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

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.