Security Concerns in Post-Secondary Educational Institutions

Arthur Berman

December 15, 2015

1 Abstract

Educational institutions are bastions of enormous amounts of student data. This data can include medical records, academic and extra-academic performance, and more beyond that. The Family Education Right to Privacy Act, hereafter referred to as FERPA, guarantees certain student rights. These rights, including specific restrictions on how student data can be distributed, are the responsibility of the educational institution to enforce. However, elements of these requirements do not specify strong protections in the face of modern security realities, whether due to loopholes in the requirements or through inadequate standards of data management. We present an enumeration of possible vulnerabilities in typical administrative infrastructure seen at the college level, and provide methods to protect student data.

2 Introduction

For many people, colleges and universities are the first private or semi-public institutions to maintain a profile of their personal information. Colleges and universities maintain a wide range of student data, including educational

records, medical information, criminal and disciplinary history, and government identification. This material, collectively considered 'student data,' is often extremely private; its disclosure can put students at risk for employment discrimination, stalking, harassment, and many other negative consequences. To standardize the practices for protecting this data, the federal government signed the Family Education Right to Privacy Act into law, establishing specific requirements for correctly collecting, handling, and releasing student data. This act, also called FERPA, specifies a clear definition for which data must be protected, what protections need to be enforced, and the circumstances under which the protections are relaxed. However, FERPA does not specify the steps that must be taken to protect student data, leaving the onus on individual schools to prescribe adequate security.

3 To the Community

3.1 Motivations

In the digital age, the tools and technologies available to administrators of higher education allow for new approaches to maintaining, updating, and administering student data. Digital tools allow for more sophisticated, efficient record-keeping, easier avenues for communication between students and teachers, and deeper insights into the needs, wants, and abilities of students. However, the appeal of digital solutions in higher education is tempered by the risks inherent to information security at an organizational scale. Inconsistent attention and care with regard to sensitive student records can severely compromise the ability of a college or university to carry out their educational goals. Because of the profound risks in data security, and the natural inertia of large institutions when it comes to technical decisions, an adquately sophisticated attacker has the enormous potential for exploiting vulnerabilities in student data; in 2013, 9% of all reported data leaks were in

the education industry, as compared to 10% in goverment and 4% in financial fields[1]. As such, it is vital that schools be cognizant of the risks they run by storing student data digitally, and to take well-defined, responsible steps to protect it. In failing to accomplish this task, schools open themselves to penalties under FERPA for the disclosure of student information.

Beyond the institutional perspective, most college students are unaware or underinformed of their rights and privileges under FERPA. More importantly, when students are unaware of the risks inherent to FERPA violations, they are unlikely to hold their school accountable when their information is lost or leaked.

4 Information Kept and Distributed by Colleges and FERPA Protections Thereof

4.1 Directory Information

Directory information is a category of data maintained by educational institutions that "would not generally be considered harmful or an invasion of privacy if disclosed."[2] This data can include the name of the student, his or her address, telephone number (land line or mobile), data and place of birth, and major or other concentration.

By extension of this personal information, student e-mail addresses, hometown, and family data can be acquired from other public sources. Directory information is typically indexed for public searches, via services like `directory.tufts.edu`. FERPA does not require colleges to receive consent

[1] *Data Breaches by Industry.* Accessed: 2015-12-14. CSID. URL: `https://www.csid.com/resources/stats/data-breaches-by-industry/`.

[2] *Family Educational Rights and Privacy Act Regulations.* Accessed: 2015-12-10. Department of Education. 2012. URL: `http://www2.ed.gov/policy/gen/guid/fpco/pdf/2012-final-regs.pdf`.

to release this information. Instead, students must specifically opt out.

