An Investigation of US Universities' Implementation of FERPA Student Directory Policies and Student Privacy Preferences

Sarah Radway
sradway@g.harvard.edu
Harvard University
Cambridge, Massachusetts, USA

Katherine Quintanilla
katherine.quintanilla@tufts.edu
Tufts University
Medford, Massachusetts, USA

Cordelia Ludden
cordelia.ludden@tufts.edu
Tufts University
Medford, Massachusetts, USA

Daniel Votipka
dvotipka@cs.tufts.edu
Tufts University
Medford, Massachusetts, USA

ABSTRACT

The Family Education Rights and Privacy Act (FERPA) is intended to protect student privacy, but has not adapted well to current technology. We consider a special class of student data: directory information. Unlike other FERPA-controlled data, directory information (e.g., student names, contact information, university affiliation) can be shared publicly online or by request without explicit permission.

To understand this policy's impact, we investigated 100 top-ranked US universities' directory information sharing practices, finding they publish student contact information online, and provide PII offline by request to many parties, including data brokers. Universities provide limited opt out choices, and focus on negative effects when advising students about opting out. Lastly, we evaluate student preferences regarding the identified directory practices through a survey of 991 US university students. Based on these results, we provide recommendations to align directory practices with student privacy preferences.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; **Privacy protections**.

ACM Reference Format:
Sarah Radway, Katherine Quintanilla, Cordelia Ludden, and Daniel Votipka. 2024. An Investigation of US Universities' Implementation of FERPA Student Directory Policies and Student Privacy Preferences. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 35 pages. https://doi.org/10.1145/3613904.3642066

1 INTRODUCTION

The Family Education Rights and Privacy Act of 1974 (FERPA) is a doctrine that advocates for collective student rights and privacy. However, it has not coped well with technological advancement; in particular with new privacy threats from student records digitization. Other works have identified how FERPA fails to account for emerging technologies: such as in-class video recordings [82], ID card swipe records to track on-campus movement [53], cloud storage/use [66], and learning analytics [60]. In this paper, we consider a special class of student records: student directory information.

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 defines directory information as data that, "would not generally be considered harmful or an invasion of privacy if disclosed" [84]. Universities share student directory information in two ways: 1) through *online publications*, typically via publicly available, online directories, and 2) through *offline requests*, where information is solicited from school registrars. According to FERPA, universities do not need student permission prior to sharing directory data.

When FERPA was passed in 1974, legislators likely did not think 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—examination of contemporaneous discussions has shown how large-scale digital data collection or surveillance in the classroom were unthinkable when FERPA was originally passed [82]. The Internet has dramatically changed the availability of user data, in particular, to bad actors. Users now face increased risks of online hate and harassment [48, 67, 75, 79]; sexual harassment, stalking, physical threats, and name calling all continue to grow online [90]. These threats increase when a wealth of personal information is available online.

Surveillance capitalism has also dramatically changed available data's value [98]. 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. Today, organizations have the techniques and motivation to gather as much information about users as possible. This has allowed new privacy risks to emerge, as organizations seek to obtain sensitive student data. Student directory data can be aggregated from online directories, obtained from registrars, or even potentially sold by universities—while the Protection of Pupil Rights Amendment (PPRA) oversees the sharing of elementary and secondary (K-12) students' data by schools [88], there are no such constraints for universities [18].

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642066

Given these threats, it is more difficult to argue that student directory information disclosure does not create privacy harms. However, there are many use cases in which sharing this data may be necessary or useful, ranging from employment verification to university event registration.

Therefore, we investigate how to best balance these functional requirements with potential student privacy concerns, addressing the following questions regarding university student directory practices:

(RQ1) What are universities' current practices for sharing student directory information?

FERPA sets upper bounds on what directory information can be shared, but schools can further limit sharing. Therefore, we investigated not just what FERPA *permits* to be shared, but how schools implement FERPA *in practice*. First, we focused on what information is available in online public directories, and then on what information is available offline by request. We surveyed 100 top-ranked universities' current practices, finding many schools have public directories containing student contact information. Further, and more importantly, there is extensive student information available via offline request. Using FOIA requests, we showed data brokers currently access some universities' rich offline directories, accessing students' emails, mailing addresses, academic statuses, and more.

(RQ2) How are students informed of potential effects of opting out, and 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. We investigated the opt-out processes of the 100 universities, finding university practices vary widely in their method of opt-out, framing, and level of student control.

(RQ3) What are students' privacy preferences regarding directory information, and how well do current systems address these preferences? We conducted a between-subjects vignette-based controlled experiment with 991 US college students. Participants were assigned hypothetical directory information definitions, data sharing policies, and opt-out mechanisms drawn from our review of current university practices. Then we asked students to indicate what sharing they would like to opt out of, using their assigned opt-out mechanism, and asked them to rate their level of comfort with their opt-out choices. We found sharing policy transparency strictly improves student comfort; students were most comfortable with data sharing internal to the university, but were also comfortable with third-party sharing in certain contexts. Students were least comfortable with all-or-nothing opt out systems, but there was no consensus regarding the correct level of additional control; and that providing all effects of opt-out decisions (i.e., loss of services students may use and privacy costs) is necessary to allow students to make well informed opt out choices.

Across our investigations, we see universities implemented vastly different practices surrounding directory publication, sharing, and student notification. Many of these practices do not align with students' preferences, leaving students uncomfortable, and with little control over their personal information's use and publication. Based on our results, we propose recommendations for both policy makers and universities, to enable students to make informed decisions about the use of their personal data.

2 BACKGROUND

2.1 What is FERPA?

FERPA is a U.S. Federal Law that protects student record privacy. These records range from personally identifiable information to academic records, to counselor observations. FERPA is intended to give students and parents comfort that students' personal information will not be shared or published without student or parent (for students under 18) permission.

FERPA in many ways minimizes the burden on students and parents—not only in terms of enforcement but in terms of decision-making. Much of FERPA's legislation places the burden of interpretation on institutions—which ultimately has the greatest impact on student privacy; as Zeide puts it, "FERPA creates a structure in which institutions, not individuals, manage student privacy" [97]. We examine how this legislative hands-off approach impacts downstream implementation and enforcement surrounding student directories.

2.2 What Does FERPA Say About Student Directories?

While FERPA mandates tight control over student data, FERPA §99.31(11) provides a specific exception—student consent is not needed for student directory information disclosure [85]. The exact data types considered directory information varies between universities; in Section 3, we investigate university definitions. However, §99.3 suggests directory information includes data such as "name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance" [87].

Schools are required by §99.37(a) to inform students of their definition and the opt-out timeline via a "public notice" [84]. What is meant by public notice, however, varies greatly, as "the actual means of notification…is left to the discretion of each school" [89]. As we discuss in Section 4, this leads to significant differences in notification and opt-out procedures between universities.

Lastly, while universities must provide notice of what data can be shared, FERPA does not require schools to inform students who data is shared with, or reasons for data sharing [84]. As we show in Section 3, universities vary greatly in what information they share, how they share it, and who they share it with.

2.3 Related Work

Risks not addressed by FERPA. Previous works identify privacy harms not appropriately addressed by FERPA, largely related to student records' digitization. Researchers have examined the potential privacy harms associated with the big data ecosystem [49, 53], cloud-based collaboration tools, and other third-party classroom technologies [9, 41, 66, 97], including learning analytics and educational technologies [3, 35, 46, 52, 53, 56, 62, 68, 69, 95]. However, these works do not address privacy harms arising from student directory information.

Legislation expanding student data sharing. Previous work also examined how recent legislation has expanded student directory record availability [18, 53, 61, 82, 97]: the 9/11 Patriot Act and No Child Left Behind Act require directory information be shared for terrorism investigations and military recruitment respectively [18]. In 2008, the School Official Exception (SOE) allowed third parties to access all student data under the pretense of educational cooperation or benefit. Prior works largely found issues with the SOE, which provided third parties access to student data, without disclosure or consent [18, 53, 61, 74, 82, 97]. However, the SOE is very different from the directory information exception we examine; universities must have a recorded justification for sharing student records under the SOE (directory information requires no justification), and access is given to the entirety of student records (rather than just directory information).

Policy compliance measurement studies. Prior work has measured the implementations and reactions to other policies, such as the GDPR [17, 19, 40, 45, 59, 96], HIPAA [8], and CCPA/CPRA [30, 64, 94]. By conducting large-scale measurements, this research has demonstrated the difference between what legislation dictates, and organizations' practical applications. Many of these studies have suggested even compliant organizations frequently suffer from a lack of transparency and mechanisms to support legislation effectively. Our results similarly show how FERPA compliance does not equate to effective student privacy protection.

FERPA measurement studies. Liu compares university FERPA Notices to the government's model FERPA notice, and analyzes their readability [43]. Additionally, others have investigated staff understanding of student record sharing policies under FERPA [16, 23, 24] and FIPPA (the Canadian FERPA equivalent) [20]. However, these prior measurements do not consider student directory information.

Most closely related to our study, a law review by Russell et al. investigated the collection and use of student data by data brokers, focusing on K-12 schools [63]. Among other data sources, they attempted to identify if directory data was given to data brokers by schools, but did not find any such evidence.

However, K-12 schools are governed by PPRA in addition to FERPA, which introduces a more strict legal framework for data sharing. Therefore, our work is the first to comprehensively investigate the privacy threats surrounding student directory information at the university level.

Learning Analytics and Student Privacy. Researchers also have examined student privacy perspectives, mainly as applied to learning analytics—the collection and use of information about students' learning, in order to improve future learning. Previous works have identified the privacy threats associated with learning analytics [36, 44, 57], and how trust can be conceptualized regarding data in the educational space, given these privacy threats [13, 37, 71]. Many of the threats identified overlap with the privacy threats associated with student directory information, specifically regarding concerns of third party data access.

Previous works have also examined student perspectives and expectations surrounding learning analytics privacy [11, 32, 33, 39, 70, 91, 92]. Relevant to our survey in Section 5, these studies generally find that students are willing to share sensitive data with their learning institutions, as long as it was for their educational benefit [33, 70]; and are more comfortable with collection and use by universities, rather than third parties [39]. We therefore examine whether these findings regarding learning analytics extend to student directory information, despite fundamental differences in the types of data and parties it is shared with.

3 DIRECTORY INFORMATION DATA SHARING PRACTICES (RQ1)

Student directory information is shared in two ways: (1) via student directories published on the internet and (2) offline by requests filed to schools from organizations or individuals. We refer to the first as *online publications* and the latter as *offline requests*. In this section, we investigate what types of student information are available in practice online and offline, and to whom they are available.

3.1 Method

We surveyed the student directory implementations of the top 100 US universities listed on the Forbes 2021 [1] Top Colleges List, which represents the top-ranked US universities [93]. This list is included in the supplementary materials. The Forbes list is generally representative of similar ranking systems, such as the U.S. News, Wall Street Journal, and Princeton Review rankings. According to the Carnegie Classifications of Institutions of Higher Education [2], our universities were all four-year, full-time institutions, which tended to be more selective (n=90) and closely divided between private (n=59) and public (n=41) institutions. Twenty-six were small (<5,000 students), eighteen were medium (5,000 to 15,000 students), and fifty-six were large (>15,000 students).

For each university, we searched for a public student directory, googling "<UNIVERSITY NAME> student directory". We manually reviewed the first page of results, determining whether any page contained a student directory. For each directory we found, we determined the student information provided publicly (e.g., name, phone number, email address, etc.). Most directories we found were search-based, requiring a query matching a record in the directory: we queried by common US first names, like Emily or Michael. We reviewed five directory records for each university to confirm consistency in case some students chose to opt out of data sharing.

Some universities made efforts to limit potential large-scale disclosure resulting from online directories. Namely, thirteen universities would not provide results for queries that had more than a given number of results. These limits were placed at more than 10 (n=1), 20 (n=1), 25 (n=3), 30 (n=1), 50 (n=3), 100 (n=1) or an undisclosed number (n=3) of matches for a given search. In these cases, we queried less common first names, such as Angelica or Devin. In a second method of limiting potential large-scale disclosure, two directories required last names, and one required first and last name; we similarly used common last names until sufficient results were returned. We take note of (1) whether the directory is publicly accessible, (2) how the directory is queried, and (3) what information is available on the directory (name, email, address, class year, etc.). Note, this data was analyzed by a single researcher,

[1] The most recent release at the time

though that researcher iteratively reported back to the full research team to discuss results and refine the review criteria. We do conduct a multi-coder process and we do not evaluate inter-rater reliability (IRR) here as we record the data directly, without interpretation, which does not require IRR evaluation [47].

To understand what data can be shared via offline requests, we obtain universities' FERPA-required published directory information definitions. Using the same process as above, we googled "<UNIVERSITY NAME> FERPA directory information definition." To confirm each page's validity, we checked that the domain matched the university's main web domain and that the website had a valid certificate. We also emailed each university's registrar requesting this notice to corroborate information found online. Our outreach to registrars is discussed in more detail in Section 4. We note what information is defined to be directory information (name, email, address, etc.), and thus *can* be shared offline.

We further submitted Freedom of Information Act (FOIA) requests to identify third party sharing *in practice.* Russell et al.'s law review requested directory information sharing records from six K-12 school districts using FOIA requests with some success [63]. We decided to repeat this effort with universities. We repeated this effort with public universities as they are covered by FOIA doctrines, which require compliance with reasonable requests, sending requests for any third-party directory information sharing in the prior six months (see text in Appendix 7.3).

3.2 Ethical Considerations

We acted to minimize harm in line with Kohno et al. [38] and the Menlo principles [5]. We carefully considered our work's negative impacts; although this study is non-Human Subjects Research (as we are neither contacting nor collecting information about individuals), we were still concerned we may allow bad actors to collect information about individuals by making them aware of vulnerable directory information practices [67]. To prevent this, we minimize risk as much as possible. We do not list which universities are in each policy category, as we believe this information points potential stalkers and other bad actors toward open, easily accessible mechanisms to obtain sensitive student information [67]. We do not collect or release information about specific students in the work. We also provided the investigated universities' registrars with an overview of our findings, in hopes of inducing changes to university practices (Appendix 7.2), and hope to engage with them moving forward throughout any potential policy changes. We are also working in collaboration with public sector advocacy organizations to make our results available directly to students at each impacted institution so we can provide tailored information and instructions for opting out of data collection to those who actually need it. We believe this study will have greater positive impact by increasing student awareness and agency.

Because we were contacting top-ranked schools, these institutions were less likely to be overwhelmed by our requests. We made an effort not to burden registrars; we did not push back on emails and FOIA requests which did not receive responses, and only asked for requests from the last 6 months, to limit the work required.

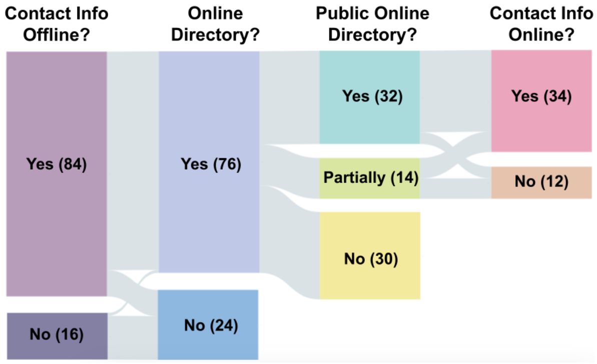


Figure 1: Summary of universities' directory practices, examining whether institutions had public/private online directories, and whether student contact information was defined as available online/offline.

3.3 Limitations

The most prominent limitation is that we consider only 100 top-ranked universities. While we expect our results generalize to schools with similar resources, lower-resourced universities may implement FERPA differently due to budgetary and workforce limits. We performed an initial investigation of the directory practices of 25 universities that were not in the top-rankings, randomly selected from a list of all U.S. universities [83]. While the publicly available policy descriptions we found generally matched those described in Section 3, information about practices was more limited in this sample. For example, none of these universities had publicly available directories, and we could only determine the opt-out method in ten cases. Because information is more sparse for lower-resourced schools, we do not report these results, as they may be misleading or unrepresentative of these schools' practices generally. Thus, our results should be considered primarily in the context of top-ranked universities.

Additionally, our search may have missed directories. However, we do not expect this impacts our analysis. We identified directories or confirmed directories were not public (based on privacy policies or landing page text) for most (76) universities. Further, our search may have identified out-of-date directory information definitions. However, we note that in our attempts to corroborate our findings with registrars, we did not observe any conflicts between the 43 registrar responses and the online definition. We did not find a definition of directory information for three universities.

3.4 Results

Most universities have student directories. Our results are shown in Figure 1, which provides an overview of universities' online directory publication practices. Of the 100 schools examined, we found 76 had student directories. We did not find a definition of directory information for three universities.

Most directories have some publicly available data. We categorized student directories into three groups: (1) hidden directories, requiring a login for access, (2) partially hidden directories, requiring a login to view some data, and (3) public directories, where all

PII			Educational Information		
Data Type	Offline	Online	Data Type	Offline	Online
Name	94	46	**Received Degree**	97	-
Email	84	34	**Academic Awards/Honors**	97	-
Phone Number	77	2	**Dates of Attendance**	95	-
Address	76	9	**Major**	95	17
Photo or Video	54	-	**Participation in Sports**	88	-
Date of Birth	47	-	**Participation in School Activities**	83	-
Place of Birth	39	-	**Athlete Height & Weight**	79	-
Student ID	23	6	**Previous Institution**	71	-
Emergency Contact	6	-	**Class Year/Expected Graduation**	66	14
Emergency Contact Address	4	-	**Enrollment Status**	61	-
			College/Affiliation	33	16
			University Assistantship Status	14	-
			Credit Hours	13	-

Table 1: Number of universities with each data type (1) available offline by request and (2) shared online in public student directories.

directory information is available publicly. Of the 76 schools with directories, 30 were hidden, 14 partially hidden, and 32 public.

Many directories contain student contact information. As shown in Figure 1, of the 46 partially and fully public directories, 34 published some student contact information. The types of contact information published varied: most universities published email addresses (N=34), eight published mailing addresses, and two published residential addresses.

Student directory publication practices vary widely: there is a clear need for consensus on best practices to ensure necessary information is shared without violating student privacy. In Section 5, we evaluate student preferences about what directory data is shared, and with whom.

All schools include a wide range of PII and educational information as directory data. For the 97 universities with published definitions, we divide directory data into 2 categories: PII and educational information. Table 1 shows the different data types in university definitions. All 97 universities included some PII in their definition, and the majority (N=76) included students' addresses. All 97 also reported some educational information, ranging from credit hours and major to participation in school-sponsored activities (e.g., sports teams and clubs). From the university's perspective, there are legitimate uses for these items; for example, universities may want to share athlete weight and height with recruiters or the media. However, this appears to exceed what is needed to verify a student's enrollment or graduation—the reason several universities report needing to share directory information by request.

Some universities explicitly stated to whom they would not provide directory information. While we can observe what information is *allowed* to be shared, it is challenging to gather what information is being shared *in practice*, and who it is shared with. While these statements cannot provide definitive answers, they do indicate current sharing practices. Two schools stated they do not share data with agencies "to prepare mailing lists or otherwise solicit students". A few (N=4) universities' notices stated they do not release information to individuals outside of the university. Lastly, a few (N=3) universities say registrars evaluate requests with 'discretion'.

Few universities indicate to whom and for what reason they will share information. Very few (N=3) schools definitively state who they **will** share data with. Some listed specific parties: for example, one school stated they share information with "the military and for the development of the university-affiliated marketing programs." Others listed specific reasons for sharing directory information: for example, one university listed the "online directory…, annual yearbook…, Dean's list or other recognition lists; Commencement programs; and Sports activity sheets."

Some universities indicated who students could opt out of sharing data with. Some (N=19) indicated who they would not share students' data with if students removed themselves from the directory. Three universities stated directory information would not be shared with, "friends, parents, relatives." Several (N=10) indicated opting out would prevent the university from sharing directory information with "potential employers, insurance companies, landlords, credit card companies, and others." This leads us to believe information *will* be shared with these groups if a student does not opt out.

It is clear much data can be shared upon request, with few explicit limitations on who data can be shared with. Next, we examined who submits directory information requests, providing an overview of a limited number of requests we were able to obtain, via FOIA requests. As might be expected, we received limited responses for several reasons. Universities did not respond because their state's FOIA doctrine did not cover our request (N=1), or they determined the request was unreasonable (N=2). Three universities stated they had no relevant documents, but it was unclear whether they did not share student data or they were not compelled to inform us of their sharing practices, because no pre-existing records matched our request. We expect the latter is more likely, as universities at a minimum are required to share student directory information with military recruiters per the Solomon Amendment [86]. Because of these confounding factors, we cannot prove a negative result (i.e., the university shares no directory information). Instead, we only discuss cases where the university responded with records of third-party sharing. Specifically, there were six universities that provided records showing who they have shared student directory information with over the last six months.

