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

Katherine Quintanilla, Sarah Radway, Dan Votipka (Tufts University)

Abstract

- FERPA allows ***student directory information*** to be shared with outside parties without explicit student permission, and without stating why, or with whom data will be shared.
- We investigate the top 100 universities' practices on student directory information sharing, to understand potential privacy harms, focusing on data sharing practices and students' ability to opt-out.

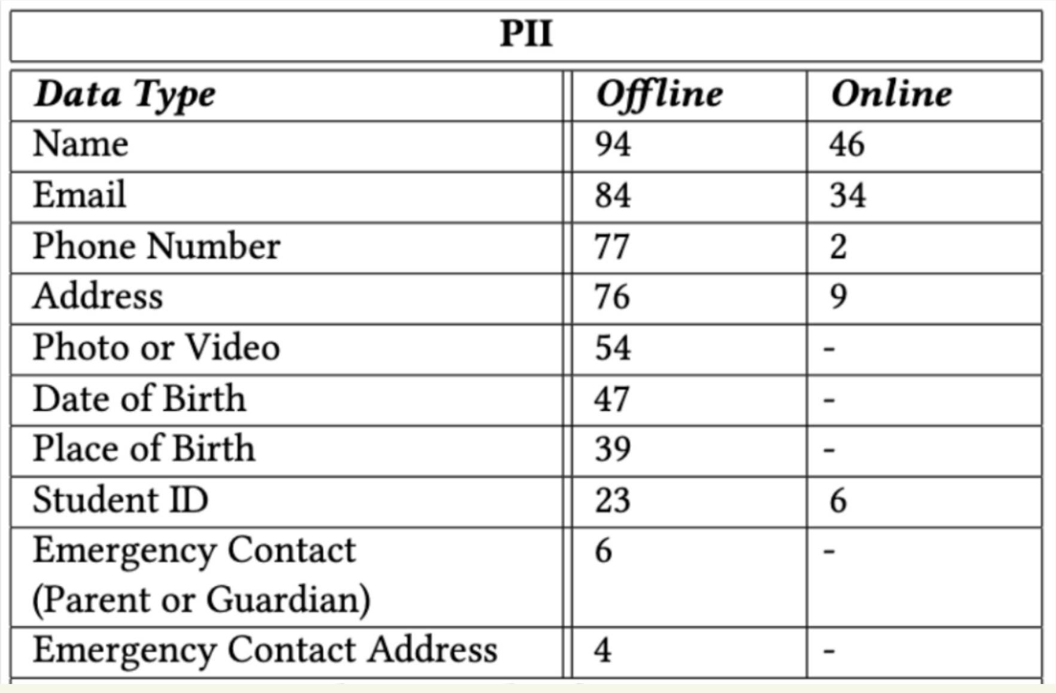
RQ1:What are the 100 universities' current practices surrounding student directory information data sharing?

Directory information is shared in 2 ways:

(1) ONLINE. Universities often have directory information available online.
(2) OFFLINE. Directory information can be requested from the registrar.