4.2 Education Records

FERPA's definition of an education record is extremely broad. Any record that is "directly related to a student"[3] or "maintained by an educational agency or institution, or by a party acting for the agency or institution"[4] is considered an education record, except for law enforcement records,[5] employment records of non-students,[6] records about a former student after that student has left the institution,[7] and others. Thus, any record that includes a student's grades, transcript, class list, course schedule, financial records, or disciplinary information is an educational record.

4.3 Personally Identifying Information

According to FERPA, personally identifying information includes any information that could identify a specific student. This data includes the identifiers that are also classified as directory information, and also includes any personal identifier (e.g. a social security number, school username, or student id number),[8] and any set of information, which would allow a "reasonable person in the school community to identify the student with reasonable certainty."[9]

[3] *Ferpa: An Introduction to the Family Education Right to Privacy Act.* Accessed: 2015-12-13. University of Virginia. URL: `http://www.virginia.edu/registrar/documents/FERPA.pdf`, p. 8.

[4] *Ferpa: An Introduction to the Family Education Right to Privacy Act*, p. 8.

[5] *Ferpa: An Introduction to the Family Education Right to Privacy Act*, p. 9.

[6] *Ferpa: An Introduction to the Family Education Right to Privacy Act*, p. 9.

[7] *Ferpa: An Introduction to the Family Education Right to Privacy Act*, p. 10.

[8] *Ferpa: An Introduction to the Family Education Right to Privacy Act*, p. 14.

[9] *Ferpa: An Introduction to the Family Education Right to Privacy Act*, p. 14.

4.4 Legal Conditions for Disclosure of Educational Records and Personally Identifying Information

In general, universities cannot disclose educational records without student consent. Consent is defined under FERPA as having been given if a student provides written consent which specifies what records can be disclosed and identifies to whom the disclosure may be rendered.[10] However, there are circumstances in which this protection does not apply. Most notably, educational records can be disclosed without consent if all personally identifying information has been removed;[11] FERPA describes this process as 'de-identifying' a document. Once a document has been de-identified, the protections administered for student data no longer apply.

Student data with identifying information can also be distributed under certain FERPA regulations. Schools can disclose student data to third parties conducting studies on their behalf,[12] to authorized government officials when pursuant to an audit or evaluation of educational policies,[13] and to any school official with a "legitimate educational interest,"[14] including contractors, clerical workers, information systems specialists, and others.[15]

4.5 The Lifespan of Student Data

4.5.1 Data Distribution and Destruction

After student data is created and stored by an institution, FERPA regulates the circumstances under which it can pass between parties. When student data is disclosed to a new party, FERPA requires that the receiving party

[10] *Family Educational Rights and Privacy Act Regulations*, p. 13.

[11] *Family Educational Rights and Privacy Act Regulations*, p. 18.

[12] *FERPA Frequently Asked Questions.* Accessed: 2015-12-13. Department of Education. URL: `http://familypolicy.ed.gov/faq-page`.

[13] *FERPA Frequently Asked Questions.*

[14] *FERPA Frequently Asked Questions.*

[15] *FERPA Frequently Asked Questions.*

be governed by, at minimum, the same restrictions governing the disclosing party with regard to disclosure. When the receiving party is a school official, FERPA does not prescribe steps by which this data must be managed, nor does it require that the school official take steps to destroy the data when it is no longer needed.[16] FERPA instead leaves standards for information security and data destruction to the institution primarily responsible for the records.[17] FERPA does mandate disclosed data be destroyed when it is no longer useful if the receiving party has been granted the data to conduct a study or audit. However, FERPA does not mandate a technical standard by which data be destroyed,[18] leaving it to the managing institution to determine a reasonable standard. While the technical process of data destruction is well established, the lack of clear requirements in FERPA with regard to its use make it unlikely that data destruction practices are consistent across schools.