Some universities shared data with advertisers, marketing firms, and data brokers. Amongst the six responses, three universities fulfilled requests from advertising/marketing firms. For example, two universities shared information with Flytedesk, a college marketing company which allows you to target "pre-built…audiences or create your own based on location (state, DMA, congressional district), demographics (affluence, ethnicity), or interests (popular majors, greek life)" [22], and three shared data with ASL Marketing, which helps organizations target media advertisements [4]. Most notably, LexisNexis, a well known data broker specializing in risk management, appeared in three universities' provided records [42]. These companies requested information including the student's name, postal address, personal email address, school email, major, and academic status. This confirms the validity of our threat model; data brokers use offline requests to obtain student directory information.

4 DIRECTORY NOTICE AND OPT-OUT PROCESSES (RQ2)

We next investigated students' ability to opt out of directory information sharing: while FERPA §99.37(a) requires universities to provide instructions and a timeline for opting out, there are no implementation requirements. The U.S. Department of Education provides a template notice [51], however, universities are not required to adhere to this template. We therefore investigate how opt-out notices are implemented in practice.

4.1 Method

We gathered information about directory information opt-out processes by (1) contacting university registrars and (2) reviewing relevant university websites. We emailed (template email shown in Appendix 7.2) each university's registrar, asking them to: (1) point us to websites containing information about the opt-out process, (2) address how students are notified of their right to opt out, and (3) provide any email examples, public notices, etc. used to notify students of their opt-out rights.

Concurrently, we performed our own search for information regarding universities' opt-out processes, using the same methodology as 3.1 with keyword "<UNIVERSITY NAME> FERPA directory opt out form." Opt-out policies were usually in FERPA notices—long documents containing various institutional privacy practices. Two researchers independently reviewed each opt-out policy to identify its characteristics. We followed an iterative open coding approach [14], reviewing policies in batches and discussing themes arising from the data among the full research team, regularly iterating our definitions. As in Section 3.1, our study did not require IRR, as we directly recorded information found in the policy and there was no subjective decision making [47].

Through this process, we identified four features:

- What is the opt-out mechanism? (Section 4.4.1)
- What is the process by which students opt out? (Section 4.4.2)
- What effects of opting out are presented to students? (Section 4.4.3)
- What restrictions are placed on students' ability to opt out? (Section 4.4.4)

These features sufficiently characterize the observed variation among universities' opt-out policies, and their potential impacts on student decision making.

4.2 Ethical Considerations

Because we contact registrars, we submitted our study for IRB review. Our IRB deemed the work Non-Human Subjects Research (HSR), as we did not ask questions about the registrars' opinions or behavior, but rather school policies. As in Section 3.2, we crafted our results to limit registrar workload and reported our findings back to the registrars to provide guidance as they seek to best support their students (Appendix 7.8).

4.3 Limitations

Only 43 universities replied to our emails, and few replied fully, instead pointing us to publicly available resources. However, from public online resources, we were able to find all information our investigation required for 72 universities. We could not find any information for the same three universities as in Section 3. For the remaining 25, we were able to answer most of our questions, but not all. This is because some universities did not respond or responded vaguely to our request, or information was publicly inaccessible (i.e., in a Student Services portal). Because we take a conservative approach in our analysis, we do not interpret unclear statements. In most cases, the ambiguity was between options on the less privacy sensitive side of the spectrum, therefore, our results likely overestimate the privacy guarantees found in university policies. While we believe our results provide a relatively complete picture of current practices, we are limited by the lack of registrar responses, which provided details of universities' policies not available publicly.

4.4 Results

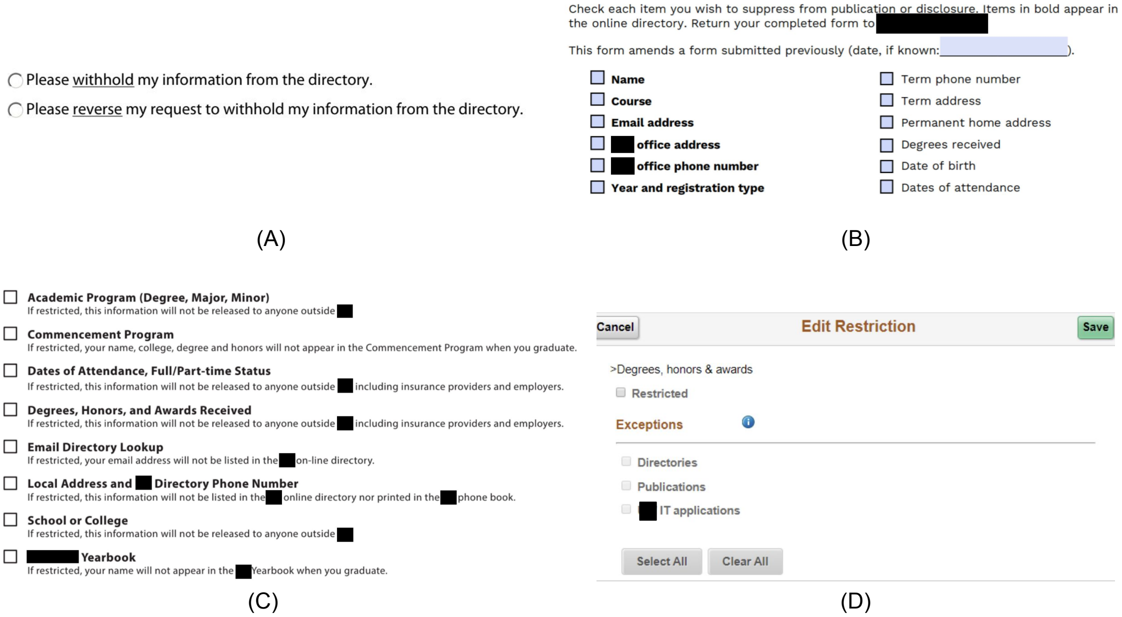
*4.4.1 **Level of Opt-out Control:*** We investigated students' ability to adapt sharing to meet their needs: specifically, we wondered if students could choose to share certain information with some parties, but not others; for example, a student may want their name and email shared within the university, so their peers can contact them, but they may not want this same information shared with marketers. We found definitive answers for 86 universities: we observed four approaches to opt-out control structures, shown in Table 2, which we outline below.

Universities most often use a FERPA block (all-or-nothing approach). Forty universities only let students request a 'FERPA Block': this prevents *any* student directory information from being released without the student's consent. Figure 2.A shows an example FERPA block request. This is the least flexible option, as students must either block the university from revealing all data with all parties, or consent to the university revealing their directory information to any third party the university deems acceptable.

Several universities allow specific data type suppression, but students are often not clearly informed of this option. Some

Model	***Description***	***Count***
Confidential/FERPA Block	Students could only opt out of sharing *all* data with *all* parties.	40
Data Type Suppression	Students could suppress *what* data is shared, but not who it's shared with.	29
Scenario-Based Sharing	Students could indicate situations in which they want different data shared.	16
Role-Based Sharing	Students could choose for each data type who it's shared with.	1

Table 2: Overview of observed opt-out processes across universities.


○ Please withhold my information from the directory.

○ Please reverse my request to withhold my information from the directory.

(A)

Check each item you wish to suppress from publication or disclosure. Items in bold appear in the online directory. Return your completed form to [redacted].

This form amends a form submitted previously (date, if known:).

□ **Name**
□ **Course**
□ **Email address**
□ [redacted] **office address**
□ [redacted] **office phone number**
□ **Year and registration type**
□ Term phone number
□ Term address
□ Permanent home address
□ Degrees received
□ Date of birth
□ Dates of attendance

(B)

□ **Academic Program (Degree, Major, Minor)**
If restricted, this information will not be released to anyone outside [redacted]

□ **Commencement Program**
If restricted, your name, college, degree and honors will not appear in the Commencement Program when you graduate.

□ **Dates of Attendance, Full/Part-time Status**
If restricted, this information will not be released to anyone outside [redacted] including insurance providers and employers.

□ **Degrees, Honors, and Awards Received**
If restricted, this information will not be released to anyone outside [redacted] including insurance providers and employers.

□ **Email Directory Lookup**
If restricted, your email address will not be listed in the [redacted] on-line directory.

□ **Local Address and** [redacted] **Directory Phone Number**
If restricted, this information will not be listed in the [redacted] online directory nor printed in the [redacted] phone book.

□ **School or College**
If restricted, this information will not be released to anyone outside [redacted]

□ [redacted] **Yearbook**
If restricted, your name will not appear in the [redacted] Yearbook when you graduate.

(C)

>Degrees, honors & awards

□ Restricted

Exceptions

□ Directories
□ Publications
□ [redacted] IT applications

(D)

Figure 2: Example opt-out methods for (A) FERPA Block, (B) Data Type Suppression, (C) SBAC, and (D) RBAC.

schools allow students to choose whether different data types are shared (N=29). The subset students can choose to suppress varies; while some universities, like Figure 2.B include a range of PII, not all provide so many options. For example, one university only allowed students to suppress their thesis information. Twelve universities used an open-ended response, asking students to specify in writing "any or all" data not to be shared. While this indicates students may remove some data types, the open-response may be challenging for students who might not know what data is shared, and therefore what they want to remove. Further, although students can control what data is shared, students cannot control who receives it, e.g., choosing different data to share internally vs. externally.

Some universities provide scenario-based sharing options. Seventeen universities allow students to opt out of a set of common sharing scenarios. These scenarios varied between universities, but often included situations where students may elect to remove their information from the public directory, while allowing some sharing, such as in thesis repositories. Six universities had separate opt-outs for online and offline directories, though they still only allowed all-or-nothing sharing for each. However, by splitting these options, students may be less aware of offline data sharing, because there is no user-facing component as with online directories. Similarly, six universities provide students with additional comprehensive choices only for their thesis (N=2) or photo (N=1), or a way to remove some information from the public directory (N=3).

Few universities gave comprehensive scenario-based options. Only four universities provided comprehensive opt-outs; for example, Figure 2.C shows one university's sharing scenarios, which include scenarios for (1) third party sharing, (2) inclusion in the online directory, and (3) inclusion in the yearbook or commencement program. This provides contextual control over students' data's use, allowing students to determine who data is shared with and what data is shared in a subset of scenarios.

Only one university allowed students to choose who data would be shared with for each data type. As shown in Figure 2.D, this university allows students to place sharing restrictions by data type, then indicate exceptions to those restrictions for various parties (i.e., directories, publications, internal IT applications), effectively allowing students to control who data is shared with and what data is shared.

4.4.2 ***Method of Opt Out:*** We found two ways opt-out processes vary: (1) in-person vs. online and (2) standardized vs. non-standardized formats. Standardized opt-outs provide students with different choices to select, whereas non-standardized opt-outs do not, telling students to inform registrars of their opt-out in writing.

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

Table 3: Overview of variations in opt-out methods.

Functional Effect	*Count*
Withheld From Third Party Sharing	40
Withheld From Various Internal Uses	32
Potential Missed Messages	7

Table 4: Prevalence of listed functional effects of opting out.

We found sufficient information for 97 universities; feature frequency is shown in Table 3. Some universities allowed students to choose between a non-standardized or standardized method (N=4), or had a standardized method for some directory data, but not for others (N=6). Thus, our counts in this section sum to 107, not 97.

Most universities have a standard method to submit opt-out preferences. The majority of universities provided a structured format for submitting opt-out preferences (N=72), typically through a fillable PDF form or in an online student services system.

35 universities did not have a standardized opt-out. The FERPA notice simply states that student may "inform the registrar" of their intent to opt out, and they may remove "any or all of the types of information", suggesting students may choose to withhold subsets of the data types. However, they do not provide clear guidance regarding the set of collected data students may opt out of sharing.

A few universities require in-person opt out. While most universities allowed students to opt out by email or an online portal, fourteen required students to come in person to opt out. For three universities, this was a separate process only required for the most restrictive form of opt-out (i.e., FERPA blocks), while students were allowed to removing subsets of information virtually. A few registrars (N=3) informed us via email that they ask students to come and meet in person to ensure students understand their decisions' impact. This likely mitigates some confusion as the registrar can explain the effects of opting out (we discuss further in Section 4.4.3). However, due to accessibility issues and the additional time burden, this requirement may inhibit some student from enacting their privacy preferences.

4.4.3 ***Opt-Out Effects and Framing:*** Given registrars' focus on ensuring students were informed of the effects of opting out, we next investigated what effects registrars present to students. We found FERPA notices and opt-out forms focused exclusively on negative effects; we only observed one institution giving a reason *for* students to opt out. Conversely, 52 universities gave at least one negative opt-out effect (i.e., reason *not to* opt out): Table 4 shows the frequency of commonly mentioned effects.

Effect 1 - Information cannot be shared with third parties. Forty universities indicated they would be unable to provide student information to third parties after an opt-out; this included being unable to give friends and family PII, or confirm attendance to potential employers or credit card companies. One university warned opting out "will prevent [University] from providing your directory information to your friends, prospective employers, and others with whom you may wish us to share such information, so make your decision carefully."

Effect 2 - Information is withheld from internal use (i.e., directories, publications, commencement, and awards). Thirty-two universities warned opting out would prevent student information from being used for directories and publications (N=21), or commencement and awards programs (N=28). For example, one university tells students, "...you will not appear in the University's online directory or any directory or Facebook produced by your school or residential college for use within the school or college." Only four universities permitted students to restrict sharing to these use cases. The other 28 schools required students to allow external sharing if they wanted to avoid this effect.

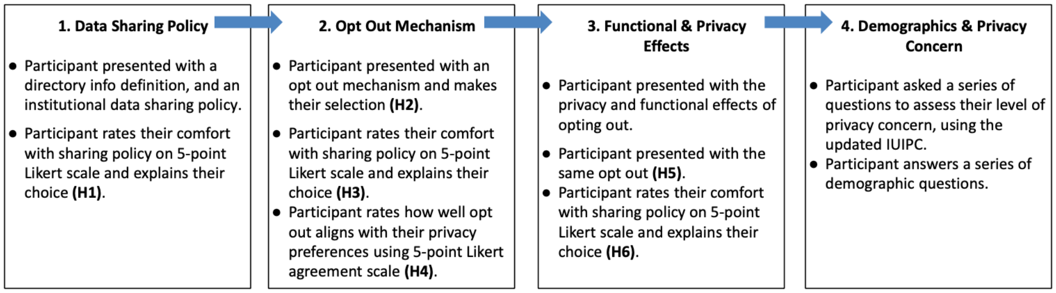
Effects 3 - Messages, Mailings, and Announcements Cannot Be Delivered. Some universities listed trouble with potential email or message delivery (N=7); one university stated, "students should be aware of the possible consequences of putting in place a FERPA Block, such as missed mailings, messages, and announcements." This may be because universities are having their mailing lists managed by external vendors; universities have structured their internal functionality to require third party access to student data, in conflict with the principle of privacy-by-design.

This set of effects is likely not the complete list; as we briefly discussed in Section 4.4.2, registrars may require students come in person to opt out. It is likely these effects are reiterated in these discussions and other effects may be described.

4.4.4 ***Restrictions on Opt Out Timeline:*** Many universities also restricted when students can opt out and how long opt-outs stay in effect. We found 28 universities required students opt out within a given time period, most commonly within the semester's first week. One university required students "submit requests for a FERPA block before the end of the first week of the semester, otherwise the block cannot be applied by the registrar". Fifteen universities also required students opt out regularly: either annually or each semester. This is likely due to systemic usability or technical problems surrounding implementing opt outs; limits are likely placed to avoid the administrative burden associated with ineffective systems.

5 STUDENT PERCEPTIONS SURVEY (RQ3)

Building on findings in Sections 3 and 4, we surveyed US university students to understand their perceptions of the identified directory information sharing and opt out practices. We conduct a vignette-based between-subjects controlled experiment where each participant is assigned one of 16 scenarios describing a directory information sharing practice, opt-out procedure, and opt-out effects. We compare differences in participant privacy perceptions as we vary each item.



1. Data Sharing Policy

- Participant presented with a directory info definition, and an institutional data sharing policy.
- Participant rates their comfort with sharing policy on 5-point Likert scale and explains their choice **(H1)**.

2. Opt Out Mechanism

- Participant presented with an opt out mechanism and makes their selection **(H2)**.
- Participant rates their comfort with sharing policy on 5-point Likert scale and explains their choice **(H3)**.
- Participant rates how well opt out aligns with their privacy preferences using 5-point Likert agreement scale **(H4)**.

3. Functional & Privacy Effects

- Participant presented with the privacy and functional effects of opting out.
- Participant presented with the same opt out **(H5)**.
- Participant rates their comfort with sharing policy on 5-point Likert scale and explains their choice **(H6)**.

4. Demographics & Privacy Concern

- Participant asked a series of questions to assess their level of privacy concern, using the updated IUIPC.
- Participant answers a series of demographic questions.

Figure 3: A high level overview of the survey's parts.

Conditions	
Who Shared	***Opt-Out System***
Not Stated: No statement regarding data sharing policy is provided to the participant.	**FERPA Block:** Students could only opt out of sharing *all* data with *all* parties (i.e., Allow all/Don't allow any sharing).
Third Parties: University shares data with any third parties that request it from the registrar. This could be for direct use, as described below, or for indirect use (e.g., companies that collect and sell user data for advertising purposes, or individuals who call to request your data).	**Data Type Suppression:** Students can suppress what data types are shared, but not who they are shared with (i.e., To opt out, check boxes for name, email, address. etc).
Third Parties For Direct Use: The university shares this data with third parties that it views as benefiting students, namely, that directly provide benefits to students or staff (ex. companies used by the school for email listserv delivery, or companies offering students moving services).	**Scenario Based Access Control (SBAC):** Students could indicate situations where they would want different data types shared (e.g., Check this box to opt out of releasing dates of attendance, full/part-time status to anyone outside the university, including insurance providers and employers.).
Institutional: Parties within the university can access directory data for purposes related to university events (e.g., to compile lists for school event entry or to allow your name to be a part of the commencement program).	**Role Based Access Control (RBAC):** Students indicate parties with whom they want different data shared (e.g., For each data type, check the appropriate boxes to opt out of sharing with the institution, third parties for direct use, and third parties for indirect use).

Table 5: The conditions used in our survey; each participant was randomly assigned a value from the "Who Shared" column, and a value from the "Opt-Out System" column.

5.1 Methods

For our study, we recruited participants using Prolific, a research recruitment service that has been found to provide high-quality samples [55, 78]. We recruited Prolific users who self-identified to Prolific as U.S. students aged 18 or older. Participants confirmed they fit these criteria as part of our consent process. We assigned participants to one of 16 conditions round-robin, until each condition had at least 60 valid participants. Participants completed the survey in 10.77 minutes on average and were paid $3.75 for participating (>$15/hr).

Our study design is outlined in Figure 3. Each survey component focused on testing a specific hypothesis about student data sharing preferences. We present each hypothesis in turn as we describe the survey chronologically. Throughout the survey, we use language largely from the real-world opt-out policies we found in Sections 3 and 4; this allows us to understand how students perceive current practices.

H1: Students prefer policies explicitly limiting data sharing (Figure 3.1). Our previous investigations (Sections 3 and 4) demonstrate student directory information implementations vary most dramatically in who universities share data with, and how students can opt out. To understand students' preferences surrounding who data is shared with, we assign participants to one of four conditions: Institutional, Third Parties For Direct Use, Third Parties For Indirect Use, and Not Stated. The scenario descriptions for each condition, drawn from our results in Section 3, which were presented to participants [2] are given in Table 5.

Our survey began by stating that we will ask participants to make decisions about what directory information they would be comfortable with their university sharing. We then provide students with two sets of information: (1) a definition of what data is included in directory information (based upon our Section 3 observations) and (2) a policy for who data is shared with (drawn from the *Who Shared* options in Table 5). These sharing policies are inclusive of all subsequent policies in the table: e.g., if a participant is assigned to the third parties for direct use condition, they were

[2] Definitions are slightly modified for brevity, exact descriptions are given in Appendix 7.1

also informed their data would be shared institutionally. This mimicked policies observed in Section 3 as there were no cases where external sharing was permitted, while restricting internal sharing. The only exception is the "Not Stated" condition, which does not indicate who data is shared with. This condition was included to test student perceptions in the cases we observed when no policy was provided.

We then ask participants how comfortable they would be with their university sharing directory information about them with the given parties, asking them to respond on a 5-point Likert scale from "Extremely uncomfortable" to "Extremely comfortable", and to explain their choice. Based on related work [6, 39], we expected students would prefer institutional over third party sharing.