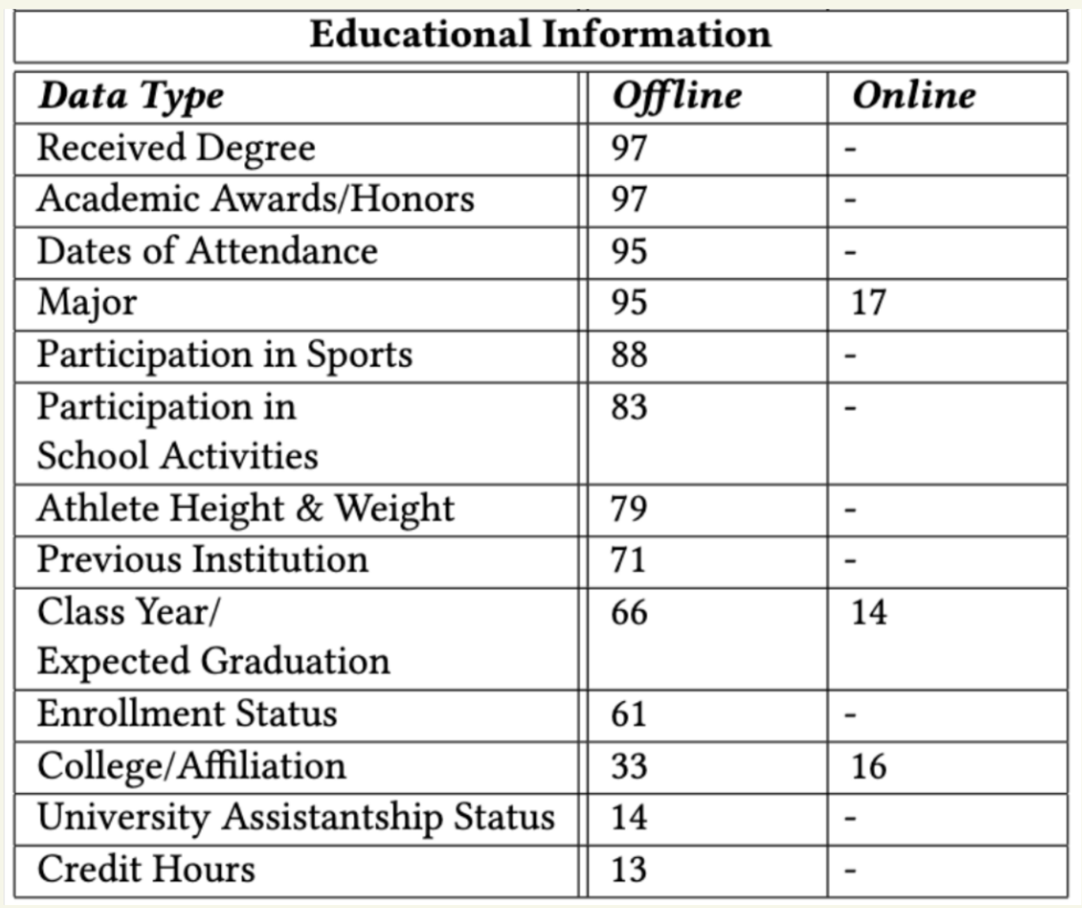
METHOD We searched to identify what types of student information are able to be shared online and offline by the universities. We corroborated our searches by contacting registrars directly.

RESULTS We see that a wide range of PII and educational information are able to be shared online and offline.



PII

Data Type	***Offline***	***Online***
Name	94	46
Email	84	34
Phone Number	77	2
Address	76	9
Photo or Video	54	-
Date of Birth	47	-
Place of Birth	39	-
Student ID	23	6
Emergency Contact (Parent or Guardian)	6	-
Emergency Contact Address	4	-