4.5.2 Data Storage and Transmission

FERPA "does not require specific security controls"[19] for data in storage or in transit, including student data in emails, databases, digital documents, and other electronic forms. Unencrypted data storage on personal devices does not inherently provide a security risk if the device is never compromised, lost, or stolen, but this is rarely a good standard by which to measure a security plan. Large-scale data storage in a shared capacity, for instance in a database, is likely to be safer to be left unencrypted due to the higher barrier for entry into the system. However, unencrypted data in these systems can be

[16] *Best Practice for Data Destruction*. Accessed: 2015-12-12. Department of Education. 2014. URL: `http://ptac.ed.gov/sites/default/files/Best%20Practices%20for%20Data%20Destruction%20(2014-05-06)%20[Final].pdf`, p. 2.

[17] *Best Practice for Data Destruction*, p. 2.

[18] *Best Practice for Data Destruction*, p. 2.

[19] *FERPA: Data & Transport Security Best Practices*. Accessed: 2015-12-14. Privacy Technical Assistance Center. URL: `http://raymarshallcenter.org/files/2013/04/Data_and_Transport_Security_PTAC.pdf`, p. 2.

easily retrieved via forensics if the storage media are not disposed of correctly and securely.

Data in transit is often easiest to acquire illicitly or leak inadvertently. It is harder to reason about the potential vulnerabilities of a computer network, particularly one where data may be stored, cached, or archived along the way, and the various means by which data can be acquired as it passes from one computer to another are extremely challenging to guard against. Because of this, network transmission of data is a context that demands encryption in order to be protected.

4.5.3 Data Access and Privileges

One of FERPA's core requirements is that disclosures only be made to school officials deemed to have a "legitimate educational interest"[20] in the data. This language maintains a clear standard of access; while any school employee can be considered a school official, data is only disclosed when necessary. This helps assuage a possible vulnerability: if any school- affiliated person, including temporary employees, contractors, and consultants, can access privileged data, then a single vulnerable device owned by any school official might be a catalyst for an information leak. By carefully restricting access to sensitive material, schools can manage these risks more effectively. However, this assertion is predicated on the assumption that student data access is managed with a sophisticated notion of privileges: if all school employees are treated equally by the security policy, the policy is not as effective.

5 Non-Prescriptive Regulations

By opting not to prescribe specific security measures in law, the writers of FERPA attempted to strike a delicate balance. With overly prescriptive

[20] *Family Educational Rights and Privacy Act Regulations*, p. 14.

rules for data security, FERPA might have set a standard that would not be protective enough, but would be the sole approach to student data security. However, the current requirements for student data security do not provide possible approaches to protection at all, instead running the risk that schools will be unable or unwilling to provide systems that are adequately sophisticated to protect their students. Organizations such as the Privacy Technical Assistance Center, which provide support and systems that schools can choose to adopt, fill a needed gap in the security infrastructure, but might be underutilised due to costliness or implementation difficulty. Third party solutions can mitigate some concerns of implementation difficulty, but are not necessarily open-source, and are therefore challenging to audit and risky to use.

6 Action Items

6.1 Produce an Impactful, Rigorous Security Policy at an Institutional Scale

Because of the variety of points inside and outside of an organization at which student data can be compromised or leaked, clearly defined, rigorously secured techniques must be employed at an institutional level. Use of Fair Information Practice Principles, the "widely accepted framework of defining principles to be used in the consideration of systems, processes, or programs that affect individual privacy,"[21] is crucial to institutions as they consider their security policy at every level.

[21] *Fair Information Practice Principles*. Accessed: 2015-12-14. NIST. URL: `http://www.nist.gov/nstic/NSTIC-FIPPs.pdf`.

6.2 Utilize Modern Standards for Encryption

6.2.1 Protect Stored Data

As hardware and software vendors increasingly adhere to a standard of easily usable storage-level encryption, protecting student information through encryption is not the technical challenge it once was. By mandating the use of secure storage features throughout the digital infrastructure of a school, policy-makers can be better assured of the safety of the data.