H2: Students are more likely to opt out when given more options (Figure 3.2). After providing their perceptions of their assigned data sharing policy, participants were told they may choose to opt out of data sharing. Participants were presented with the opt-out options from one of four assigned conditions drawn from Section 4: FERPA Block, Data Type Suppression, Scenario Based Access Control (SBAC), and Role Based Access Control (RBAC). Each condition is summarized in Table 5 and examples of the opt-out text for each condition are given in Appendix 7.5. We evaluate H2 by examining whether students choose to opt out, and what choices students select between conditions. Our model must treat opt-outs as binary, because there is only one option for a FERPA Block opt-out (to deny all sharing). As opt-out options provide progressively more control, we expected participants would take one of the growing number of opt-out options.

H3: Students are more comfortable when given more opt-out options (Figure 3.2). Next, we repeat the question about participant comfort with data sharing from H1, this time asking participants to consider their comfort after making their opt-out choice. Again, we asked participants to explain the comfort reasoning in an open-ended question. H3 addresses changes in comfort associated with different opt-out systems; because previous work suggests people prefer greater control over their information [34, 80], we expected students would also be more comfortable in opt-out system which provided more control.

H4: Students perceive more detailed opt-out systems fit their privacy preferences better (Figure 3.2). We then asked participants to indicate the degree they felt the opt-out system allowed a choice aligned with their privacy preferences, using a 5-point Likert scale from "Strongly disagree" to "Strongly agree". H4 investigates the extent participants feel their assigned opt-out system provides them the ability to act on their privacy preferences. Given prior findings [34, 80], we expected students would value more flexible systems which allowed control over specific sharing.

H5: Students are likely to opt back in after seeing the effects of opting out (Figure 3.3). Finally, we evaluate the impact of showing students the *effects of the decision to opt out.* While some universities inform students of things they will lose if they opt out (e.g., not being a part of the commencement program), most do not provide students full information about their decision's impact. We were interested to understand the impact of stating these effects in the opt-out process.

To test H5, we informed participants of the opt-out effects and asked them to repeat the opt-out process. Specifically, we presented participants with the functional effects, drawn from Section 4.4.3's results, associated with their assigned data sharing policy. For example, participants assigned to the Third Party sharing condition were informed of effects such as their directory information would not be shared with "anyone outside of the university, such as family members, insurance providers, or employers." Unlike almost all of the policies we observed in Section 4.4.3, we also described privacy effects. For example, participants assigned to the Third Party sharing condition were informed that opting out would "prevent third parties from using your data for advertising, and other unauthorized purposes." By comparing students' opt-outs before and after being exposed to the effects, H5 captures whether and how this information impacts student decision making. Because the effects listed were likely to have a significant impact on students' university experiences, we expected students would chose to opt out less.

H6: Student comfort with data sharing decreases after seeing the opt-out effects (Figure 3.3). One last time, we repeated our question from H1 and H3 about participant comfort with data sharing after providing participants full information about opt-out effects. Again, we used the same 5-point comfort Likert scale and open-ended question.

H6, similar to H5, expects the privacy and functional effects will impact students' comfort with their opt-out choice. Again, because the listed effects likely have a significant impact on student experience, we expected students would feel they were unable to select choices aligning with their functional or privacy inclinations, and would thus be less comfortable with their choices.

Demographics (Figure 3.4). We concluded with additional questions to provide context about the participants. First, we asked participants to indicate their level of general privacy concern using Grob's modified Users' Information Privacy Concerns (IUIPC) scale [25]. For the sake of our analysis, we consider privacy concern to be the average privacy score across the IUIPC categories. We then asked participants a series of questions about their current academic institution (its size, whether it was public or private) and their major/degree program. We ended the survey with a series of demographic questions (e.g. age, gender, race and ethnicity, income).

5.2 Ethical Considerations

Our study was approved by our university's IRB; we asked for participant consent at the beginning of the survey, and allowed participants to stop at any point. We protected participant privacy by securely storing data, and never collecting identifiable information beyond the participant's Prolific ID.

5.3 Analysis

We use ordinal logistic regressions to assess our hypotheses. Our explanatory variables include the assigned conditions, participant demographics and privacy concern levels, and two-way interactions between the opt-out systems and data sharing policies; these factors are shown in Table 6. For each hypothesis, we compared all

Factors		
Conditions		
Factor	**Description**	**Baseline/Levels**
Who Shared*	Which of the 4 data sharing policy conditions was the participant was assigned to (Not Stated, Third Parties For Direct Use, Third Parties For Indirect Use, Institutional); see 5.	Not Stated
Opt-Out System*	Which of the 4 opt-out system conditions was the participant was assigned to (FERPA Block, Data Type Suppression, SBAC, RBAC); see 5.	FERPA Block
Demographics		
Privacy Concern	We average the scores across the three categories of the updated IUIPC scale [25], and group participants into 2 categories: "Concerned" and "Unconcerned".	Unconcerned
Size	We ask participants to report whether they attend a small (less than 5,000 students) institution, medium (5,000-15,000 students) institution, or large (more than 15,000 students) institution.	Small Institution
Technical	We ask participants to self-report their major of study which we classify based upon its relation to relevant technical fields (i.e. computer science or engineering, IT, etc.)	Not Technical

Table 6: The factors used in our regression models.
***We also include factors for the relationship between Who Shared and Opt-Out System.**

possible explanatory factor combinations and selected the model with minimum Bayesian Information Criterion (BIC)—appropriate for assessing model goodness-of-fit [58, 73].

For all free-response questions, we perform iterative open coding [76]. Two researchers collaboratively coded 50 responses to develop the initial codebook. They then independently coded responses in rounds of 50, calculating Krippendorff's α [29], resolving disagreements, and updating the codebook when necessary. After 9 rounds, a Krippendorff's α of 0.8 was reached, indicating acceptable agreement [29]. The remaining 541 responses were coded by one researcher. The final codebook is in Appendix 7.7.

5.4 Limitations

While we believe our results generally represent the privacy behaviors and beliefs of university students, our participants were asked questions about a hypothetical scenario; therefore, our results may differs from real world behaviors. Namely, in line with the privacy paradox [7], students may say they want more privacy than they will actually take action to achieve. However, this difference is likely due to social or technical challenges in making the decision to prioritize privacy, such as unusable or inaccessible opt-out mechanisms [65]. We attempt to mitigate this effect by describing the effects of prioritizing privacy, replicating the consequences that might persuade students in real life. However, we cannot get exactly to true participant behaviors, because even though we include costs, the costs have no real impact on the participant's life. Thus, our results serve as an upper bound for student privacy behaviors.

Also, we rely on participants to self-report their student status through Prolific's built-in screening questions. It is possible some participant are not in fact students. This could be because a participant did not answer honestly, but Prolific has been shown to provide high-quality responses [55] and our sample demographically matched other studies with university students [6, 10, 21, 26, 27, 50]. It is also possible some participants may have been students when they filled out Prolific's screening questionnaire, but graduated prior to participating in the study. However, we do not expect this to have occurred often as we ask students to explicitly re-affirm their student status in our survey.

Selection bias (People who took our survey were more interested in privacy) and social desirability bias (people tell us they care about privacy because they know we care about privacy) are also possible. However, our IUIPC scores match similar studies, and our population does not appear to be skewed, and appears representative of university student privacy behaviors.

When describing responses from open-ended questions, we give the number of participants who expressed each idea. However, not mentioning an idea does not indicate participant disagreement. Instead, they may have just failed to state the idea or perceived other thoughts as more relevant. Thus, our open-response results measure what was "front of mind" during the survey.

Participants may not pay full attention when taking the survey. In order to address data quality, we remove participants who took the survey unreasonably fast, or who failed our attention check.

Finally, our results are limited by recruitment to Prolific users. However, prior work has shown that privacy concerns identified from Prolific users can generalize to the broader population [78]. Additionally, Prolific participants tend to be younger and more tech-savvy than the broader US population [78], which is also true of US university students [31, 72].

Because participants are assigned randomly, these biases are distributed across conditions, so we focus specifically differences between conditions.

Participant Demographics									
Age		**Gender**		**Race & Hispanic**		**Education**		**Privacy Concern**	
18-23	(42.73%)	**Man**	(47.58%)	**White**	(61.72%)	**H.S. or Below**	(5.76%)	**Average Score:**	5.97
24-29	(24.75%)	**Woman**	(46.97%)	**African American**	(14.55%)	**Some college**	(39.6%)	*(Scale 1-7)*	
30-39	(14.24%)	**Non-Binary**	(4.14%)	**Asian**	(11.82%)	**Associate's**	(12.12%)		
40+	(13.54%)	**Not Stated**	(1.31%)	**2 Or More Races**	(5.86%)	**Bachelor's or Above**	(41.11%)		
Not Stated	(4.75%)			**Other**	(4.14%)	**Not Stated**	(1.41%)		
				Not Stated	(1.92%)				
				Hispanic (14.24%), Not Hispanic (84.44%), Not Stated (1.31%)					

Participant University Information					
School Size		**School Type**		**Technical Degree**	
Small	(14.04%)	**Public**	(76.67%)	**Technical***	(15.66%)
Medium	(37.17%)	**Private**	(21.92%)	**Not Technical**	(71.11%)
Large	(48.59%)	**Other**	(0.71%)	**Not Stated**	(13.23%)
Not Stated	(0.2%)	**Not Stated**	(0.71%)	*(relevant degrees only)	

Table 7: Demographic information for participants of our study.

5.5 Results

Participant Demographics. Our survey was completed by 991 participants. Our participant sample resembles U.S. university students, but is more white (63% in our survey, as opposed to 51% nationally [50]), includes less women (47% in our survey, 58% nationally [26]), and is older (42.7% reported ages of 18-23, compared to 56.2% nationally [21]). This is likely because our sample also contains students pursuing education beyond bachelor's degrees, which likely incurs demographic differences. Additionally, privacy concern is unevenly distributed. The vast majority of our participants' (97.6%) responses on the IUIPC scale indicated they were privacy concerned. However, this distribution of IUIPC scores matches prior college student samples [6].

Participants' university information was also generally representative; we only slightly over-represent public institutions (76.67% in our survey, 73% nationally [27]). We were unable to find statistics regarding the national university size distributions, but the average size of US institutions was 6,354 students [10], which aligns with our distribution.

5.5.1 ***Students preferred policies with greater limitations on who data is shared with (H1)***. Figure 4 displays students' comfort across data sharing policies and Table 8 summarizes our final regression model for H1. Compared to those not informed who data was shared with, participants were 3.20× and 1.62× more likely to increase one point on the comfort Likert scale when told data was only shared within the institution ($p < 0.001$) and only with third parties for direct use ($p = 0.003$), respectively.

We can further stratify the sharing policies by comparing non-overlapping confidence intervals, which show participants were more likely to feel comfortable with institutional sharing ($CI = [2.3, 4.46]$) than sharing with third parties for direct use ($CI = [1.17, 2.24]$) and sharing with third parties for indirect use ($CI = [0.66, 1.26]$). While more participants felt uncomfortable in the any third party sharing condition (67.07%) than the third party for direct use condition (54.47%), we did not find a statistically significant difference as these conditions' confidence intervals overlapped.

Variable	Value	Odds Ratio	CI	*p*-value
Data Sharing Policies	**Not Stated**	–	–	–
	Third Parties	0.91	[0.65, 1.26]	0.556
	Third Parties, Direct Use	1.62	[1.17, 2.24]	0.003*
	Institutional Use	3.20	[2.3, 4.46]	< 0.001*
Privacy Concern	**Unconcerned**	–	–	–
	Concerned	0.23	[0.11, 0.5]	< 0.001*
Technical	**No**	–	–	–
	Yes	0.71	[0.52, 0.98]	0.035*
	Not Stated	0.51	[0.36, 0.71]	< 0.001*

*Significant effect – Base case

Table 8: Summary of regression for H1: participant comfort with different data sharing policies. Pseudo R^2 measures for the model were 0.04 (McFadden) and 0.11 (Nagelkerke).

This trend is also supported by participants' open responses; participants differentiate between institutional and third party sharing, and attribute this difference as part of their discomfort. Specifically, 122 participants expressed comfort with institutional data sharing, while only 15 specifically expressed discomfort with institutional data sharing. For example, one participant said, "As long as it's only used within the institution I don't mind too much. I would still prefer it not to be shared." Alternatively, only 13 participants explicitly expressed comfort with third party data sharing, while 177 specifically expressed discomfort. One participant explained, "...while I understand that some data sharing is necessary for administrative purposes and university events, I am cautious about the potential indirect use of my data by companies that collect and sell user data for advertising..." Those expressing discomfort with third parties often focused on spam/undesired messages from third parties like advertisers, or cited concerns surrounding data security or potential data misuse. It is clear participants are most comfortable when data sharing is limited to only that necessary for university functionality.

Students interpret ambiguity as the worst case scenario.

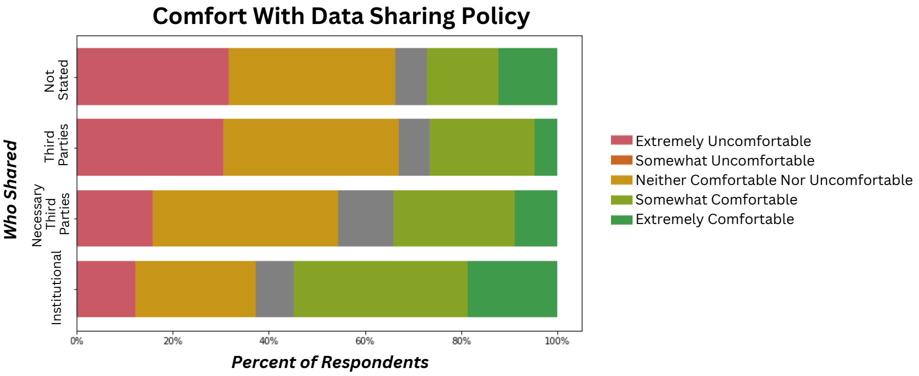


Figure 4: Self-reported participant comfort with respect to different directory data sharing policies.

Variable	Value	Odds Ratio	CI	*p*-value
Data Sharing Policies	**Not Stated**	–	–	–
	Third Parties	1.50	[0.74, 3.05]	0.261
	Third Parties, Direct Use	0.82	[0.43, 1.56]	0.543
	Institutional Use	0.32	[0.18, 0.57]	< 0.001*
Opt-Out Systems	**FERPA Block**	–	–	–
	Data Type Suppression	8.00	[4.36, 14.7]	< 0.001*
	SBAC	10.83	[5.47, 21.45]	< 0.001*
	RBAC	9.57	[4.96, 18.44]	< 0.001*
Privacy Concern	**Unconcerned**	–	–	–
	Concerned	7.46	[2.71, 20.52]	< 0.001*

*Significant effect – Base case

Table 9: Summary of regression for H2: participants' likelihood of opting out. Pseudo R^2 measures for the model were 0.20 (McFadden) and 0.26 (Nagelkerke).

While we found participants were less likely to be comfortable with data sharing with any third party than when a data sharing policy is not stated ($OR = 0.91$), this was not statistically significant ($p = 0.556$). This suggests students consider not stating a policy similarly to third party sharing, the group students are least comfortable sharing data with. Nineteen of 243 students assigned to the Not Stated condition made this connection explicitly when asked to explain their comfort response, perceiving the information as being shared to the "public." These results suggest if a university is not sharing with unnecessary third parties, they should be transparent to increase student comfort.

5.5.2 ***Students were more likely to opt out when given more options (H2).*** Figure 5 displays initial participant opt-out choices, and Table 9 displays our final regression model for H2. Compared with FERPA Block, students assigned to the three other systems (Data Type Suppression $OR = 8.00$, SBAC $OR = 10.83$, and RBAC $OR = 9.57$), were statistically significantly more likely to opt-out of data sharing, all with p-values < 0.001. This is as we expected—there is only one potential choice for FERPA Block, so participants will be less likely to opt out as they have more options and control. Our qualitative coding supports this reasoning; when asked how their opt-out system could be improved, many respondents described wanting more control or options for data sharing (N=532). We do not see a statistically significant difference between the other opt-out systems; the confidence intervals of Data Type Suppression ($CI = [4.36, 14.7]$), SBAC ($CI = [5.47, 21.45]$), and RBAC ($CI = [4.96, 18.44]$) are overlapping

Additionally, participants assigned to Institutional data sharing are less likely to opt out (79.8% of participants), compared to participants not told who data was shared with ($OR = 0.32$, $p < 0.001$). Participants assigned to Third Parties For Direct Use and All Third Parties opted out 89.4% and 93.2% percent of the time, respectively, and neither was statistically significantly different compared with Not Stated (91.40%). These differences align with our findings regarding participant comfort in the prior section and suggest participants expecting data will only be used within the institution are willing to allow greater directory information sharing. Thus, we see both opt-out systems and data sharing policies impacted students' opt-out decisions.

Participants are more likely to opt out of institutional data sharing when it is the only data sharing type. In the RBAC opt-out condition, because sharing policies were inclusive of all less intrusive sharing policies, all participants were given the option to opt out of institutional sharing—with further sharing options given in the Third Parties For Direct Use and All Third Parties conditions. Appendix 7.6 shows the full opt-out rates by data type, who data is shared with, and *Who Shared* condition. Interestingly, participants chose to opt out of institutional data sharing less when other options (i.e., third parties for direct use and all third parties) were shown then when only institutional sharing was included. That is, the opt-out rates are higher for RBAC participants assigned to Institutional data sharing only, compared to RBAC participants assigned to third party sharing. In some cases, almost twice as many participants chose to opt out of Institutional sharing when it is the only option. Participants appear more willing to allow institutional sharing when they have the opportunity to opt out of third party data sharing. This may suggest action bias surrounding these privacy options [54] or a tendency to allow more sharing than intended in the conditions with multiple data recipients [12].

Students preferred limitations on the data types shared, in particular on personally identifiable information. While our regressions must rely upon a binary representation of opting in and out, as FERPA Block only has this binary choice, in Figure 5, we

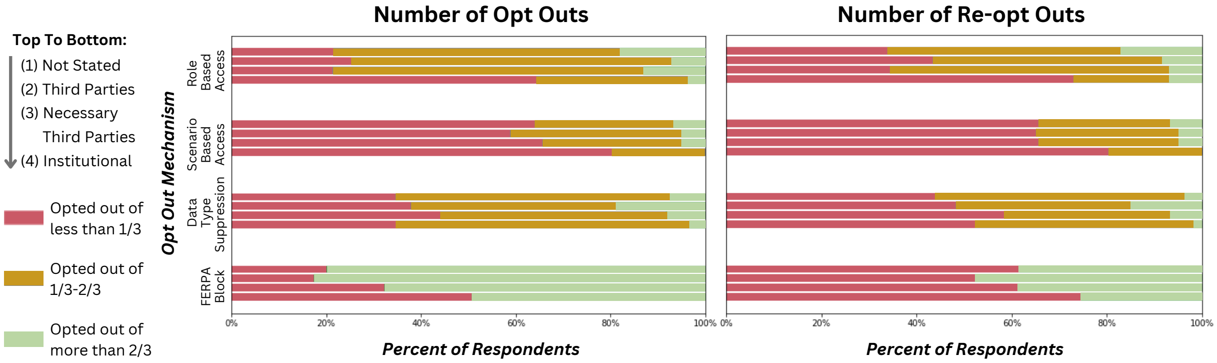


Figure 5: The number of opt-outs by opt-out system and data sharing policy. Left figure displays results for the initial opt out (Figure 3.2). Right figure displays results for the opt out after participants are presented with effects of opting out (Figure 3.3).

display how the number of opt-outs varies across these conditions. We see that for systems where students can choose specific data types for opting out, students often only select a limited number of data items; very few participants chose to select greater than two-thirds of available options. The data types most often chosen for opt out largely consisted of contact and residential information, as can be seen in Appendix 7.6. These results allow us to understand *what* information participants are comfortable sharing, and who they are comfortable sharing it with. Home addresses were the only data type suppressed by more than half (74.19%) of RBAC participants with Institutional data sharing. Conversely, for both RBAC Third Party and Not Stated data sharing, all data types were opted out of by more than half of participants from third party sharing.

In the initial open response, students voiced discomfort with the provided definition of directory information. Most students were comfortable with some data sharing, but wanted control over what specific data types are being shared; i.e., were fine with school sharing name and school email, but not address or phone number. Participants mentioned several data types as being particularly sensitive or not sensitive; for example, 154 participants mentioned addresses as being sensitive, 117 mentioned phone number, 73 mentioned place of birth, 70 mentioned date of birth, 43 mentioned email, and 23 participants mentioned contact information more generally. Very few students specifically mentioned this information was not sensitive, with the exception of email which 20 participants said they were comfortable sharing. In stating their reasons for not wanting to sharing this information, participants gave specific consequences they had experienced at their current institutions. For example, one participant stated, "I will give you a particular example — my school shared my private information including my address and now I am getting all kinds of loan offers to pay my tuition. this is terrible!"