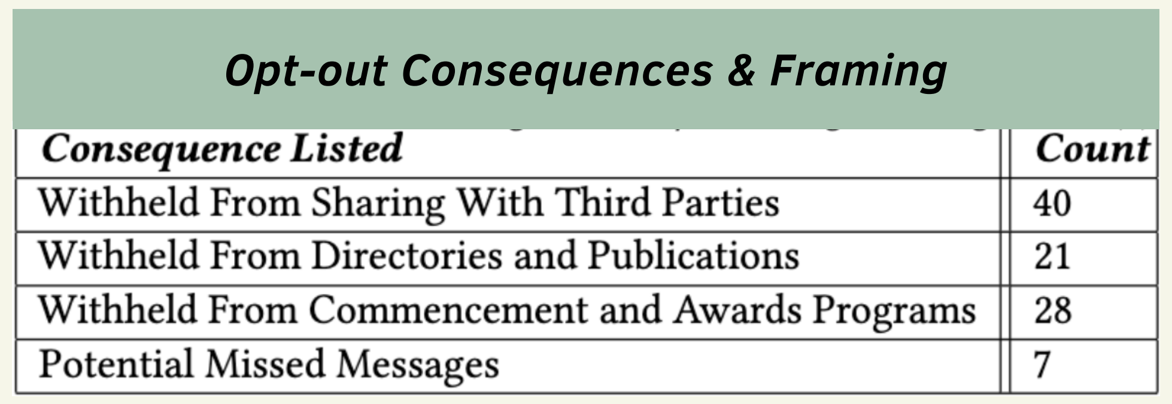


Educational Information

Data Type	***Offline***	***Online***
Received Degree	97	-
Academic Awards/Honors	97	-
Dates of Attendance	95	-
Major	95	17
Participation in Sports	88	-
Participation in School Activities	83	-
Athlete Height & Weight	79	-
Previous Institution	71	-
Class Year/ Expected Graduation	66	14
Enrollment Status	61	-
College/Affiliation	33	16
University Assistantship Status	14	-
Credit Hours	13	-

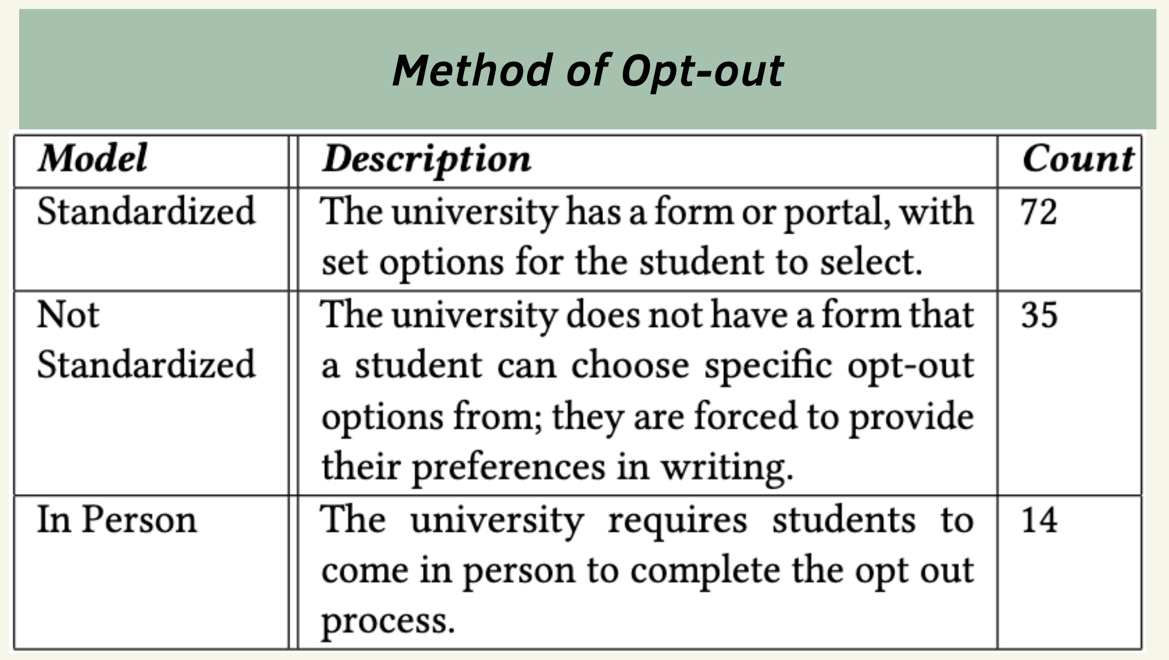
RQ2: What are the current opt-out processes?

METHOD We gathered information about opt-out processes by: (1) emailing each of the universities' registrars, and (2) reviewing relevant university websites. We followed an iterative open coding approach, ultimately focusing on the level of control, method, and consequences associated with opting out at each university.



