Educational Data in the Cloud
Legal Implications and Technical Recommendations

Ben Cohen,* Ashley Hu,* Deisy Patino,* Joel Coffman*†
* Engineering for Professionals, Whiting School of Engineering, Johns Hopkins University
Email: { bcohen49, ahu16, dpatino2, joel.coffman }@jhu.edu
† Department of Computer and Cyber Sciences, United States Air Force Academy

***Abstract*—Moving operations to the cloud has become a way of life for educational institutions. Much of the information these institutions store in the cloud is protected by the Family Educational Rights and Privacy Act (FERPA), which was last amended in 2002, well before cloud computing became ubiquitous. The application of a 1974 law to 21st-century technology presents a plethora of legal and technical questions.**

This work presents an interdisciplinary analysis of existing statutes (i.e., FERPA) and case law. We find that FERPA excludes information that students and faculty often believe is protected and that lower-court decisions have created further ambiguity. Given current technology, the statute is no longer sufficient to protect student data, and we offer recommendations based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework to improve educational institutions' management of protected data.

***Index Terms*—the Family Educational Rights and Privacy Act (FERPA), NIST Cybersecurity Framework, student records**

I. Introduction

Since 1974, FERPA has governed the release of student records by primary, secondary, and post-secondary institutions in the United States. While FERPA is often casually interpreted as establishing a blanket prohibition on releasing student data without permission, in actuality the statue merely deters the unauthorized release of students' records by threatening the withdraw of federal funds from institutions that systematically violate students' privacy. Moreover, FERPA has not been updated since 2002 despite significant changes in the education-record landscape in the interim, particularly the shift away from physical documents toward cloud-based electronic records. The result is a legal morass, with the courts declaring that "FERPA does not contemplate that education records are maintained in numerous places" [5]. Existing Supreme Court precedent establishes a high bar for data to enter a student's "education record" and thus gain the protections of FERPA while lower-court rulings appear to be in conflict with each other. Applying precedents dating back to the 1970s to modern technology raises important questions for both educational institutions and the cloud service providers (CSPs) with which they contract.

II. Statute and Case Law

FERPA, sometimes referred to as the Buckley Amendment, provides for the maintenance and protection of student records in both K–12 and higher education. The portion of the statute most relevant to our work prohibits any educational institution that receives federal funding from maintaining a "policy or practice" of disclosing a student's educational records, or personally identifiable information (PII) other than "directory information," to "any individual, agency, or organization" without the written consent of the student's parents (or the student, if over the age of 18 or attending an institution beyond high school) [2]. The Code of Federal Regulations includes what is known as the "school official" exception, which states that information may be disclosed without consent to "other school officials... within the agency or institution whom the agency or institution has determined to have legitimate educational interests" [1]. The Department of Education (DOE) has explicitly stated that cloud providers fall under the "school official" exception.

As of the 2021 term, the Supreme Court has decided only two cases in which the FERPA statute played a central role: *Gonzaga v. Doe* (2002) and *Owasso Independent School District v. Falvo* (2002). In *Gonzaga*, the Supreme Court ruled that the language of FERPA "fail[s] to confer enforceable rights." Barring students from bringing suit against educational institutions for alleged FERPA violations is enormously consequential. At issue in *Owasso* were peer grading (i.e., allowing students to score each other's work) and the system of reporting the scores. The majority opinion affirmed both practices, as "the word 'maintain' suggests FERPA records will be kept in a filing cabinet in a records room at the school or on a permanent secure database," and "FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar" [4]. The term "maintain" is significant, as numerous state and federal courts have also cited this description of "education records" in subsequent cases whose filings reference FERPA.

Figure 1 summarizes additional case law pertaining to FERPA. Notably, these rulings imply that not all data that passes through a CSP's systems is subject to FERPA. For instance, Gmail and Google Drive, despite being offered by the same company (and presumably being part of the same contract), face differing privacy regulations. Furthermore, technological changes call into question what constitutes a student's "educational record:" the release of the same information may or may not be a FERPA violation depending on what is released—e.g., an email vs. a learning management system (LMS) entry. Another challenge is the increasing ubiquity