Students were less decided on the sensitivity of university data. Alternatively, 38 participants mentioned university-related information as sensitive, and 44 mentioned university-related information as not sensitive. Students wanted different policies for personally identifiable information and university-related information. One participant explained, ”I would not want my university to share my home address, phone number, date, and place of birth for any reason. I could understand the other information in regard to university events or scholarships, but information that is not directly related to the university, should not be shared." This is similar to Korir et al.'s results, and corroborates their findings that students have different data sharing preferences for personally identifiable information and university-related information [39]. While there were a significant number of participants who felt university-related information was sensitive, in many cases this was because this university-related information could be reflective of aspects of their identity. As an example, a participant stated, "I'm active on the "Gay club" on campus, [CLUB NAME]. I don't know who they're giving this information too but it seems like a lot to include school activities."

Variable	Value	Odds Ratio	CI	p-value
Data Sharing Policies	**Not Stated**	–	–	–
	Third Parties	1.14	[0.83, 1.57]	0.409
	Third Parties, Direct Use	0.65	[0.47, 0.9]	0.009*
	Institutional Use	0.43	[0.31, 0.59]	< 0.001*

*Significant effect – Base case

Table 10: Summary of regression for H3: change in student comfort after opt out. Pseudo R^2 measures for the model were 0.01 (McFadden) and 0.05 (Nagelkerke).

Some students felt this data sharing had no effect because they already lost their privacy. Several students indicated they accepted the data sharing because they felt this information was already available from other sources (N=70), so their decision would have no effect even if they felt uncomfortable with the data sharing.

5.5.3 *Comfort increases after allowing opt-outs, particularly for more invasive data sharing, but no difference between opt-out systems (H3).*

As we observe in Figure 6, allowing students to opt-out of data sharing produces a large increase in participant comfort. For most conditions, the number of uncomfortable participants halves.

Table 10 displays our final regression model for H3. Our results indicate participants were most likely to increase their comfort after opting out when assigned to the Not Stated and Third Parties conditions. Participants with both Institutional ($OR = 0.43$ $p =< 0.001$) and Third Parties For Direct Use ($OR = 0.65$ $p = 0.009$) policies were

Variable	Value	Odds Ratio	CI	p-value
Opt-Out Policies	**FERPA Block**	–	–	–
	Data Type Suppression	2.19	[1.56, 3.08]	< 0.001*
	SBAC	1.78	[1.27, 2.5]	< 0.001*
	RBAC	1.44	[1.03, 2.02]	0.033*
Technical	**No**	–	–	–
	Yes	0.96	[0.69, 1.35]	0.829
	Not Stated	0.96	[0.69, 1.35]	0.829

*Significant effect – Base case

Table 11: Summary of regression for H4: opt-out system alignment with student privacy preferences. Pseudo R^2 measures for the model were 0.02 (McFadden) and 0.04 (Nagelkerke).

Variable	Value	Odds Ratio	CI	p-value
Opt-Out Policies	**FERPA Block**	–	–	–
	Data Type Suppression	1.07	[0.76, 1.5]	0.703
	SBAC	0.60	[0.43, 0.84]	0.003*
	RBAC	1.06	[0.75, 1.49]	0.742
Privacy Concern	**Unconcerned**	–	–	–
	Concerned	2.47	[1.16, 5.26]	0.019*

*Significant effect – Base case

Table 12: Summary of regression for H5: students change their opt-out decisions after seeing the effects. Pseudo R^2 measures for the model were 0.01 (McFadden) and 0.02 (Nagelkerke).

less likely to increase their comfort after opting out compared to those in the Not Stated condition. Participants were also more likely to increase their comfort in the Third Parties condition than the Institutional Use condition, as their confidence intervals ([0.83, 1.57] and [0.31, 0.59], respectively) do not overlap. This is likely because Institutional and Third Parties For Direct Use participants were more comfortable in the first place.

Interestingly, we did not observe a statistically significant difference between opt-out systems, suggesting more options for opting out does not necessarily increase comfort.

5.5.4 ***Students believed all other opt-out systems fit their preferences better than FERPA Block (H4).*** While participant comfort does not appear to differ by opt-out system, all three other opt-out systems were more likely to align with students' privacy preferences than FERPA Block. Of those, Data Type Suppression had the highest odds ratio ($OR = 2.19$, $p < 0.001$), though we did not observe any statistically significant difference between these three methods.

These findings are also reflected in participant open-ended responses. When asked how the opt-out system could be improved, participants were least likely to suggest changes to Data Type Suppression (N=98). Participants most often requested greater customization of what data could be shared and with whom (i.e. "I want people to know my age. I do not want to give out my full date of birth though.") for FERPA Block (N=176) and SBAC (N=153). For example, one FERPA Block participant stated, "Have lists available to opt out of specific things being shared with specific groups." and another participant with SBAC explained, "I feel like you should be able to opt out of each for both internal and external use separately." Our results suggest all three other opt-out systems fit participants privacy preferences better than FERPA Block, as students may customize with whom and what data is shared.

5.5.5 ***Students often remove their opt-outs after seeing the effects, but least often with SBAC (H5).*** We see in Figure 5, on average, students chose to remove some opt-outs they initially selected after being told the effects of opting out. Across all opt-out systems (35.9% of participants shown FERPA Block, 41.8% shown Data Type Suppression, 25.6% shown SBAC, and 43.7% shown RBAC) students chose to share more data than in their initial opt-out decision. Conversely, only 3.6% for FERPA Block, 11.6% for Data Type Suppression, 11.4% for SBAC, and 13.1% for RBAC opted out of more sharing. Our regression for H5 (Table 12) shows that the only statistically significantly different opt-out system was the SBAC. Participants in the SBAC condition were less likely to remove opt-outs after being shown the effects ($OR = 0.60$, $p = 0.003$) when compared with the FERPA Block condition.

There are a couple of potential reasons SBAC elicits this behavior. First, some scenarios combine privacy and functional effects in a way that may discourage students from opting out. For example, if a student wanted potential employers to access their enrollment information but not advertisers, these would be governed by the same scenario selection. This may impact students' choices, though this is also true for Data Type Suppression and FERPA Block and we expect that if this was the case, student comfort would be negatively impacted as with FERPA Block. However, this is not the case (see Figure 6). Alternatively, the scenarios provide some information about functional effects that matched the effects provided in this last section of the survey (e.g., inclusion of information in the commencement program). Therefore, students may be better informed during their initial decision because of the narrative form of information presentation than in the other conditions, reducing any surprise after showing effects that triggers students opting back in.

Next, we considered the specific data types changed during the opt-out in the non-FERPA Block conditions. The opt out rates and changes after effects are shown are given in Appendix 7.6. We observed that the data types students chose to opt back into matched those they were more likely to opt out of originally, which is expected as those are the data types students can opt out of. It does appears that the privacy considerations of the re-opt out process were unique from the original opt out privacy decisions, but instead just more informed by the newly raised functional concerns.

5.5.6 ***Student comfort changes after seeing the effects of opting out (H6).*** While the comfort gained through the opt-out process is not annihilated, we do see the effects cause some decreases in participant comfort. As shown in Figure 6, we see the largest decrease for FERPA Block, especially for non-institutional data sharing. Our final regression model for H6 (Table 13), found participants in the FERPA Block conditions had a statistically significantly greater decrease in comfort than SBAC ($OR = 1.89$, $p < 0.001$) and RBAC ($OR = 1.87$, $p < 0.001$). Data Type Suppression had an odds ratio of 1.24 (representing less of a decrease in comfort relative to FERPA Block), but this difference was not statistically significant ($p = 0.228$).

When making the opt-out decision after being shown the effects, many respondents (N=158) said they considered both privacy and functional effects. 73 respondents explicitly stated that even though

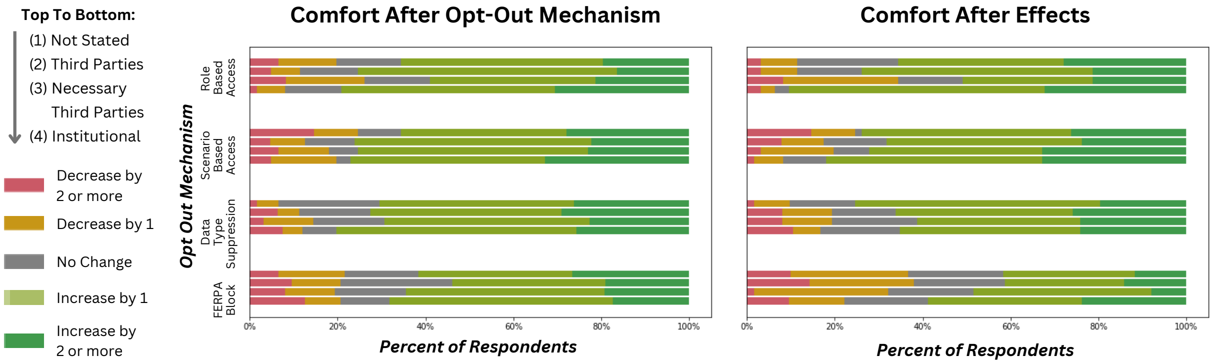


Figure 6: The relative change in self-reported Likert scale comfort after participants are given the opportunity to opt out with their respective systems (left) and after participants are shown the functional and privacy effects associated with opting out (right).

Variable	Value	Odds Ratio	CI	p-value
	FERPA Block	–	–	–
Opt-Out Policies	**Data Type Suppression**	1.24	[0.87, 1.75]	0.228
	SBAC	1.89	[1.33, 2.68]	$< 0.001^*$
	RBAC	1.87	[1.31, 2.65]	$< 0.001^*$

*Significant effect – Base case

Table 13: Summary of regression for H6: student comfort after seeing the effects of opting out. Pseudo R^2 measures for the model were 0.01 (McFadden) and 0.02 (Nagelkerke).

they wanted to opt out because of privacy concerns, they felt the functional effects mandated they opt in–they had no choice. For example, one participant stated: “I am not satisfied with the current level of privacy I have selected, but it appears that I have no choice. In order to stay up to date with my university, it seems I have to relinquish my qualms against third parties seeing my information.”

6 DISCUSSION

Through our investigation, we identify a number of issues with the current system for student directory information sharing when compared to students' reported preferences. In this section, we outline those issues along with recommendations for how policy makers and universities can implement changes to address them.

Universities are not transparent about directory sharing practices. Of the 100 universities we surveyed, almost all (n=97) did not explicitly provide students information regarding which parties their data will be shared with, and what directory data will be shared. Those that do provide information to students about who information will be shared with do not do so comprehensively, instead only providing examples of who they may share data with. Only four schools explicitly stated they would not share this data with any third parties outside of the university. This appeared to be the biggest mismatch between practices and student preferences.

This lack of transparency regarding sharing practices does not match student preferences; We demonstrate students are more comfortable when they know what data is being shared, and especially with whom.

Students cannot control data sharing by scenario. While students are provided opt-out mechanisms, these opt out mechanisms are generally quite limited. 40 universities only allow students a binary choice to opt in or out of sharing all directory data. Alternatively, 29 universities allowed students to opt out of sharing different data types. Only 16 universities allowed students to control data sharing for different scenarios or different parties.

This is not in alignment with the findings of our study, which suggest students were least comfortable with “all or nothing" approaches, and most comfortable when provided with control over with whom data is shared, and what data is shared, the least common approach in practice.

Universities state strong consequences of opting out that discourage students from making that choice. There are many reasons a student may choose to opt out, ranging from concern with data broker collection, to concerns surrounding stalking or doxxing. However, when students go to opt out, often before they may do so (n=52 universities), they are shown the potential consequences of choosing to opt out, ranging from missing emails or messages, to not getting employment verification or having their awards listed, to not being listed in the yearbook or graduation program. Our survey results demonstrate that students view these consequences as eliminating any real choice to opt out. Furthermore, in Section 4, we observe that universities often make it difficult for students to complete the opt out process, requiring students to opt out in-person, by a certain date, and on an annual basis.

Based on these results, we provide recommendations for policy makers and university staff members to address these concerns and align university policies with student preferences.

6.1 Recommendations For Policy Makers

There are several changes that can be made to existing legislation to target student concerns, through limiting the amount of information that can be shared, and limiting the situations under which that information can be shared.

Reconsider the need for broad FERPA exemptions. Carve-outs are common in privacy legislation; allowing for certain information to be disclosed on the basis that it is reasonable to believe the information is otherwise available to the public [67]. In some sense, §99.31(11) is a public information carve out, allowing for certain (directory) information to be exempt from the restrictions put in place by FERPA, and shared with the general public. Our survey results demonstrate that the data included in the student directory information exemption is unacceptably large: students agree that at least a significant subset of this data should not be shared.

Based upon these findings, we recommend minimizing the data included in this exemption. For example, one data type that survey participants regularly voiced discomfort with was the sharing of addresses; universities could remove this from the list and require student consent to share. It is unlikely the full extent of data in Table 1 needs to be shared without student consent.

These policy concerns are also echoed in research surrounding learning analytics. FERPA's School Officials Exemption discussed in Section 2.3, is currently being used by companies to get around legislation such as FERPA and COPPA, that are intended to prevent collection of student data [60]. It appears that, in the case of both learning analytics and student directory information, the exemptions to FERPA are excessively broad, and are thus being taken advantage of by companies seeking to profit off student data.

Consider the impact of additional privacy legislation. It is worth considering whether additional federal privacy legislation would address the issues our study brings to light. Comprehensive federal privacy legislation may address concerns surrounding consent to data sharing. Specifically, it is possible that federal privacy legislation could overstep the directory information exemption. For example, if the recently proposed American Data Privacy and Protection Act (ADPPA) were to be adopted, the FTC would resolve the interaction between FERPA and any new federal privacy legislation [15]; thus, the FTC would determine whether the student directory information exemption would remain in compliance.

Additionally, legislation could take a more targeted form to address student information privacy beyond the K-12 level. For example, PPRA, as mentioned in Section 2.3, regulates elementary and secondary (K-12) schools sharing students' data [88]. Extending this legislation to higher education would likely address the ability of marketers to obtain student data in the current manner, or at a minimum, discourage it. However, Rhoades discusses whether the Department of Education has the resources to challenge massive corporations, as would be necessary [60].

Create templates for student notification that allow students greater autonomy. Federal legislation is slow to change, thus, it is important to consider policy changes that can be made in the short term. As mentioned in Section 4, the Department of Education (DoE) maintains a template notice schools can use as an example when crafting what information to provide students about university directory information sharing practices. This template (see Appendix 7.4) suggests text similar to what we see in many universities' implementations: the form provides the data types considered to be directory information, and then says students may contact registrars to opt out of "any or all" sharing (N=12). This form, however, does not provide any specific negative effects, and does not provide an explicit policy on who data will and will not be shared with.

Further, at the top of this form, it states universities may choose to adopt a *limited directory information policy*, in which they "must specify parties who may receive information and/or the purposes for which it may be disclosed." Following this suggestion would better address the student preferences expressed in our survey, which demonstrated students want control over not only **what** data is shared, but **who** it is shared with. However, no template is provided for this type of directory policy. Since it appears many universities are directly or indirectly basing their directory information policies on the DoE template, creating a limited directory information policy template would likely increase the adoption of policies aligning with student preferences to control **who** has access to their data. This change would likely not require legislative action.

Limit the data types defined as directory information in template notices. As shown in Table 1, current definitions of directory information contain various data types. The DoE template notice contains a wide range of data types. While some of these data types may be necessary for a given use case–for example, sharing an athlete's height and weight with recruiters, it is unlikely the full scope of information contained in this definition is necessary. Even if FERPA itself is not able to be modified to regulate these data types more specifically, reducing the data listed on the DoE's template would potentially contribute to universities sharing a smaller list of directory information. For example, we see little reason that information like students' date and place of birth need to be shared without their consent.

We recognize that all cases are not as clear cut—-for example, including participation in officially recognized activities in the definition of directory information allows institutions to share information about organizations on campus, and any achievements or events students may have taken part in through that club. However, this can also lead to large-scale doxxing of students for their affiliation with affinity or political groups [28]. Our results in Section 5 make it clear that students are uncomfortable with many of the data types included in these directory information definitions. Policy makers ought to update definitions to align with student preferences.

6.2 Recommendations For Universities

In our experience with university registrars in Section 4, they are striving to act in their students' interest, but are functioning with limited time and resources. Therefore, we expect many registrars would adopt simple changes, providing direct benefit to students as we wait for the government to enact the broader changes described above. For this reason, we also provide recommendations for universities and registrars to create more effective student directory information policies.

Universities should explicitly tell students with whom they will and will not share data. If universities are in fact only sharing within their institution or necessary third parties, students should be informed, as it will likely improve student comfort. This negative mismatch between student perception and sharing reality is likely true in several schools that already exercise caution by not sharing data with third parties (this was true of multiple schools that responded to our FOIA responses), but are not transparent about this fact to students.

It is likely that part of why schools do not currently share a list of who data is shared with is because this list would regularly change as they receive requests. However, we believe it is worth the administrative overhead of sharing this list. If universities are sharing directory information with third parties students might be uncomfortable with, we did not observe any benefit to hiding this from students.

Universities should tailor third party sharing to organizations that provide useful services to students. In Section 3, we found some universities share personally identifiable information (students' names, contact information, etc.) and university-related information (major and academic status) with third parties, including data brokers and advertisers. However, our survey (Section 5) suggests students are much more uncomfortable when data is shared with third parties for indirect use, compared with when data is shared institutionally or with third parties for direct use.

To increase student comfort, universities should exercise caution in sharing student information with third parties, though this does not mean universities should cease all data sharing. Students were comfortable sharing data with outside parties in some cases: for example, with potential employers calling for degree verification. However, data sharing in these situations should be limited to data types students were more comfortable with, e.g., student name and degree status, rather than more sensitive information, e.g., emails, addresses, phone numbers, and more detailed university information. These items, are likely unnecessary to share with third parties for university function, but rather are shared for optional services. As a possible solution, universities could remove most personally identifiable information from third party sharing by default. Implementing these more detailed systems would allow universities to fulfill essential functions, allow students to access useful university services and events, and allow universities to use directory information internally, while fitting student privacy needs. Several universities in our study minimized sharing to these necessary conditions, so this should be possible for other similar institutions.

We also observed an interesting trend regarding institutional data that should be investigated further. That is, students were more likely to opt out of institutional (internal) sharing when institutional sharing was the only option given, compared to conditions where they could opt out of external sharing as well. Further research is needed to determine whether this is the result of action bias [54] or if students do not indicate their true privacy preferences when given more options. Prior work has shown users are less likely to act privacy consciously when given more control (i.e., the control paradox) [12] and that available options and default settings can impact privacy decisions [1, 81], suggesting there can be unexpected impacts on student decision-making depending on the display of opt-out options.

Students should be presented with the functional effects *and privacy effects* of opting out. In Section 4, we see schools frequently present the functional effects of opting out, but rarely mention positive impacts of opting out, namely protecting student privacy.

Our survey results demonstrate students are concerned about both the privacy and functional effects of opting out; they were less comfortable with systems which prevent students from balancing these trade-offs. Describing privacy and functional effects also led many students to revisit their opt-out decisions (N=462), in most cases loosening their opt-out restrictions (N=346). Without knowing the full effects of opting out, students would have lost functionalities they would have been comfortable trading for privacy. It is important universities present both privacy and functional effects, and allow students to make decisions with full information. RBAC and SBAC fit this requirement well, allowing students to evaluate and control the trade-off for themselves.

Universities should limit the need for functional effects of opting out. In Section 4, we saw that universities listed strong functional effects of opting out, such as missing emails and messages, not being able to do employment verification, and not being listed in commencement programs. In Section 5, we observed that these functional effects have a large impact on student decisions. Therefore, it is important that institutions avoid levying them if they're unnecessary, but rather, adjust the way the policy and technical systems are structured to remove unnecessary burdens. For example, rather than informing students that they may miss emails or messages, the university could ensure that any important communications are not managed by a third party mailing service, so students will not be negatively impacted. Similarly, instead of informing the student that they will not be listed in the commencement program or able to have their employment verified if they choose to opt out, universities could provide students with contextual choices, that allow them to share their data in different sharing scenarios.

Universities should avoid "all-or-nothing" opt out approaches, but more research needed to determine the right opt-out system. In Section 4, schools most frequently used FERPA Block systems, which give students minimal autonomy—only an all-or-nothing opt out. As we might expect, Section 5 finds students generally did not like this approach.