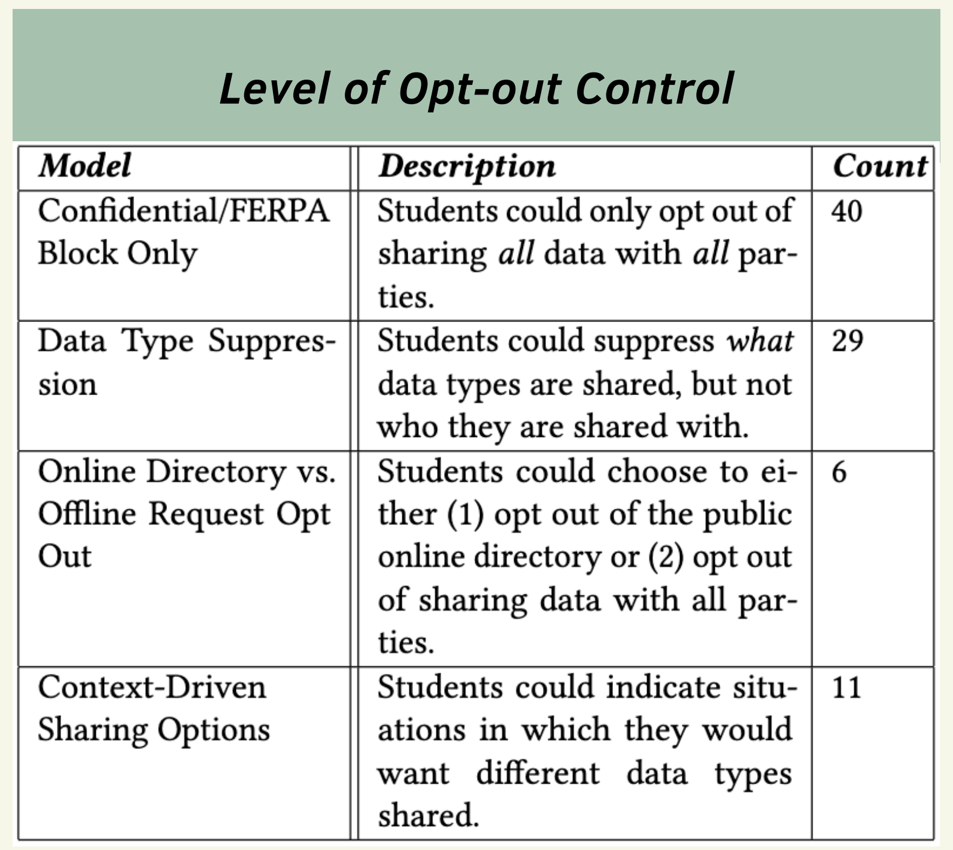
Opt-out Consequences & Framing

Consequence Listed	***Count***
Withheld From Sharing With Third Parties	40
Withheld From Directories and Publications	21
Withheld From Commencement and Awards Programs	28
Potential Missed Messages	7



Method of Opt-out

Model	***Description***	***Count***
Standardized	The university has a form or portal, with set options for the student to select.	72
Not Standardized	The university does not have a form that a student can choose specific opt-out options from; they are forced to provide their preferences in writing.	35
In Person	The university requires students to come in person to complete the opt out process.	14



Level of Opt-out Control

Model	***Description***	***Count***
Confidential/FERPA Block Only	Students could only opt out of sharing *all* data with *all* parties.	40
Data Type Suppression	Students could suppress *what* data types are shared, but not who they are shared with.	29
Online Directory vs. Offline Request Opt Out	Students could choose to either (1) opt out of the public online directory or (2) opt out of sharing data with all parties.	6
Context-Driven Sharing Options	Students could indicate situations in which they would want different data types shared.	11

RESULTS

- No institutions gave a reason students may want to opt-out, yet 52 gave at least one consequence of opting-out.
- Most universities did not have contextual approaches, but rather, use an all or nothing approach through offering FERPA Block, or only allow students to hide certain data types.
- Most universities have a standardized process of opting out through a form or student portal, but a considerable amount make students either write their preference and submit to the Office of the Registrar or go to the office in person.

