# Fixing FERPA: A Survey of Current Student Directory Sharing Practices at U.S. Universities

Katherine Quintanilla
*Tufts University*

Sarah Radway
*Tufts University*

Dan Votipka
*Tufts University*

## 1 Introduction

The Federal Education Rights and Privacy Act of 1974 (FERPA) has not coped well as student records become digital. Other works have identified how FERPA fails to account for emerging technologies: such as in-class video recordings [5] and cloud storage/use [3]. In this work, we consider a special class of student records: student directory information.

Universities share student directory information in two ways: 1) through *online publications*—many schools have publicly available, online directories, and 2) through *offline requests*, where information is solicited from school registrars. According to FERPA, the university does not need student permission prior to sharing directory data.

Directory information's definition varies between schools from student contact information (e.g., phone number, email address) to student residential address and date and place of birth. The Department of Education describes directory information as data that which "would not generally be considered harmful or an invasion of privacy if disclosed" [6].

When FERPA was passed in 1974, it is unlikely legislators were thinking about the Internet's impact, as it was yet to be created. It is therefore understandable that sharing this information could have been considered harmless—contemporaneous discussions examine how large-scale digital data collection or surveillance in the classroom were unthinkable when FERPA was originally passed [5]. Even when FERPA was last modified in 2012, the public was largely unaware of the emerging targeted advertising profit models of companies like Google or Meta, or of data brokers', e.g., Acxiom and LexisNexis, mass-scale data collection practices. Surveillance capitalism has dramatically changed the value of available data [8]. There is now motivation to learn as much about a person as possible to target advertising. This has allowed new privacy risks to emerge surrounding student privacy–namely, the mass sale, sharing, and use of student data. Student directory data can be aggregated from online directories, obtained from registrars under misleading contexts, or even sold by universities—while the Protection of Pupil Rights Amendment (PPRA) oversees the sharing of elementary and secondary (K-12) students' data by schools [7], universities do not face these constraints [1].

Further, due to the wealth of user data available online, students also face increased risks of stalking and harassment [2, 4]. In the face of these types of threats, it becomes less easy to argue that disclosure of student directory information does not create privacy harms. Therefore, in this work, we will address the following questions regarding University student directory practices:

**RQ1:** What are universities' current practices for student directory information data sharing?

**RQ2:** What are current opt-out processes?

**RQ3:** What are the privacy harms associated with current practices?

Across our investigations, we see that different universities used vastly different practices surrounding directory publication, sharing, and student notification. Some of these practices leave students with little control over the use and publication of their personal information. Based on our results, we propose policy and technical recommendations to allow students to make informed decisions about their personal data's use.

## 2 RQ1: What are universities' current practices for student directory information data sharing?

For student directory information, FERPA sets an upper limit on what information may be shared; schools then choose what


*USENIX Symposium on Usable Privacy and Security (SOUPS)* 2023.
August 6–8, 2023, Anaheim, CA, USA

information below that limit to make available. Therefore, we set out to understand not just what FERPA *permits* to be shared, but how schools are implementing FERPA *in practice*.

**Method:** First, we focus on information available in online public directories, and then on what information is available offline by request. We survey the top 100 universities' current directory publication practices; therefore, our results should be considered primarily as related to more prestigious, well-staffed universities. For each university, we searched for a publicly accessible student directory using the query "<UNIVERSITY NAME> student directory". We then manually reviewed the first page of Google's results to determine whether any page contained a student directory.

**Results:** We find that many schools have public directories containing student contact information. Further, and more importantly, there is extensive student information available via offline request, ranging from phone numbers and addresses, to date and place of birth. The information that can be requested offline is listed in the university's definition of directory information, typically available online as a part of their FERPA notice. However, registrars are not required to fulfill all requests.

## 3 RQ2: What are current opt-out processes?

FERPA requires students be able to remove themselves from university directories. However, FERPA does not mandate a particular opt out process.

**Method:** We investigated the opt-out process of each university, using an iterative open-coding approach. We focus on the following questions:

- What is the opt-out mechanism? What level of control do students have over what data is shared and who data is shared with?
- How are students required to indicate their wish to opt out? Is opting out completed through an online or paper form, written statement, verbally in person? Are students required to speak with an administrator prior to submitting their opt-out request?
- How is the choice to opt out framed in university communication? What consequences of opting out are presented in notices and forms?
- What restrictions are placed on students' ability to opt out? Is opting out limited to specific time periods (e.g., start of the semester) or required on a recurring basis?

**Results:** We found that many universities make opting out challenging, and use practices likely to discourage students from opting out. For example, the most common opt-out approach was to let students request a 'FERPA Block' (N=40), which prevents *any* student directory information from being released without the student's expressed consent. This is the least flexible option, as students must either block the university from revealing all data with all third parties, or consent to the university revealing all their directory information to any third party the university deems acceptable. Few universities provide specific context-driven sharing options, allowing students to choose in which specific situations they want their data to be used (ex. in the commencement book, but not with third parties).

Similarly, we found that FERPA notices and opt-out forms focused exclusively on negative consequences. We did not identify any institutions that gave a reason students may want to opt out. Conversely, 52 universities gave at least one consequence of opting out, ranging from not having their name read at commencement to having mail be withheld. Throughout our investigations, we found current student directory data sharing practices lack clear standards and effective student control.

## 4 RQ3: What are the privacy harms associated with current practices?

Finally, to demonstrate the impact of the data sharing practices discussed above, we mapped student directory data to data types discussed in prior literature, which examined the harms resulting from their publication. Then, to demonstrate the threats posed by public online directories, we conduct a case study, in which we use database matching to match a target University's directory records with Tinder profiles, with a success rate of about 10%. This allows an attacker to align students' personal information with information regarding gender and sexual identity. By submitting FOIA requests of public universities, we also show that advertising firms and data brokers currently access some universities' offline directories.

While there are valuable reasons for sharing student directory information, recent increases in doxxing, stalking, and other harassment may necessitate greater limits on directory information. Similarly, organizational requests should be scrutinized to reduce access for data brokers, unless students opt in to this sharing. As can be seen in the opt-out processes currently in place, students have minimal control over the use of their data. Providing effective notice and reasonable choices for students via scenario-based access control systems will allow students to make informed decisions about the sharing of their data.

## References


[1] Lynn M Daggett. Ferpa in the twenty-first century: Failure to effectively regulate privacy for all students. *Cath. UL Rev.*, 58:59, 2008.

[2] Karen McVeigh. Cyberstalking'now more common'than face-to-face stalking. *The Guardian*, 13:31, 2011.

[3] Alexander R Schrameyer, Tracy M Graves, David M Hua, and Nile C Brandt. Online student collaboration and ferpa considerations. *TechTrends*, 60(6):540–548, 2016.

[4] Francesca Stevens, Jason RC Nurse, and Budi Arief. Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, 24(6):367–376, 2021.

[5] Julie Underwood. Under the law: You say 'records,'and i say 'data'. *Phi Delta Kappan*, 98(8):74–75, 2017.

[6] United States Code. Title 34 Subtitle A Part 99 Subpart D §99.37. https://www.ecfr.gov/current/title-34/subtitle-A/part-99/subpart-D/section-99.37, 1974.

[7] U.S. Department of Education. PPRA Model General Notice of Rights. https://studentprivacy.ed.gov/resources/ppra-model-general-notice-rights, 2020.

[8] Shoshana Zuboff. *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books, 2019.