Instead, students viewed Data Type Suppression, SBAC, and RBAC policies as better aligned with their privacy preferences, and are more comfortable than students shown FERPA Block. Of these three systems, participants did not demonstrate a strong preference; their comfort levels were similar. The only difference observed between these systems was that participants were less likely to opt back into sharing after being shown the opt out effects in the SBAC condition. This suggests SBAC may provide more context upfront to better support opt out decisions. However, SBAC provides less control over data sharing than RBAC (a feature students commonly requested). Future work should investigate the reason for this difference and each system's utility in practice.

ACKNOWLEDGMENTS

We would like to thank the reviewers for their helpful feedback, as well as the student survey participants and the registrars for their engagement. We would also like to thank Josephine Wolff for her helpful feedback. This work was supported in part by a Google Research Award.

REFERENCES

[1] Idris Adjerid, Alessandro Acquisti, and George Loewenstein. 2014. Framing and the malleability of privacy choices. In *Proceedings of the 13th Workshop on the Economics of Information Security.*

[2] American Council on Education. [n. d.]. Carnegie Classification of Institutions of Higher Education. https://carnegieclassifications.acenet.edu. Accessed 12/11/2023.

[3] Janine Arantes. 2023. Educational data brokers: using the walkthrough method to identify data brokering by edtech platforms. *Learning, Media and Technology* (2023), 1–14. https://doi.org/10.1080/17439884.2022.2160986

[4] ASL Marketing. [n. d.]. Privacy-First Student & Youth Data. https://aslmarketing.com. https://aslmarketing.com Accessed 12/11/2022.

[5] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. 2012. The menlo report. *IEEE Security & Privacy* 10, 2 (2012), 71–75. https://doi.org/10.1109/MSP.2012.52

[6] David G Balash, Dongkun Kim, Darika Shaibekova, Rahel A Fainchtein, Micah Sherr, and Adam J Aviv. 2021. Examining the examiners: Students' privacy and security perceptions of online proctoring services. In *Seventeenth symposium on usable privacy and security (SOUPS 2021).* 633–652.

[7] Susan B Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* (2006). https://doi.org/10.5210/fm.v11i9.1394

[8] Kathleen Benitez and Bradley Malin. 2010. Evaluating re-identification risks with respect to the HIPAA privacy rule. *Journal of the American Medical Informatics Association* 17, 2 (2010). https://doi.org/10.1136/jamia.2009.000026

[9] Erik Carl Bennett. 2020. *Jumping into the Cloud: Privacy, Security and Trust of Cloud-Based Computing within K-12 American Public Education.* Ph. D. Dissertation. City University of New York.

[10] College Board. [n. d.]. Understand College Campus and Student Body Size. https://bigfuture.collegeboard.org/plan-for-college/college-basics/types-of-colleges/understand-college-campus-student-body-size. Accessed 12/11/2023.

[11] Stian Botnevik, Mohammad Khalil, and Barbara Wasson. 2020. Student awareness and privacy perception of learning analytics in higher education. In *Addressing Global Challenges and Quality Education: 15th European Conference on Technology Enhanced Learning, EC-TEL 2020, Heidelberg, Germany, September 14–18, 2020, Proceedings 15.* Springer, 374–379. https://doi.org/10.1007/978-3-030-57717-9_30

[12] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4, 3 (2013), 340–347. https://doi.org/10.1177/1948550612455931

[13] Michael Brown and Carrie Klein. 2020. Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents. *The Journal of Higher Education* 91, 7 (2020), 1149–1178. https://doi.org/10.1080/00221546.2020.1770045

[14] Juliet Corbin and Anselm Strauss. 2014. *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Sage publications. https://doi.org/10.1177/1094428108324514

[15] Jarret Cummings. 2022. A Possible Move Toward Comprehensive Federal Privacy Legislation. *Educause Review* (2022). https://er.educause.edu/articles/2022/8/a-possible-move-toward-comprehensive-federal-privacy-legislation

[16] Michele Lee Cunha. 2018. *Privacy Rights for Families and Children in K-12 Schools: A Mixed-Methods Study on the Effects of Perceptions of Educators on Implementation of the Family Educational Rights and Privacy Act (FERPA).* Ph. D. Dissertation. Concordia University Irvine.

[17] Adrian Dabrowski, Georg Merzdovnik, Johanna Ullrich, Gerald Sendera, and Edgar Weippl. 2019. Measuring Cookies and Web Privacy In a Post-GDPR World. In *Passive and Active Measurement: 20th International Conference, PAM 2019, Puerto Varas, Chile, March 27–29, 2019, Proceedings 20.* Springer, 258–270. https://doi.org/10.1007/978-3-030-15986-3_17

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

[19] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2018. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. *arXiv preprint arXiv:1808.05096* (2018). https://doi.org/10.48550/arXiv.1808.05096

[20] Martin R Dowding. 2011. Interpreting privacy on campus: the freedom of information and personal privacy and Ontario universities. *Canadian Journal of Communication* 36, 1 (2011), 11. https://doi.org/10.22230/cjc.2011v36n1a2252

[21] Rachel Fishman. 2012. Perception vs. Reality: The Typical College Student. https://www.newamerica.org/in-depth/varying-degrees/perception-vs-reality-typical-college-student/. Accessed 12/11/2023.

[22] Flytedesk. [n. d.]. Flytedesk - How It Works. https://www.flytedesk.com/how-it-works. https://www.flytedesk.com/how-it-works Accessed 12/11/2022.

[23] Jorge Galarza. 2019. *A Learning Style Group Comparison of Southern California Public School Employees: Investigating the Level of Understanding Family Educational Rights and Privacy Act (FERPA) When Using a Preferred Learning Style Training.* Ph. D. Dissertation. California Baptist University.

[24] Ann Gilley and Jerry W Gilley. 2006. FERPA: What do faculty know? What can universities do? *College and University* 82, 1 (2006), 17.

[25] Thomas Groß. 2021. Validity and reliability of the scale internet users' information privacy concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies* (2021). https://doi.org/10.2478/popets-2021-0026

[26] Melanie Hanson. 2022. College Enrollment & Student Demographic Statistics. https://educationdata.org/college-enrollment-statistics. Accessed 12/11/2023.

[27] Melanie Hanson. 2022. College Enrollment & Student Demographic Statistics. https://educationdata.org/college-enrollment-statistics. Accessed 12/11/2023.

[28] Sarah Hartman-Caverly. 2023. The Failure of FERPA. *Inside Higher Ed* (2023). https://www.insidehighered.com/opinion/views/2023/10/26/harvard-doxing-truck-shows-ferpas-obsolescence-opinion

[29] Andrew F Hayes and Klaus Krippendorff. 2007. Answering the call for a standard reliability measure for coding data. *Communication methods and measures* 1, 1 (2007), 77–89. https://doi.org/10.1080/19312450709336664

[30] Maximilian Hils, Daniel W Woods, and Rainer Böhme. 2020. Measuring the emergence of consent management on the web. In *Proceedings of the ACM Internet Measurement Conference.* 317–332. https://doi.org/10.1145/3419394.3423647

[31] John B. Horrigan. 2016. Digital Readiness Gaps. https://www.pewresearch.org/internet/2016/09/20/digital-readiness-gaps/. Accessed 12/11/2023.

[32] Steven Johns and Karen Lawson. 2005. University undergraduate students and library-related privacy issues. *Library & Information Science Research* 27, 4 (2005), 485–495. https://doi.org/10.1016/j.lisr.2005.08.006

[33] Kyle ML Jones, Abigail Goben, Michael R. Perry, Mariana Regalado, Dorothea Salo, Andrew D. Asher, Maura A. Smale, and Kristin A. Briney. 2023. Transparency and Consent: Student Perspectives on Educational Data Analytics Scenarios. *portal: Libraries and the Academy* 23, 3 (2023), 485–515. https://doi.org/10.1353/pla.2023.a901565

[34] Patrick Gage Kelley, Michael Benisch, Lorrie Faith Cranor, and Norman Sadeh. 2011. When are users comfortable sharing locations with advertisers?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* 2449–2452. https://doi.org/10.1145/1978942.1979299

[35] Mohammad Khalil, Paul Prinsloo, and Sharon Slade. 2018. User consent in MOOCs–micro, meso, and macro perspectives. *International Review of Research in Open and Distributed Learning* 19, 5 (2018). https://doi.org/10.19173/irrodl.v19i5.3908

[36] Mohammad Khalil, Paul Prinsloo, and Sharon Slade. 2022. In the nexus of integrity and surveillance: Proctoring (re) considered. *Journal of Computer Assisted Learning* 38, 6 (2022), 1589–1602. https://doi.org/10.1111/jcal.12713

[37] Mohammad Khalil, Paul Prinsloo, and Sharon Slade. 2023. Fairness, Trust, Transparency, Equity, and Responsibility in Learning Analytics. *Journal of Learning Analytics* 10, 1 (2023), 1–7. https://doi.org/10.18608/jla.2023.7983

[38] Tadayoshi Kohno, Yasemin Acar, and Wulf Loh. 2023. Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations. *arXiv preprint arXiv:2302.14326* (2023). https://doi.org/10.48550/arXiv.2302.14326

[39] Maina Korir, Sharon Slade, Wayne Holmes, Yingfei Héliot, and Bart Rienties. 2023. Investigating the dimensions of students' privacy concern in the collection, use and sharing of data for learning analytics. *Computers in human behavior reports* 9 (2023), 100262. https://doi.org/10.1016/j.chbr.2022.100262

[40] Michael Kretschmer, Jan Pennekamp, and Klaus Wehrle. 2021. Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web (TWEB)* 15, 4 (2021), 1–42. https://doi.org/10.1145/3466722

[41] Daniel G Krutka, Ryan M Smits, and Troy A Willhelm. 2021. Don't be evil: Should we use Google in schools? *TechTrends* 65, 4 (2021), 421–431. https://doi.org/10.1007/s11528-021-00599-4

[42] LexisNexis. [n. d.]. LexisNexis Risk Solutions. https://risk.lexisnexis.com. https://risk.lexisnexis.com Accessed 12/11/2022.

[43] David M Liu. 2017. Mining FERPA Notices for Textual Analysis of Education Privacy Policy. https://dliu18.github.io/files/papers/legal_nlp.pdf.

[44] Qinyi Liu and Mohammad Khalil. 2023. Understanding privacy and data protection issues in learning analytics using a systematic review. *British Journal of Educational Technology* 54, 6 (2023), 1715–1747. https://doi.org/10.1111/bjet.13388

[45] Chaoyi Lu, Baojun Liu, Yiming Zhang, Zhou Li, Fenglu Zhang, Haixin Duan, Ying Liu, Joann Qiongna Chen, Jinjin Liang, Zaifeng Zhang, et al. 2021. From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR. In *NDSS.* https://doi.org/10.14722/ndss.2021.23134

[46] Roxana Marachi and Lawrence Quill. 2020. The case of Canvas: Longitudinal datafication through learning management systems. *Teaching in Higher Education* 25, 4 (2020), 418–434. https://doi.org/10.1080/13562517.2020.1739641

[47] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23. https://doi.org/10.1145/3359174

[48] Karen McVeigh. 2011. Cyberstalking 'now more common' than face-to-face stalking. https://www.theguardian.com/uk/2011/apr/08/cyberstalking-study-victims-men. *The Guardian* 13 (2011), 31. Accessed 12/11/2023.

[49] Alex Molnar and Faith Boninger. 2020. The commercial transformation of America's schools. *Phi Delta Kappan* 102, 2 (2020), 8–13. https://doi.org/10.1177/0031721720963223

[50] National Center For Education Statistics. 2021. Fast Facts - Enrollment. https://nces.ed.gov/fastFacts/display.asp?id=98. Accessed 12/11/2023.

[51] Department of Education. 2011. Model Notice for Directory Information. https://studentprivacy.ed.gov/resources/model-notice-directory-information.

[52] Abelardo Pardo and George Siemens. 2014. Ethical and privacy principles for learning analytics. *British journal of educational technology* 45, 3 (2014), 438–450. https://doi.org/10.1111/bjet.12152

[53] Cecelia Parks. 2017. Beyond compliance: Students and FERPA in the age of big data. *Journal of Intellectual Freedom and Privacy* 2, 2 (2017), 23. https://doi.org/10.5860/jifp.v2i2.6253

[54] Anthony Patt and Richard Zeckhauser. 200. Action Bias and Environmental Decisions. *Journal of Risk and Uncertainty* 21, 1 (200), 45–72. https://doi.org/10.1023/A:1026517309871

[55] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153 – 163. https://doi.org/10.1016/j.jesp.2017.01.006

[56] Paul Prinsloo and Sharon Slade. 2015. Student privacy self-management: Implications for learning analytics. In *Proceedings of the fifth international conference on learning analytics and knowledge*. 83–92. https://doi.org/10.1145/2723576.2723585

[57] Paul Prinsloo, Sharon Slade, and Mohammad Khalil. 2022. The answer is (not only) technological: Considering student data privacy in learning analytics. *British Journal of Educational Technology* 53, 4 (2022), 876–893. https://doi.org/10.1111/bjet.13216

[58] Adrian E Raftery. 1995. Bayesian model selection in social research. *Sociological methodology* (1995), 111–163. https://doi.org/10.2307/271063

[59] Tamjid Al Rahat, Minjun Long, and Yuan Tian. 2022. Is Your Policy Compliant? A Deep Learning-based Empirical Study of Privacy Policies' Compliance with GDPR. In *Proceedings of the 21st Workshop on Privacy in the Electronic Society*. 89–102. https://doi.org/10.1145/3559613.3563195

[60] Amy Rhoades. 2020. Big tech makes big data out of your child: The FERPA loophole edtech exploits to monetize student data. *Am. U. Bus. L. Rev.* 9 (2020), 445.

[61] Katelyn Ringrose. 2018. Data Collection in Schools: Privacy Implications for K-12 Students under a Weakened FERPA. *Dartmouth LJ* 16 (2018), 130.

[62] Alan Rubel and Kyle ML Jones. 2016. Student privacy in learning analytics: An information ethics perspective. *The information society* 32, 2 (2016), 143–159. https://doi.org/10.1080/01972243.2016.1130502

[63] N Cameron Russell, Joel R Reidenberg, Elizabeth Martin, and Thomas B Norton. 2018. Transparency and the marketplace for student data. *Va. JL & Tech.* 22 (2018), 107.

[64] Nikita Samarin, Shayna Kothari, Zaina Siyed, Primal Wijesekera, Jordan Fischer, Chris Hoofnagle, and Serge Egelman. 2021. Investigating the Compliance of Android App Developers with the CCPA. In *5th Workshop on Technology and Consumer Protection (ConPro'21)*.

[65] Benjamin Scheibehenne, Rainer Greifeneder, and Peter M Todd. 2010. Can there ever be too many options? A meta-analytic review of choice overload. *Journal of consumer research* 37, 3 (2010), 409–425. https://doi.org/10.1086/651235

[66] Alexander R Schrameyer, Tracy M Graves, David M Hua, and Nile C Brandt. 2016. Online Student Collaboration and FERPA Considerations. *TechTrends* 60, 6 (2016), 540–548. https://doi.org/10.1007/s11528-016-0117-5

[67] Justin Sherman. 2023. People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs. https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs. *Lawfare* (2023).

[68] Sharon Slade and Paul Prinsloo. 2013. Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist* 57, 10 (2013), 1510–1529. https://doi.org/10.1177/0002764213479366

[69] Sharon Slade and Paul Prinsloo. 2014. Student perspectives on the use of their data: Between intrusion, surveillance and care. In *EDEN Conference Proceedings*. 291–300.

[70] Sharon Slade, Paul Prinsloo, and Mohammad Khalil. 2019. Learning analytics at the intersections of student trust, disclosure and benefit. In *Proceedings of the 9th International Conference on learning analytics & knowledge*. 235–244. https://doi.org/10.1145/3303772.3303796

[71] Sharon Slade, Paul Prinsloo, and Mohammad Khalil. 2023. Trust us, they said. Mapping the contours of trustworthiness in learning analytics. *Information and Learning Sciences* 124, 910 (2023), 306–325. https://doi.org/10.1108/ILS-04-2023-0042

[72] Aaron Smith, Lee Rainie, and Kathryn Zickuhr. 2011. College students and technology. https://www.pewresearch.org/internet/2011/07/19/college-students-and-technology/. Accessed 12/11/2023.

[73] Elliott Sober. 2002. Instrumentalism, Parsimony, and the Akaike Framework. *Philosophy of Science* 69, S3 (2002), S112–S123. https://doi.org/10.1086/341839

[74] Mindy B Steinberg. 2003. *A comparative study of the policies, procedures, training and enforcement of the Family Educational Rights and Privacy Act (FERPA) at public and private colleges and universities in four Carnegie classifications of institutions of higher education in the United States*. University of Louisville.

[75] Francesca Stevens, Jason RC Nurse, and Budi Arief. 2021. Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking* 24, 6 (2021), 367–376. https://doi.org/10.1089/cyber.2020.0253

[76] Anselm Strauss and Juliet Corbin. 1990. *Basics of qualitative research*. Vol. 15. Newbury Park, CA: Sage. https://doi.org/10.5072/genderopen-develop-7

[77] Student Press Law Center. [n. d.]. FERPA: What it means and how it works. https://splc.org/ferpa-what-it-means-and-how-it-works/. Accessed 12/11/2023.

[78] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 367–385. https://doi.org/10.48550/arXiv.2202.14036

[79] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, et al. 2021. Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 247–267. https://doi.org/10.1109/SP40001.2021.00028

[80] Melody M Tsang, Shu-Chun Ho, and Ting-Peng Liang. 2004. Consumer attitudes toward mobile advertising: An empirical study. *International journal of electronic commerce* 8, 3 (2004), 65–78. https://doi.org/10.1080/10864415.2004.11044301

[81] Markus Tschersich. 2015. Comparing the Configuration of Privacy Settings on Social Network Sites Based on Different Default Options. In *2015 48th Hawaii International Conference on System Sciences*. 3453–3462. https://doi.org/10.1109/HICSS.2015.416

[82] Julie Underwood. 2017. Under The Law: You say 'records,'and I say 'data'. *Phi Delta Kappan* 98, 8 (2017), 74–75. https://doi.org/10.1177/0031721717708303

[83] UniRank. [n. d.]. A-Z Universities in the United States. https://www.4icu.org/us/a-z/. Accessed 12/11/2023.

[84] US Code. 1974. 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.

[85] US Congress. 1974. Family Educational Rights and Privacy Act (FERPA). 20 U.S.C. § 1232g. 1974.

[86] US Congress. 1996. Solomon Act - 10 U.S. Code § 983. https://www.law.cornell.edu/uscode/text/10/983.

[87] US Department of Education. [n. d.]. Directory Information. https://studentprivacy.ed.gov/content/directory-information. Accessed 12/11/2022.

[88] U.S. Department of Education. 2020. PPRA Model General Notice of Rights. https://studentprivacy.ed.gov/resources/ppra-model-general-notice-rights. Accessed 12/11/2023.

[89] US Department of Education. 2021. Family Educational Rights and Privacy Act (FERPA) Home Page. "https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html".

[90] Emily Vogels. 2021. The State of Online Harassment. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/. Accessed 12/11/2023.

[91] Alexander Whitelock-Wainwright, Dragan Gašević, Ricardo Tejeiro, Yi-Shan Tsai, and Kate Bennett. 2019. The student expectations of learning analytics questionnaire. *Journal of Computer Assisted Learning* 35, 5 (2019), 633–666. https://doi.org/10.1111/jcal.12366

[92] Alexander Whitelock-Wainwright, Yi-Shan Tsai, Hendrik Drachsler, Maren Scheffel, and Dragan Gašević. 2021. An exploratory latent class analysis of student expectations towards learning analytics services. *The Internet and Higher Education* 51 (2021), 100818. https://doi.org/10.1016/j.iheduc.2021.100818

[93] Emma Whitford and Caroline Howard. [n. d.]. Forbes America's Top Colleges 2021. https://www.forbes.com/top-colleges/. https://www.forbes.com/top-colleges/ Accessed 12/11/2022.

[94] Richmond Y Wong, Andrew Chong, and R Cooper Aspegren. 2023. Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023). https://doi.org/10.1145/3579515

[95] Eric James York. 2021. Digital surveillance in online writing instruction: Panopticism and simulation in learning management systems. *Computers and Composition* 62 (2021), 102680. https://doi.org/10.1016/j.compcom.2021.102680

[96] Razieh Nokhbeh Zaeem and K Suzanne Barber. 2020. The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)* 12, 1 (2020), 1–20. https://doi.org/10.1145/3389685

[97] Elana Zeide. 2015. Student privacy principles for the age of big data: Moving beyond FERPA and FIPPS. *Drexel L. Rev.* 8 (2015), 339.