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

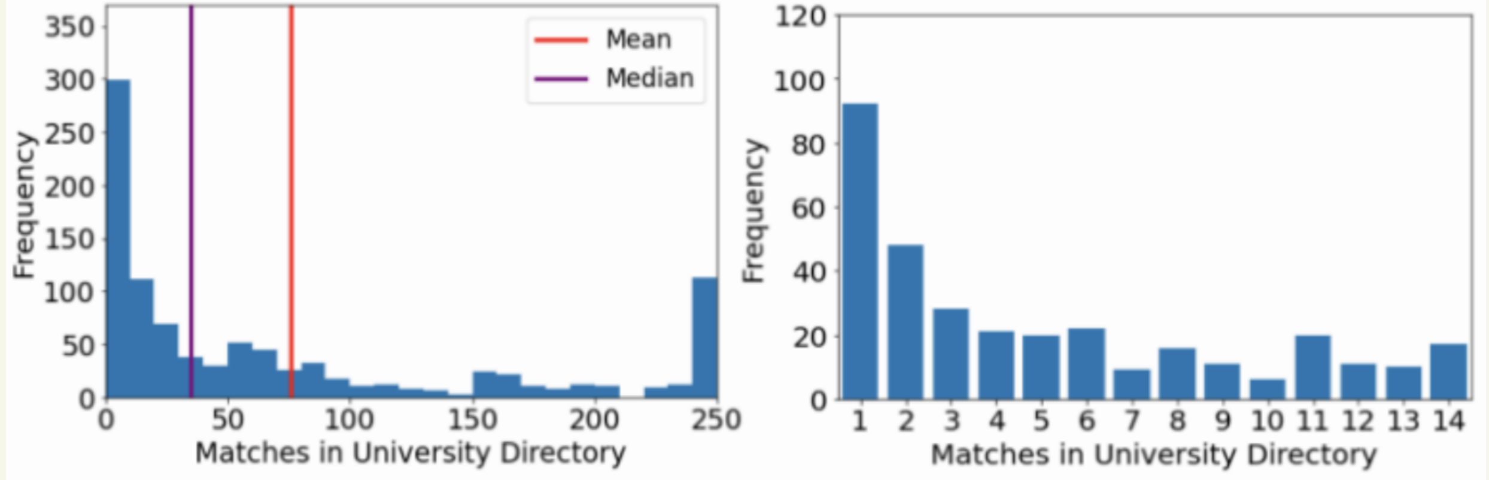
TinderU Database Matching*

We demonstrate the feasibility of limited attackers performing large-scale database matching with student directories.

METHOD We collected and parsed TinderU profiles in a university town, programmatically searching the university's directory for entries matching our 980 collected Tinder profiles, based upon first name matches.

RESULTS Using this method, we had a 10% identification rate.

**We recieved IRB clearance for this portion of the study.*



FOIA Requests

METHOD We submitted FOIA requests to 32 public universities, requesting records of who had requested student directory information in the last 6 months.

RESULTS At the time of submission only received responses from 6 universities; we are able to see some trends emerge:

- 3/6 universities shared data **with advertisers and marketing firms**, including FlyteDesk and ASL Marketing.
- 3/6 universities shared data with **data brokers**, notably, LexisNexis, a which specializes in risk management.

This confirms that data brokers are using offline requests to obtain student directory information.

Recommendations & Future Work

- Universities often make student directory information publicly available. While there are valuable reasons for sharing this data, with recent increases in doxxing, stalking, and other harassment, students may benefit from greater limits on directory information. Similarly, organizational requests should be scrutinized to reduce access for data brokers, unless students opt in to this sharing.
- Dark patterns likely limit student understanding of the privacy harms of current data sharing practices. 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.
- We plan to carry out a user study, examining how students make decisions surrounding directory information sharing under current opt-out frameworks. By presenting students with data usage conditions, assessing their comfort, and then presenting them with one of the various opt-out frameworks, we can understand their privacy considerations, to determine whether students continue to opt in even if they're concerned.