978-1-6654-6087-3/22/$31.00 ©2022 IEEE
DOI 10.1109/UCC56403.2022.00032

***Rios v. Read* (1978)** FERPA does not confer a privilege analogous to doctor-patient or attorney-client privilege

***Student Bar Association v. Byrd* (1978)** FERPA threatens the withdrawal of federal funding from institutions that have a policy or practice of releasing student records

***Frasca v. Andrews* (1979)** FERPA protections do not extend to information that is derived independently of school records

***United States v. Miami University* (1997)** Data on student discipline is an "education record" and subject to FERPA's provisions and protections

***Jensen v. Reeves* (1999)** FERPA is intended to address systematic violations of students' privacy by unauthorized releases of educational data

***Curto v. Smith* (2003)** FERPA is not enforceable through private lawsuits

***S.A. v. Tulare County Office of Education* (2009)** Emails that reference students are not considered "education records" unless they are specifically placed in the relevant students' permanent files

***Burnett v. San Mateo–Foster City School District* (2018)** Information contained in emails sent by employees of an educational institution is not subject to FERPA restrictions unless the institution specifically adds a physical or digital copy to a student's permanent file

Fig. 1. Lower-court decisions related to FERPA

of social media, particularly among school-aged youth. One can reasonably argue that the prospect of FERPA-protected information being disclosed through non-school channels is omnipresent, and FERPA cannot be used to suppress information that is public knowledge.

III. Technology Implications

The aforementioned cases have profound implications for the use of cloud computing by educational institutions. In particular, information learned following a data breach would be "derived from a source independent of school records," which suggests that an educational institution or CSP can be held responsible for allowing a third party to acquire information through a data breach but bears no responsibility for the spread of this information beyond the breaching party. It is thus essential that CSPs take steps to ensure the security of the data stored on their servers—and, by extension, that institutions ensure that their contracted CSPs are doing so.

Educational institutions looking for ways to strengthen their digital defenses are likely to encounter a variety of obstacles, including financial constraints and a lack of awareness and training among the user community. The NIST framework provides five main "core functions" that serve as the basis for its implementation and the objectives it sets, as well as the key pillars upon which its success rests [3]. The applications of each pillar to educational institutions are as follows:

Identify School officials should ensure that existing policies and rules emphasize the protection of employees' and students' personal information and update them if this is not the case. School officials should also create cybersecurity manuals to further this goal.

Protect IT administrators must encrypt critical data, ensure all institutional software is kept patched, and teach staff and students how to identify signs of potential cyber threats.

Detect IT administrators must confirm that only authorized users have access to the network and should ensure that procedures are in place to flag any unusual or suspicious behavior.

Respond The institution should create an incident response plan, which includes steps to promptly inform anyone whose information may have been exposed in a breach and alert the proper authorities in the event of a breach.

Recover IT staff must restore any inaccessible data and repair any damaged equipment; staff should also keep all impacted parties apprised of the status of recovery efforts.

Additional tactics can help educational institutions reduce the likelihood of cyberattacks, an option preferable to adopting a reactive stance.

IV. Conclusion

FERPA has become increasingly inadequate to protect student data as that data continues its move to the cloud. When proposed in 1974, it was unthinkable that student records would be stored anywhere other than file cabinets in the school office. Now, however, a teacher can go an entire school year without ever handling a paper document. Homework and tests are completed online, special-education documents are disseminated through OneDrive, and report cards are posted in the LMS. These developments could not have been foreseen in 1974 or even the most recent Supreme Court case related to FERPA in 2002—but student privacy is becoming increasingly limited by a series of outdated standards.

Acknowledgments

We thank Paul Cohen, Esq., of Cipriani & Werner, PC, and Rory Parks, Esq., of Winegrad, Hess & Heimlicher, LLC, for their legal expertise at interpreting case law related to the topic.

References

[1] Code of Federal Regulations, Title 34, Part 99, section 31.

[2] Family Educational Rights and Privacy Act of 1974, *U.S. Statutes at Large*, vol. 88, pp. 828–834 (codified as amended in U.S. Code, Title 20, Section 1232g).

[3] National Institute of Standards and Technology. (2018) Framework for improving critical infrastructure cybersecurity. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[4] Owasso Independent School District v. Falvo, *U.S. Reports*, vol. 534, p. 426, 2002.

[5] S.A. v. Tulare County Office of Education (No. CV F 08-1215 LJO GSA), 2009, (U.S. District Court for the Eastern District of California).