[98] Shoshana Zuboff. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Profile books.

7 APPENDIX

7.1 Qualtrics Survey

We provide the complete text of our survey for one condition (Third Party Sharing and FERPA Block), the remaining conditions are attached in supplementary materials.

In this study, we will ask you to make decisions as a student about what data you would or would not be comfortable with your university sharing about you.

While federal laws protect most student data from distribution, universities are permitted to share student directory information. For this study, assume your university defines the following to be student directory information:

- Your name, email, mailing address, phone number, date and place of birth.
- Your degree status, academic awards, dates of attendance, major, participation in sports and school activities, previous institution, class year, and enrollment status.

Your university will share this data with **any third parties that call the registrar and request it**.
This could be for **direct use**, for example, these parties may include third party mailing service providers used by the school for email listserv delivery, or companies that offer moving services for students.
This could also be for **indirect use**, for example, these parties could include companies that collect and sell user data for advertising purposes, or with individuals who call to request your data.

Your university will also share this data for **institutional use**.
This means that parties within the university can access this data for purposes related to university events.
For example, the data maybe used to compile lists for school event entry and to allow your name to be a part of the commencement program.

How comfortable would you be with your university sharing the information about you as described above?

(1) Extremely uncomfortable
(2) Somewhat uncomfortable
(3) Neither comfortable nor uncomfortable
(4) Somewhat comfortable
(5) Extremely comfortable

Please briefly explain why you chose this level of comfort.

Please select the data type that the university DOES NOT consider directory data.

(1) Place of Birth
(2) Dates of Attendance
(3) Emergency Contact
(4) Phone Number

FERPA requires universities to allow students to opt out of data sharing. Now, we will show you how you can opt out of the previously described data sharing and ask you to indicate what sharing you would choose to opt out of in this scenario.

Given the previous information about your school's data sharing policy, please pick the one of these options that most closely reflects your data sharing preference.

(1) Allow my information to be shared with the given parties.
(2) Do not allow my information to be shared with the given parties.

How comfortable are you with the university sharing your directory information in the way you have opted to share it above?

(1) Extremely uncomfortable
(2) Somewhat uncomfortable
(3) Neither comfortable nor uncomfortable
(4) Somewhat comfortable
(5) Extremely comfortable

Do you think the data sharing opt-out options provided above allowed you to make a selection that matches your privacy preferences?

(1) Strongly disagree
(2) Somewhat disagree
(3) Neither agree nor disagree
(4) Somewhat agree
(5) Strongly agree

Please briefly explain why you do or do not think these opt-out options allowed you to make a selection matching you privacy preferences?

What is one thing you would change about the opt-out options described above?

Your opt-out decisions impact on both your privacy (i.e., what data is shared about you) and the functionalities available to you (i.e., services provided by parties the data is shared with). In this section of the survey, we will describe these impacts of opting-out and ask you to reconsider your opt-out decision given this new information.

You should be aware of the possible effects of opting-out.

We will share these effects with you below, and ask you to reconsider your opt-out decision given this new information.
If you choose not to share any directory information, this information will not be released to anyone outside of the university.

If you choose to opt-out (i.e., choose not to allow data to be shared with the given parties), there may be **privacy effects**:

(1) Opting-out will prevent third parties from using your data for advertising, and other unauthorized purposes.

If you choose to opt-out, you may also have **functional effects**:

(1) You might not receive mailings, messages, and announcements from your school, department, or other university groups.
(2) You will not appear in the Commencement program or yearbook. You will also not be listed in the online directory or university phone book.
(3) This also will prevent the university from providing your directory information to your friends, prospective employers, and others with whom you may wish us to share such information.

With knowledge of these effects of opting-out, please make your selection as you would based upon the previous information about your school's data sharing policy.

(1) Allow my information to be shared with the given parties.
(2) Do not allow my information to be shared with the given parties.

Given your selections using the above opt-out policy, how comfortable are you with the university sharing your directory information in the way you selected?

(1) Extremely uncomfortable
(2) Somewhat uncomfortable
(3) Neither comfortable nor uncomfortable
(4) Somewhat comfortable
(5) Extremely comfortable

Please briefly explain why you chose to or not to change your opt-out selection preferences.

7.2 Registrar Emails

The various email templates we used to reach out to registrars are shown in Figures 7, 8, and 9.

7.3 FOIA Request Template

The template we used to submit our FOIA requests is shown in Figure 10.

7.4 FERPA directory information notice template

See Figure 11.

7.5 Opt-Out Systems

Below are the opt-outs as used in our survey:

FERPA Block Opt-Out:
Given the previous information about your school's data sharing policy, please pick the one of these options that most closely reflects your data sharing preference.
□ Allow my information to be shared with the given parties.
□ Do not allow my information to be shared with the given parties.

Data Type Suppression:
Given the previous information about your school's data sharing policy, please check each item you **do not want to be shared**.
□ Name
□ Course
□ Email Address
□ Campus Address
□ Campus Phone Number
□ Year and Registration Type
□ Phone Number
□ Term Address
□ Permanent Home Address
□ Degree Received
□ Date of Birth
□ Dates of Attendance

Scenario Based Access Control - All But Institutional
Given the previous information about your school's data sharing policy, please check each item you **do not want to be shared**:
□ The release of your academic degree program (degree, major, minor) to anyone outside of the university.
□ The inclusion of your name, college, degree and honors program in the Commencement program when you graduate.
□ The release of dates of attendance, full/part-time status to anyone outside the university, including insurance providers and employers.
□ The release of your date of birth and home address to anyone outside the university.
□ The release of your degrees, honors, and awards received to anyone outside the university.
□ The inclusion of your email address in the university online directory.
□ The inclusion of your local address and directory phone number in the university's online directory and phonebook.
□ The release of your school or college to anyone outside the university.
□ The inclusion of your name in the university yearbook when you graduate.

Scenario Based Access Control - Institutional
Given the previous information about your school's data sharing policy, please check each item you **do not want to be shared**:
□ The inclusion of your name, college, degree and honors program in the Commencement program when you graduate.
□ The release of dates of attendance, full/part-time status to anyone outside the university, including insurance providers and

employers.
□ The inclusion of your email address in the university online directory.
□ The inclusion of your local address and directory phone number in the university's online directory and phonebook.
□ The inclusion of your name in the university yearbook when you graduate.

Role Based Access Control - Third Parties and Not Stated
Given the previous information about your school's data sharing policy, please select the boxes for parties who you do not want to share data with.
As a reminder:
Sharing with **third parties** for indirect use means the data will be shared with any third parties that call the registrar and request it. For example, these parties may include third party mailing service providers used by the school for email listserv delivery, or companies that offer moving services for students.
Sharing for **direct use** means that data will be shared with third parties that the university views as benefiting students, namely, organizations that directly provide services to students and staff. For example, these parties could include companies that collect and sell user data for advertising purposes, or with individuals who call to request your data. Sharing for **institutional use** means that parties within the university can access this data for purposes related to university events. For example, the data maybe used to compile lists for school event entry and to allow your name to be a part of the commencement program.

[Third Parties Opt-Out Table (Table 14) is shown].

Role Based Access Control - Third Parties For Direct Use
Given the previous information about your school's data sharing policy, please select the boxes for parties who you do not want to share data with.
As a reminder:
Sharing for **direct use** means that data will be shared with third parties that the university views as benefiting students, namely, organizations that directly provide services to students and staff. For example, these parties could include companies that collect and sell user data for advertising purposes, or with individuals who call to request your data. Sharing for **institutional use** means that parties within the university can access this data for purposes related to university events. For example, the data maybe used to compile lists for school event entry and to allow your name to be a part of the commencement program.

[Third Parties Direct Sharing Opt-Out Table (Table 15) is shown].

Role Based Access Control - Institutional Given the previous information about your school's data sharing policy, please select the boxes for parties who you do not want to share data with.
As a reminder:
Sharing for **institutional use** means that parties within the university can access this data for purposes related to university events. For example, the data maybe used to compile lists for school event entry and to allow your name to be a part of the commencement program.

[Institutional Opt-Out Table (Table 16) is shown].

7.6 Opt-Out Data Type Results

We provide the participant opt out rates by data type for opt-out systems.

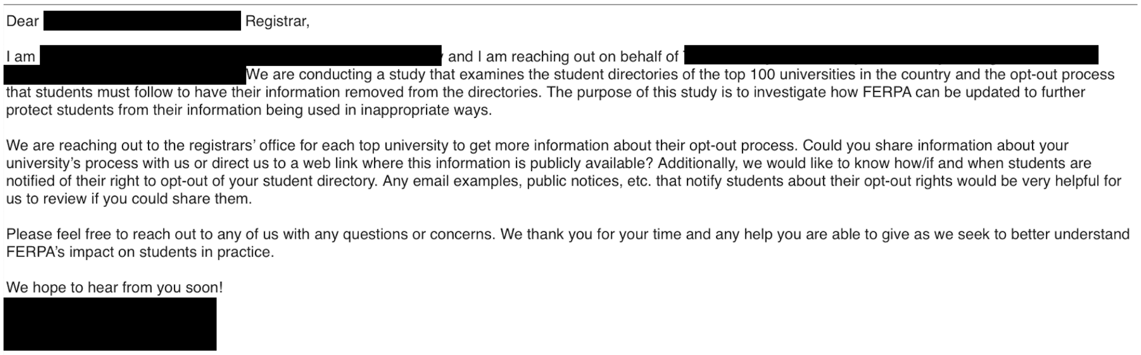
The **first percentage** represents the percent of participants who initially opted out of sharing the given data type.
The **second percentage** represents the percent change in opt out for the data type between the initial opt out and the second opt out, after the presentation of effects.
Data Type Suppression is shown in Table 17.
Scenario Based Access Control is shown in Table 18.
Role Based Access Control is shown in Tables 19 and 20.

7.7 Codebook

The codebooks we developed for our evaluating our survey data are shown in Figures 12, 13, 14.

7.8 Registrar Recommendations

Figures 15, 16, 17, and 18 show the document we sent to registrars at the conclusion of our study, providing an overview of best practices for student directory information management, as suggested by our findings.



Dear [redacted] Registrar,

I am [redacted] and I am reaching out on behalf of [redacted] We are conducting a study that examines the student directories of the top 100 universities in the country and the opt-out process that students must follow to have their information removed from the directories. The purpose of this study is to investigate how FERPA can be updated to further protect students from their information being used in inappropriate ways.

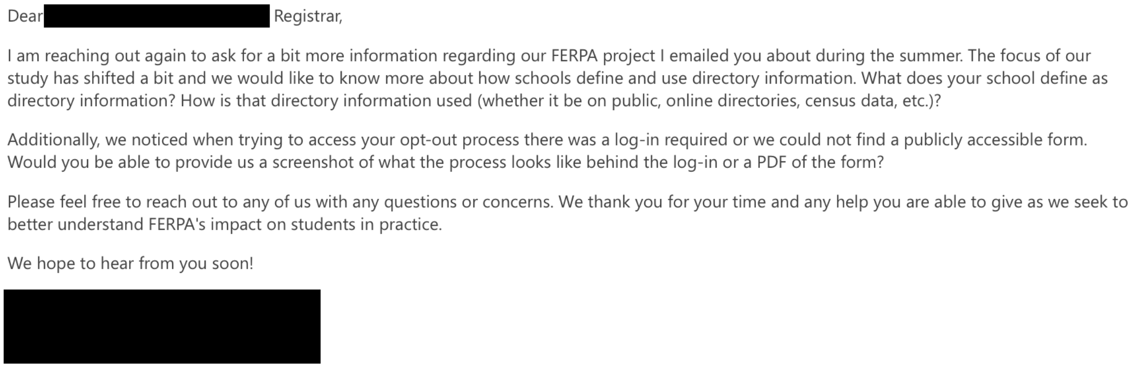
We are reaching out to the registrars' office for each top university to get more information about their opt-out process. Could you share information about your university's process with us or direct us to a web link where this information is publicly available? Additionally, we would like to know how/if and when students are notified of their right to opt-out of your student directory. Any email examples, public notices, etc. that notify students about their opt-out rights would be very helpful for us to review if you could share them.

Please feel free to reach out to any of us with any questions or concerns. We thank you for your time and any help you are able to give as we seek to better understand FERPA's impact on students in practice.

We hope to hear from you soon!

[redacted]

Figure 7: First email sent to registrars of universities with public or partially-public online directories



Dear [redacted] Registrar,

I am reaching out again to ask for a bit more information regarding our FERPA project I emailed you about during the summer. The focus of our study has shifted a bit and we would like to know more about how schools define and use directory information. What does your school define as directory information? How is that directory information used (whether it be on public, online directories, census data, etc.)?

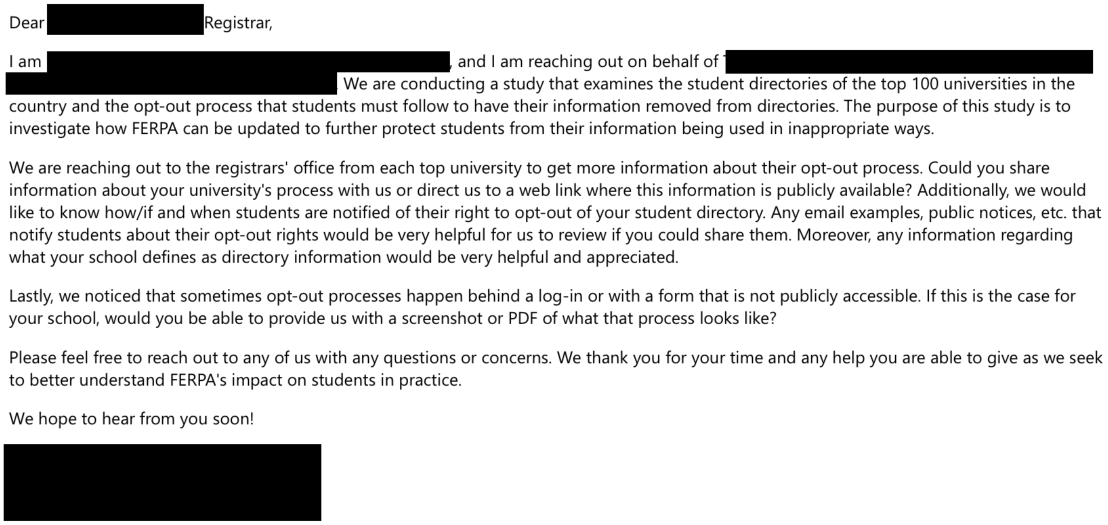
Additionally, we noticed when trying to access your opt-out process there was a log-in required or we could not find a publicly accessible form. Would you be able to provide us a screenshot of what the process looks like behind the log-in or a PDF of the form?

Please feel free to reach out to any of us with any questions or concerns. We thank you for your time and any help you are able to give as we seek to better understand FERPA's impact on students in practice.

We hope to hear from you soon!

[redacted]

Figure 8: Follow up email we sent to registrars of universities with public or partially-public online directories.



Dear [redacted] Registrar,

I am [redacted], and I am reaching out on behalf of [redacted] We are conducting a study that examines the student directories of the top 100 universities in the country and the opt-out process that students must follow to have their information removed from directories. The purpose of this study is to investigate how FERPA can be updated to further protect students from their information being used in inappropriate ways.

We are reaching out to the registrars' office from each top university to get more information about their opt-out process. Could you share information about your university's process with us or direct us to a web link where this information is publicly available? Additionally, we would like to know how/if and when students are notified of their right to opt-out of your student directory. Any email examples, public notices, etc. that notify students about their opt-out rights would be very helpful for us to review if you could share them. Moreover, any information regarding what your school defines as directory information would be very helpful and appreciated.

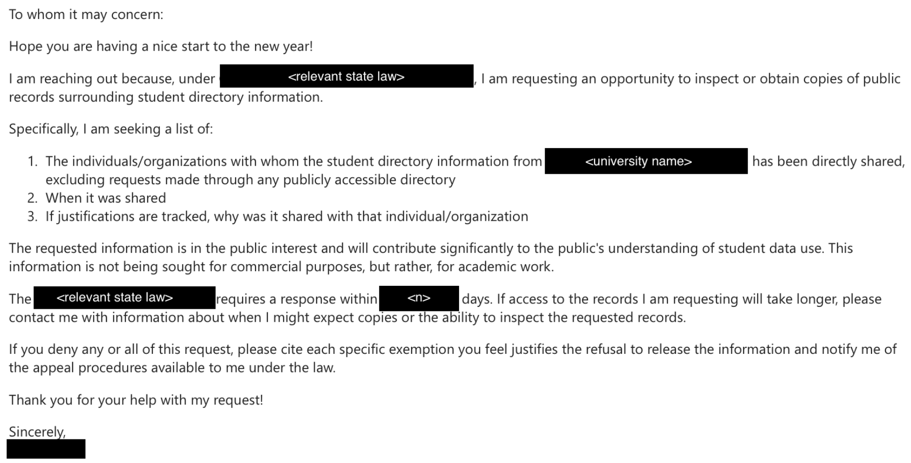
Lastly, we noticed that sometimes opt-out processes happen behind a log-in or with a form that is not publicly accessible. If this is the case for your school, would you be able to provide us with a screenshot or PDF of what that process looks like?

Please feel free to reach out to any of us with any questions or concerns. We thank you for your time and any help you are able to give as we seek to better understand FERPA's impact on students in practice.

We hope to hear from you soon!

[redacted]

Figure 9: Email we sent to registrars of universities without public directories.



To whom it may concern:

Hope you are having a nice start to the new year!

I am reaching out because, under <relevant state law>, I am requesting an opportunity to inspect or obtain copies of public records surrounding student directory information.

Specifically, I am seeking a list of:

1. The individuals/organizations with whom the student directory information from <university name> has been directly shared, excluding requests made through any publicly accessible directory
2. When it was shared
3. If justifications are tracked, why was it shared with that individual/organization

The requested information is in the public interest and will contribute significantly to the public's understanding of student data use. This information is not being sought for commercial purposes, but rather, for academic work.

The <relevant state law> requires a response within <n> days. If access to the records I am requesting will take longer, please contact me with information about when I might expect copies or the ability to inspect the requested records.

If you deny any or all of this request, please cite each specific exemption you feel justifies the refusal to release the information and notify me of the appeal procedures available to me under the law.

Thank you for your help with my request!

Sincerely,
[redacted]

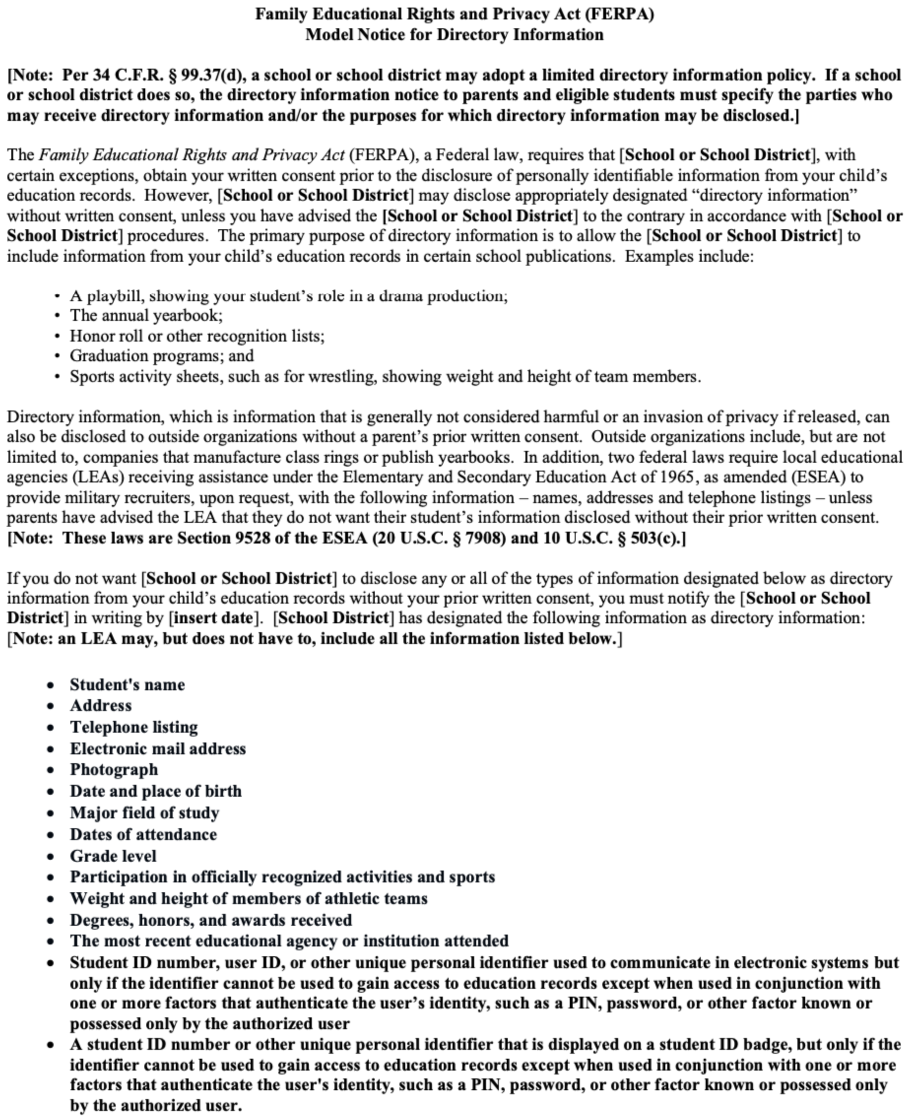
Figure 10: Email template we sent to each of the public universities who accepted FOIA requests by email.