6.2.2 Protect Data in Transit

The infrastructure for network-level security has developed continuously as bandwidth and latency have been reduced. Modern network security is not prohibitively slow or bandwidth-intensive, and can go great lengths in protecting confidential material as it travels over the internet. Enforced requirements for encryption in inter-computer communication of student data helps prevent major information leaks as data passes from computer to computer.

6.3 Be Aware of Information Leaks in Directory Information

The scope of directory information is clearly defined under FERPA, and leaks of information through directory information can lead to FERPA violations. For instance, usernames assigned by a university typically do not qualify as directory information, so a process that allows one to correctly identify a username belonging to a particular student may constitute an information leak. In the supporting material, we provide an example of how to obtain this information in the file 'utln.py,' which utilizes an information leak at `directory.tufts.edu` to associate student names with student usernames.

6.4 Maintain Clear Standards for Consensual Disclosure

Traditional techniques for establishing consent, e.g. signatures, are inconvenient in a digital context. However, verifying that consent has been given is still critical. By using cryptographic signatures, it is possible to verify student consent for the disclosure of their information.

6.5 Partition Access to Data

By introducing logical restrictions on data access to a system, it is possible to avert leaks caused by inadvertent unpermitted access. Granting general access based on privilege level is a solution, while specifying access to specific resources based on identity is a stronger, but more challenging option. Utilizing strong protections based on privilege is necessary in order to prevent data leaks.

6.6 Maintain and Enforce Clear Requirements for Data Stewardship and Destruction

FERPA mandates that student data not be disclosed without the receiving party agreeing to requirements about protecting this data. When applied to parties other than school officials, these requirements must include the same non-disclosure standards followed by the primary holder of the data, and also must demand the data be destroyed when it is no longer needed. To protect student data in this context, it is vital that the third party has a clear strategy for obeying these requirements, and a way to demonstrate that the data has been disposed of correctly.

Correct data disposal must be executed through a secure, unrecoverable means. Disposal should not be conducted through one-way encryption, disk

formatting, or traditional file delection,[22] as the potential for correct recovery is too great. The exclusive use of true irrversible techniques, including information randomization and disk destruction, should be required for data disposal.

7 Conclusion

The current requirements of the Family Education Right to Privacy Act strongly describe the appropriate and inappropriate circumstances in which student data can be disclosed. However, the lack of clear recommendations and requirements for information security in the context of digital systems raise the barrier for effective management of information risks. By improving the standards to which educational infrastructure is held, FERPA and related laws will improve the safety and consistency of information stewardship in post-secondary institutions.

References

[1] *Data Breaches by Industry*. Accessed: 2015-12-14. CSID. URL: https://www.csid.com/resources/stats/data-breaches-by-industry/.

[2] *Family Educational Rights and Privacy Act Regulations*. Accessed: 2015-12-10. Department of Education. 2012. URL: http://www2.ed.gov/policy/gen/guid/fpco/pdf/2012-final-regs.pdf.

[3] *Ferpa: An Introduction to the Family Education Right to Privacy Act*. Accessed: 2015-12-13. University of Virginia. URL: http://www.virginia.edu/registrar/documents/FERPA.pdf.

[4] *FERPA Frequently Asked Questions*. Accessed: 2015-12-13. Department of Education. URL: http://familypolicy.ed.gov/faq-page.

[22] *Best Practice for Data Destruction*, p. 7.

[5] *Best Practice for Data Destruction*. Accessed: 2015-12-12. Department of Education. 2014. URL: http://ptac.ed.gov/sites/default/files/Best%20Practices%20for%20Data%20Destruction%20(2014-05-06)%20[Final].pdf.

[6] *FERPA: Data & Transport Security Best Practices*. Accessed: 2015-12-14. Privacy Technical Assistance Center. URL: http://raymarshallcenter.org/files/2013/04/Data_and_Transport_Security_PTAC.pdf.

[7] *Fair Information Practice Principles*. Accessed: 2015-12-14. NIST. URL: http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.