8%
		Was the document obtained post-Open Records request?		0	0.0%
	Miscellaneous	Does the District have a **policy on employee's use of Internet-based services** that limits employees to services approved by the District?		0	0.0%
		Are the services provided **without financial charge** to the district?		6	27.3%

UNIDENTIFIABLE FUNCTION

		CATEGORY	Unidentifiable Function	
		AGGREGATE RESULTS	***Total (out of 25)***	***Percentage***
DOCUMENT CONTENTS	**Type of Data Transferred**	Does the document specify transfer of **type of student data: NAME?**	4	16.0%
		Does the document specify transfer of **type of student data: ADDRESS?**	5	20.0%
		Does the document specify transfer of **type of student data: SEX?**	2	8.0%
		Does the document specify transfer of **type of student data: ID?**	1	4.0%
		Does the document specify transfer of **type of student data: AGE/GRADE?**	1	4.0%
		Does the document specify transfer of **type of student data: BIOMETRIC?**	1	4.0%
		Does the document specify transfer of **type of student data: MEDICAL/HEALTH?**	1	4.0%
		Does the document specify transfer of **type of student data: SOCIO-ECONOMIC?**	0	0.0%
		Does the contract clearly indicate if **transaction data is collected and analyzed**?	0	0.0%
	Sharing, Data Mining, Redisclosure Limits, and Data Control	Does the document provide **prohibitions or limitations on redisclosure**?	15	60.0%
		Does the contract include **a contractual provision giving exclusive control** of **all** data analytics to the school district?	4	16.0%
		Does the District have **audit and inspection** rights with respect to the vendor?	2	8.0%
		Does the contract give the District **exclusive control to determine access** to data based on the user's role?	2	8.0%
		Does the contract specify an **Audit/evaluation purpose** for disclosure to vendor?	2	8.0%
		Is data being used for sale or marketing of **instructional materials, student recognition, colleges, the military, or low-cost literary materials?**	0	0.0%
		Does the agreement provide that information may be disclosed for a **health, safety, or emergency purpose?**	0	0.0%
		Does contract prohibit the **sale and marketing use** of student data including transaction data?	4	16.0%
		Does the contract prohibit: **FOREIGN STORAGE**?	0	0.0%
		Does the contract prohibit: **ACCESS BY OTHER GOV'T AGENCIES**?	1	4.0%
	Notice, Consent, Access, and Transparency	Does the document provide **Parental Notice**?	2	8.0%
		Does the document provide **Parental Consent**?	2	8.0%
		Does the contract give the District a contractual right that enables the District to provide **parental access and correction** to student data?	3	12.0%
		Does the arrangement provide that **parents must activate account** directly with vendor?	0	0.0%
	COPPA Obligations	Does the service **enable a child to supply PII**?	2	8.0%
		Does the service **enable a child** to be **tracked**?	1	4.0%
	Data Security	Does the contract provide for the **Destruction/Deletion of student data** at the end of the contract period?	5	20.0%
		Does the document include any of the following **Data security requirement: NON-SPECIFIED SECURITY OBLIGATION?**	11	44.0%
		Does the document include any of the following **Data security requirement: ENCRYPTION LEVEL?**	0	0.0%
		Does the document include any of the following **Data security requirement: NIST LEVEL?**	0	0.0%
		Does the contract address **data breach notification**?	3	12.0%
	Contracting	Is there a **direct contract** between the District and data recipient/vendor?	13	52.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/notice)**?	1	4.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **YES (w/out notice)**?	7	28.0%
		Does the contract provide a **Unilateral** right to **amend** by vendor: **NO**?	14	56.0%
	Document Completeness	Is the document complete?	10	40.0%
		Was the document obtained post-Open Records request?	0	0.0%
	Miscellaneous	Does the District have a **policy on employee's use of Internet-based services** that limits employees to services approved by the District?	0	0.0%
		Are the services provided **without financial charge** to the district?	2	8.0%