Data Types	Do Not Share With Third Parties For Indirect Use	Do Not Share With Third Parties For Direct Use	Do Not Share For Institutional Use
Name	□	□	□
Course	□	□	□
Email Address	□	□	□
Campus Address	□	□	□
Campus Phone Number	□	□	□
Year and Registration Type	□	□	□
Phone Number	□	□	□
Term Address	□	□	□
Permanent Home Address	□	□	□
Degree Received	□	□	□
Date of Birth	□	□	□
Dates of Attendance	□	□	□

Table 14: Third Parties Opt-Out

Data Types	Do Not Share With Third Parties For Direct Use	Do Not Share For Institutional Use
Name	□	□
Course	□	□
Email Address	□	□
Campus Address	□	□
Campus Phone Number	□	□
Year and Registration Type	□	□
Phone Number	□	□
Term Address	□	□
Permanent Home Address	□	□
Degree Received	□	□
Date of Birth	□	□
Dates of Attendance	□	□

Table 15: Third Parties For Direct Use Opt-Out



Family Educational Rights and Privacy Act (FERPA)
Model Notice for Directory Information

[Note: Per 34 C.F.R. § 99.37(d), a school or school district may adopt a limited directory information policy. If a school or school district does so, the directory information notice to parents and eligible students must specify the parties who may receive directory information and/or the purposes for which directory information may be disclosed.]

The *Family Educational Rights and Privacy Act* (FERPA), a Federal law, requires that [**School or School District**], with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, [**School or School District**] may disclose appropriately designated "directory information" without written consent, unless you have advised the **[School or School District**] to the contrary in accordance with [**School or School District**] procedures. The primary purpose of directory information is to allow the [**School or School District**] to include information from your child's education records in certain school publications. Examples include:

- A playbill, showing your student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and
- Sports activity sheets, such as for wrestling, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965, as amended (ESEA) to provide military recruiters, upon request, with the following information – names, addresses and telephone listings – unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent. **[Note: These laws are Section 9528 of the ESEA (20 U.S.C. § 7908) and 10 U.S.C. § 503(c).]**

If you do not want [**School or School District**] to disclose any or all of the types of information designated below as directory information from your child's education records without your prior written consent, you must notify the [**School or School District**] in writing by [**insert date**]. [**School District**] has designated the following information as directory information: [**Note: an LEA may, but does not have to, include all the information listed below.**]

- **Student's name**
- **Address**
- **Telephone listing**
- **Electronic mail address**
- **Photograph**
- **Date and place of birth**
- **Major field of study**
- **Dates of attendance**
- **Grade level**
- **Participation in officially recognized activities and sports**
- **Weight and height of members of athletic teams**
- **Degrees, honors, and awards received**
- **The most recent educational agency or institution attended**
- **Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user**
- **A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.**

Figure 11: The template FERPA student directory information notice provided by the U.S. Department of Education [51].

Data Types	Do Not Share For Institutional Use
Name	□
Course	□
Email Address	□
Campus Address	□
Campus Phone Number	□
Year and Registration Type	□
Phone Number	□
Term Address	□
Permanent Home Address	□
Degree Received	□
Date of Birth	□
Dates of Attendance	□

Table 16: Institutional Opt-Out

Data Type	INST	TP-D	TP	NS
Name	21.2%, -9.1%	21.0%, -4.9%	30.6%, -9.6%	19.7%, -1.7%
Course	9.1%, -1.5%	14.5%, -1.6%	32.3%, -4.9%	27.9%, -6.6%
Email	39.4%, -15.2%	46.8%, -16.2%	48.4%, -11.3%	45.9%, -9.8%
Campus Address	42.4%, -4.5%	45.2%, -6.5%	54.8%, -6.4%	47.5%, -8.2%
Campus Phone	31.8%, -4.5%	33.9%, -1.6%	50.0%, -1.6%	50.8%, -11.5%
Year	18.2%, -3.0%	17.7%, 1.7%	37.1%, -8.1%	21.3%, -4.9%
Term Phone	57.6%, -4.6%	53.2%, -11.3%	59.7%, -1.6%	70.5%, -4.9%
Term Address	60.6%, -12.1%	58.1%, -17.8%	62.9%, -4.8%	67.2%, -6.5%
Home Address	84.8%, -10.6%	82.3%, -21.0%	90.3%, -14.5%	91.8%, -16.4%
Degree Status	15.2%, -4.6%	16.1%, -3.2%	25.8%, 0.0%	18.0%, -4.9%
DOB	56.1%, -13.7%	50.0%, -6.5%	71.0%, -6.5%	55.7%, -3.2%
Attendance Dates	21.2%, -10.6%	27.4%, 0.0%	38.7%, -1.6%	23.0%, -3.3%

Table 17: Data Type Suppression Opt-Out Rates By Data Sharing Policy (Institutional, Third Parties-Direct Use, Third Parties, and Not Stated)

Data Type	INST	TP-D	TP	NS
Confirm Degree	N/A	21.3%, -3.3%	17.5%, -1.6%	24.6%, -1.6%
Commencement	9.8%, 0.0%	14.8%, 3.2%	20.6%, -6.3%	18.0%, 1.7%
Attendance Dates	47.5%, -3.2%	41.0%, -3.3%	39.7%, -11.1%	41.0%, 0.0%
DOB & Address	N/A	77.0%, 1.7%	93.7%, -4.8%	90.2%, -9.9%
Honors	N/A	24.6%, -6.6%	23.8%, -1.6%	19.7%, -1.7%
Public Dir	34.4%, -4.9%	39.3%, -8.2%	46.0%, -4.7%	45.9%, -8.2%
Uni Dir	83.6%, -9.8%	80.3%, -11.4%	87.3%, -4.8%	90.2%, -9.9%
School	N/A	18.0%, 6.6%	25.4%, -4.8%	24.6%, 6.5%

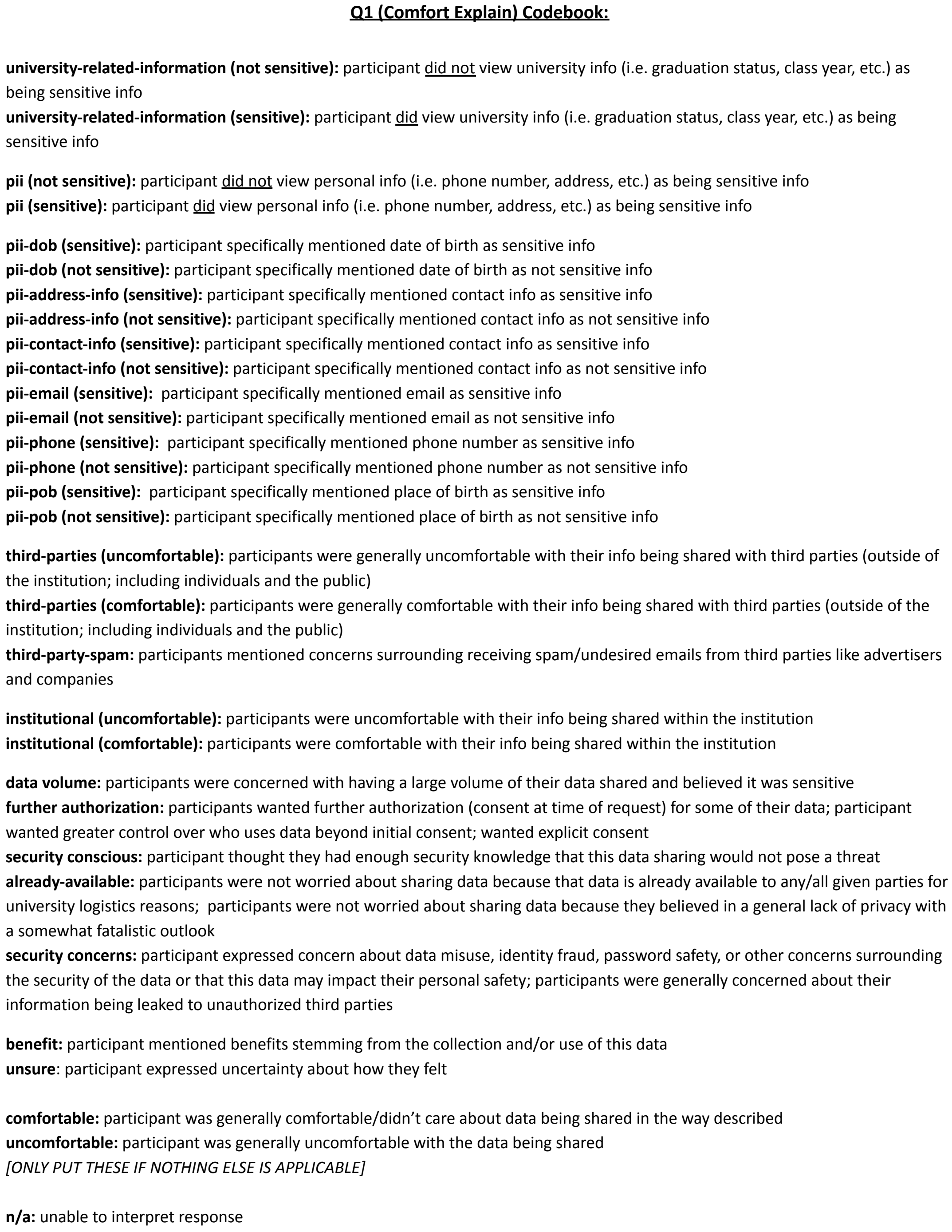
Table 18: Scenario Based Access Control: Opt-Out Rates By Data Sharing Policy (Institutional, Third Parties-Direct Use, Third Parties, and Not Stated)

Data Type	INST	TP-D-I	TP-D-D	TP-I	TP-D	TP-A
Name	11.3%, -3.2%	19.7%, -6.6%	55.7%, -9.8%	8.2%, -4.9%	42.62%, -9.8%	52.46%, -14.8%
Course	11.3%, 1.6%	14.8%, -1.7%	59.0%, 0.0%	4.92%, -1.6%	45.9%, 1.6%	54.1%, -3.3%
Email	17.7%, 0.0%	19.7%, -3.3%	62.3%, -3.3%	8.2%, 1.6%	55.74%, -13.1%	65.57%, -14.7%
Campus Address	35.5%, -3.2%	31.1%, -6.5%	72.1%, -4.9%	4.92%, 0.0%	60.66%, -11.5%	62.3%, -6.6%
Campus Phone	21.0%, -4.9%	34.4%, -13.1%	70.5%, -1.6%	8.2%, -3.3%	63.93%, -11.5%	67.21%, -13.1%
Year	17.7%, -4.8%	16.4%, -8.2%	59.0%, -6.5%	6.56%, 0.0%	62.3%, -18.0%	63.93%, -11.5%
Term Phone	40.3%, -4.8%	36.1%, -13.1%	77.0%, 0.0%	13.11%, -4.9%	70.49%, -8.2%	73.77%, -13.1%
Term Address	46.8%, -1.6%	41.0%, -16.4%	80.3%, -3.3%	13.11%, -1.6%	65.57%, -4.9%	70.49%, -4.9%
Home Address	74.2%, -1.6%	47.5%, -18.0%	91.8%, -3.3%	31.15%, -3.3%	81.97%, -16.4%	86.89%, -9.8%
Degree Status	12.9%, -3.2%	18.0%, -8.2%	49.2%, 3.3%	8.2%, -3.3%	44.26%, -4.9%	55.74%, -11.5%
DOB	38.7%, -4.8%	39.3%, -9.8%	73.8%, 1.6%	14.75%, 1.6%	59.02%, -6.6%	70.49%, -13.1%
Attendance Dates	19.4%, -4.9%	21.3%, -6.5%	54.1%, 0.0%	11.48%, -3.3%	55.74%, -13.1%	59.02%, -9.8%

Table 19: Role Based Access Control Opt-Out Rates By Data Sharing Policy & Type: Institutional, Third Parties Direct Use - Institutional Sharing, Third Parties Direct Use - Direct Use Sharing, Third Parties - Institutional Sharing, Third Parties - Direct Use Sharing, Third Parties - All Parties Sharing

Data Type	NS-I	NS-D	NS-A
Name	13.11%, -1.6%	49.18%, -9.8%	67.21%, -4.9%
Course	13.11%, -4.9%	45.9%, -4.9%	60.66%, 0.0%
Email	11.48%, 1.6%	55.74%, -4.9%	63.93%, 3.3%
Campus Address	19.67%, -4.9%	65.57%, -9.8%	73.77%, -6.6%
Campus Phone	18.03%, -4.9%	67.21%, -9.8%	75.41%, -9.8%
Year	14.75%, -4.9%	50.82%, -8.2%	59.02%, -1.6%
Term Phone	26.23%, -9.8%	73.77%, -11.5%	80.33%, -6.6%
Term Address	26.23%, -8.2%	75.41%, -8.2%	81.97%, -6.6%
Home Address	44.26%, -13.1%	83.61%, -13.1%	90.16%, -8.2%
Degree Status	13.11%, -3.3%	40.98%, -4.9%	55.74%, -3.3%
DOB	29.51%, -9.8%	60.66%, -6.6%	77.05%, -4.9%
Attendance Dates	13.11%, 0.0%	49.18%, -6.6%	63.93%, -6.5%

Table 20: Role Based Access Control Opt-Out Rates By Data Sharing Policy & Type: Not Stated - Institutional Sharing, Not Stated - Direct Use Sharing, and Not Stated - All Parties Sharing



Q1 (Comfort Explain) Codebook:

university-related-information (not sensitive): participant did not view university info (i.e. graduation status, class year, etc.) as being sensitive info
university-related-information (sensitive): participant did view university info (i.e. graduation status, class year, etc.) as being sensitive info

pii (not sensitive): participant did not view personal info (i.e. phone number, address, etc.) as being sensitive info
pii (sensitive): participant did view personal info (i.e. phone number, address, etc.) as being sensitive info

pii-dob (sensitive): participant specifically mentioned date of birth as sensitive info
pii-dob (not sensitive): participant specifically mentioned date of birth as not sensitive info
pii-address-info (sensitive): participant specifically mentioned contact info as sensitive info
pii-address-info (not sensitive): participant specifically mentioned contact info as not sensitive info
pii-contact-info (sensitive): participant specifically mentioned contact info as sensitive info
pii-contact-info (not sensitive): participant specifically mentioned contact info as not sensitive info
pii-email (sensitive): participant specifically mentioned email as sensitive info
pii-email (not sensitive): participant specifically mentioned email as not sensitive info
pii-phone (sensitive): participant specifically mentioned phone number as sensitive info
pii-phone (not sensitive): participant specifically mentioned phone number as not sensitive info
pii-pob (sensitive): participant specifically mentioned place of birth as sensitive info
pii-pob (not sensitive): participant specifically mentioned place of birth as not sensitive info

third-parties (uncomfortable): participants were generally uncomfortable with their info being shared with third parties (outside of the institution; including individuals and the public)
third-parties (comfortable): participants were generally comfortable with their info being shared with third parties (outside of the institution; including individuals and the public)
third-party-spam: participants mentioned concerns surrounding receiving spam/undesired emails from third parties like advertisers and companies

institutional (uncomfortable): participants were uncomfortable with their info being shared within the institution
institutional (comfortable): participants were comfortable with their info being shared within the institution

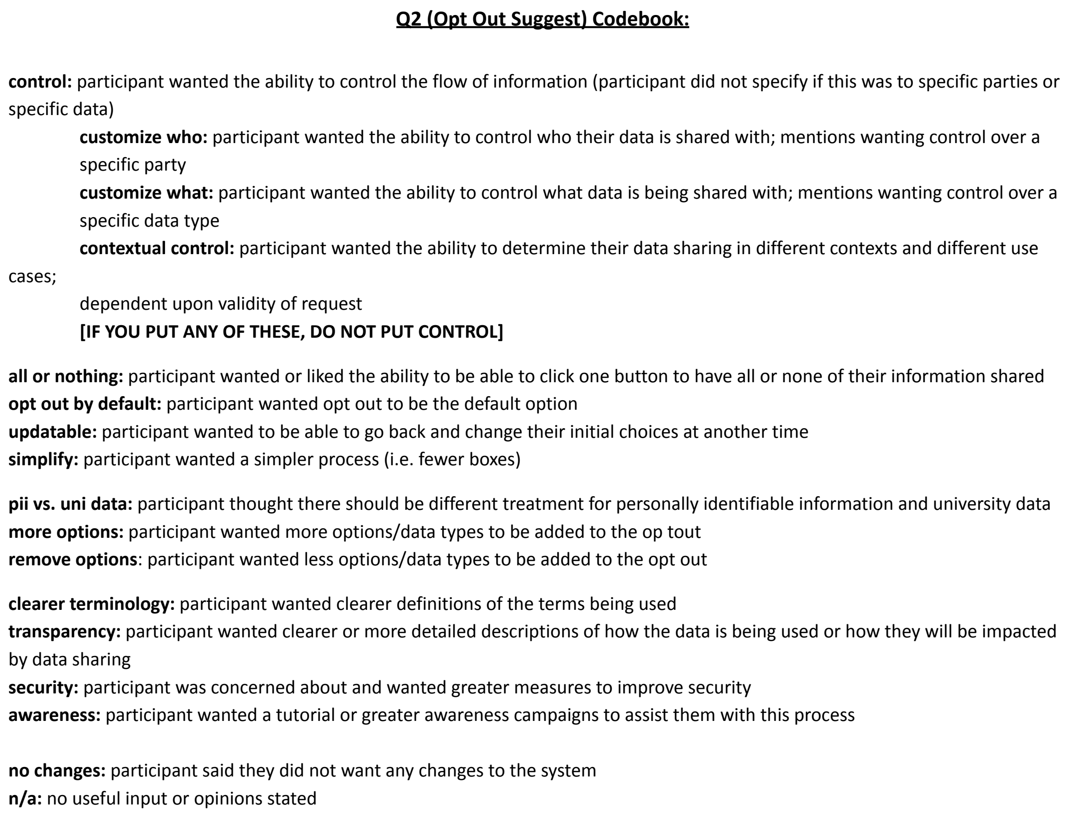
data volume: participants were concerned with having a large volume of their data shared and believed it was sensitive
further authorization: participants wanted further authorization (consent at time of request) for some of their data; participant wanted greater control over who uses data beyond initial consent; wanted explicit consent
security conscious: participant thought they had enough security knowledge that this data sharing would not pose a threat
already-available: participants were not worried about sharing data because that data is already available to any/all given parties for university logistics reasons; participants were not worried about sharing data because they believed in a general lack of privacy with a somewhat fatalistic outlook
security concerns: participant expressed concern about data misuse, identity fraud, password safety, or other concerns surrounding the security of the data or that this data may impact their personal safety; participants were generally concerned about their information being leaked to unauthorized third parties

benefit: participant mentioned benefits stemming from the collection and/or use of this data
unsure: participant expressed uncertainty about how they felt

comfortable: participant was generally comfortable/didn't care about data being shared in the way described
uncomfortable: participant was generally uncomfortable with the data being shared
[ONLY PUT THESE IF NOTHING ELSE IS APPLICABLE]

n/a: unable to interpret response

Figure 12: Codebook Page 1



Q2 (Opt Out Suggest) Codebook:

control: participant wanted the ability to control the flow of information (participant did not specify if this was to specific parties or specific data)

- **customize who:** participant wanted the ability to control who their data is shared with; mentions wanting control over a specific party
- **customize what:** participant wanted the ability to control what data is being shared with; mentions wanting control over a specific data type
- **contextual control:** participant wanted the ability to determine their data sharing in different contexts and different use

cases;

dependent upon validity of request

[IF YOU PUT ANY OF THESE, DO NOT PUT CONTROL]

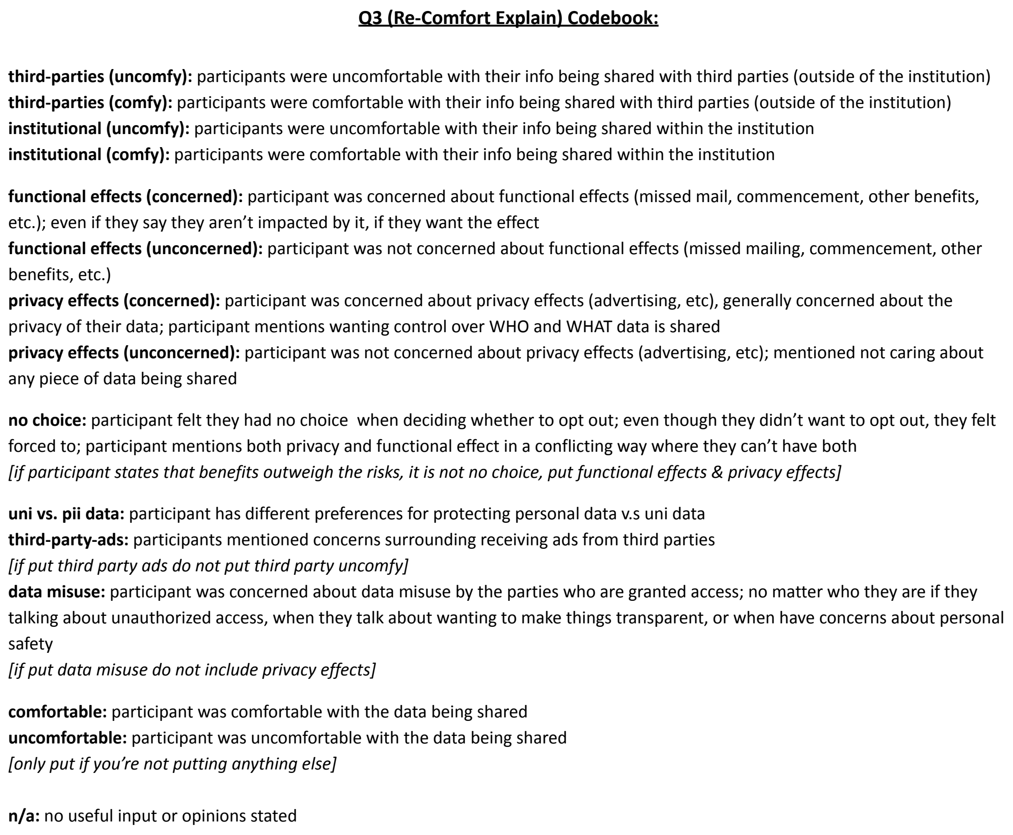
all or nothing: participant wanted or liked the ability to be able to click one button to have all or none of their information shared
opt out by default: participant wanted opt out to be the default option
updatable: participant wanted to be able to go back and change their initial choices at another time
simplify: participant wanted a simpler process (i.e. fewer boxes)

pii vs. uni data: participant thought there should be different treatment for personally identifiable information and university data
more options: participant wanted more options/data types to be added to the op tout
remove options: participant wanted less options/data types to be added to the opt out

clearer terminology: participant wanted clearer definitions of the terms being used
transparency: participant wanted clearer or more detailed descriptions of how the data is being used or how they will be impacted by data sharing
security: participant was concerned about and wanted greater measures to improve security
awareness: participant wanted a tutorial or greater awareness campaigns to assist them with this process

no changes: participant said they did not want any changes to the system
n/a: no useful input or opinions stated

Figure 13: Codebook Page 2



Q3 (Re-Comfort Explain) Codebook:

third-parties (uncomfy): participants were uncomfortable with their info being shared with third parties (outside of the institution)
third-parties (comfy): participants were comfortable with their info being shared with third parties (outside of the institution)
institutional (uncomfy): participants were uncomfortable with their info being shared within the institution
institutional (comfy): participants were comfortable with their info being shared within the institution

functional effects (concerned): participant was concerned about functional effects (missed mail, commencement, other benefits, etc.); even if they say they aren't impacted by it, if they want the effect
functional effects (unconcerned): participant was not concerned about functional effects (missed mailing, commencement, other benefits, etc.)
privacy effects (concerned): participant was concerned about privacy effects (advertising, etc), generally concerned about the privacy of their data; participant mentions wanting control over WHO and WHAT data is shared
privacy effects (unconcerned): participant was not concerned about privacy effects (advertising, etc); mentioned not caring about any piece of data being shared

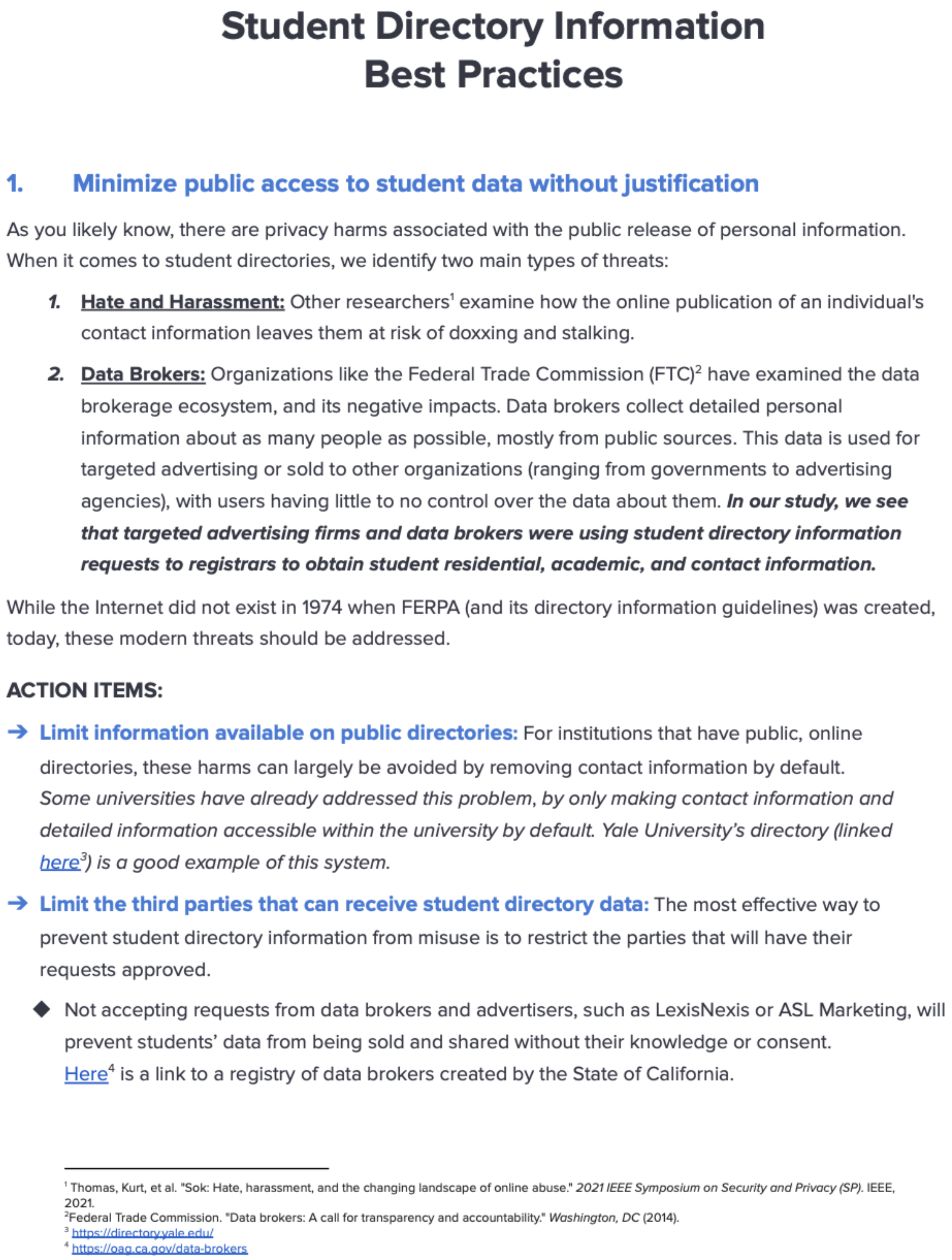
no choice: participant felt they had no choice when deciding whether to opt out; even though they didn't want to opt out, they felt forced to; participant mentions both privacy and functional effect in a conflicting way where they can't have both
[if participant states that benefits outweigh the risks, it is not no choice, put functional effects & privacy effects]

uni vs. pii data: participant has different preferences for protecting personal data v.s uni data
third-party-ads: participants mentioned concerns surrounding receiving ads from third parties
[if put third party ads do not put third party uncomfy]
data misuse: participant was concerned about data misuse by the parties who are granted access; no matter who they are if they talking about unauthorized access, when they talk about wanting to make things transparent, or when have concerns about personal safety
[if put data misuse do not include privacy effects]

comfortable: participant was comfortable with the data being shared
uncomfortable: participant was uncomfortable with the data being shared
[only put if you're not putting anything else]

n/a: no useful input or opinions stated

Figure 14: Codebook Page 3



Student Directory Information Best Practices

1. Minimize public access to student data without justification

As you likely know, there are privacy harms associated with the public release of personal information. When it comes to student directories, we identify two main types of threats:

1. **Hate and Harassment:** Other researchers[1] examine how the online publication of an individual's contact information leaves them at risk of doxxing and stalking.
2. **Data Brokers:** Organizations like the Federal Trade Commission (FTC)[2] have examined the data brokerage ecosystem, and its negative impacts. Data brokers collect detailed personal information about as many people as possible, mostly from public sources. This data is used for targeted advertising or sold to other organizations (ranging from governments to advertising agencies), with users having little to no control over the data about them. ***In our study, we see that targeted advertising firms and data brokers were using student directory information requests to registrars to obtain student residential, academic, and contact information.***

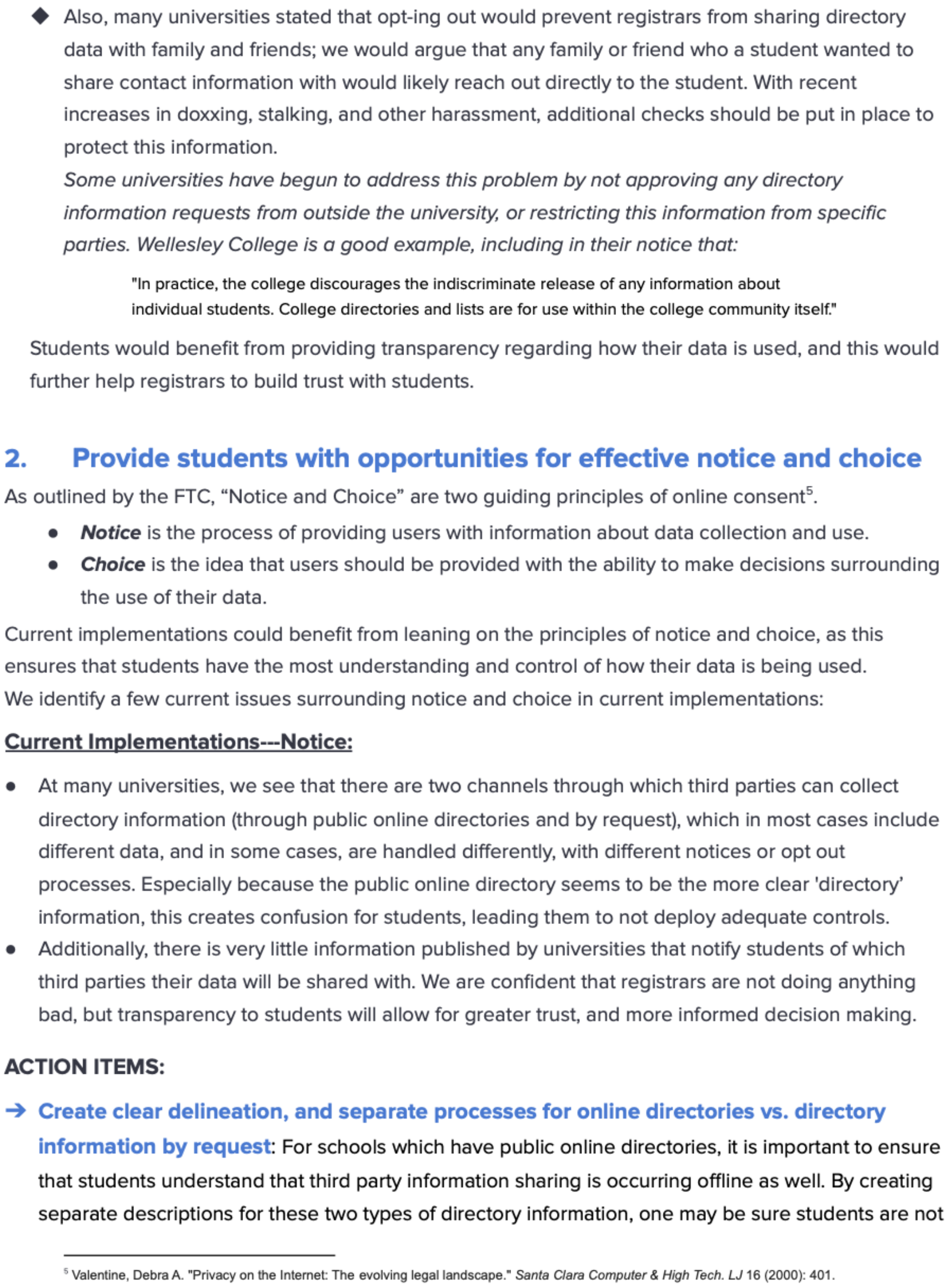
While the Internet did not exist in 1974 when FERPA (and its directory information guidelines) was created, today, these modern threats should be addressed.

ACTION ITEMS:

- **Limit information available on public directories:** For institutions that have public, online directories, these harms can largely be avoided by removing contact information by default. *Some universities have already addressed this problem, by only making contact information and detailed information accessible within the university by default. Yale University's directory (linked here[3]) is a good example of this system.*
- **Limit the third parties that can receive student directory data:** The most effective way to prevent student directory information from misuse is to restrict the parties that will have their requests approved.
    - Not accepting requests from data brokers and advertisers, such as LexisNexis or ASL Marketing, will prevent students' data from being sold and shared without their knowledge or consent. Here[4] is a link to a registry of data brokers created by the State of California.

[1] Thomas, Kurt, et al. "Sok: Hate, harassment, and the changing landscape of online abuse." *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021.
[2] Federal Trade Commission. "Data brokers: A call for transparency and accountability." *Washington, DC* (2014).
[3] https://directory.yale.edu/
[4] https://oag.ca.gov/data-brokers

Figure 15: Registrar Message Page 1



- Also, many universities stated that opt-ing out would prevent registrars from sharing directory data with family and friends; we would argue that any family or friend who a student wanted to share contact information with would likely reach out directly to the student. With recent increases in doxxing, stalking, and other harassment, additional checks should be put in place to protect this information.
  Some universities have begun to address this problem by not approving any directory information requests from outside the university, or restricting this information from specific parties. Wellesley College is a good example, including in their notice that:

  > "In practice, the college discourages the indiscriminate release of any information about individual students. College directories and lists are for use within the college community itself."

Students would benefit from providing transparency regarding how their data is used, and this would further help registrars to build trust with students.

2. Provide students with opportunities for effective notice and choice

As outlined by the FTC, "Notice and Choice" are two guiding principles of online consent[5].

- ***Notice*** is the process of providing users with information about data collection and use.
- ***Choice*** is the idea that users should be provided with the ability to make decisions surrounding the use of their data.

Current implementations could benefit from leaning on the principles of notice and choice, as this ensures that students have the most understanding and control of how their data is being used.
We identify a few current issues surrounding notice and choice in current implementations:

Current Implementations---Notice:

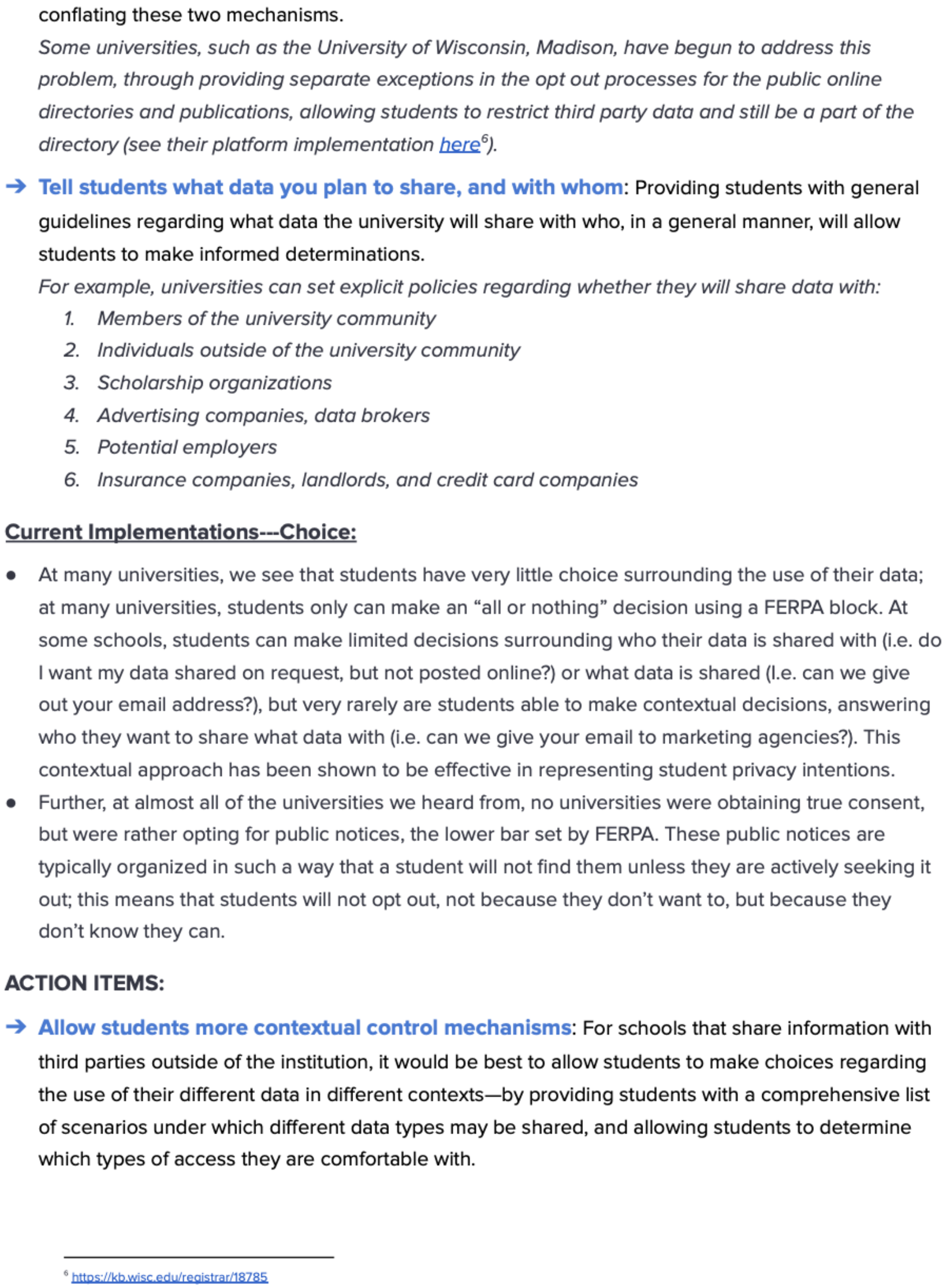
- At many universities, we see that there are two channels through which third parties can collect directory information (through public online directories and by request), which in most cases include different data, and in some cases, are handled differently, with different notices or opt out processes. Especially because the public online directory seems to be the more clear 'directory' information, this creates confusion for students, leading them to not deploy adequate controls.
- Additionally, there is very little information published by universities that notify students of which third parties their data will be shared with. We are confident that registrars are not doing anything bad, but transparency to students will allow for greater trust, and more informed decision making.

ACTION ITEMS:

➔ **Create clear delineation, and separate processes for online directories vs. directory information by request**: For schools which have public online directories, it is important to ensure that students understand that third party information sharing is occurring offline as well. By creating separate descriptions for these two types of directory information, one may be sure students are not

[5] Valentine, Debra A. "Privacy on the Internet: The evolving legal landscape." *Santa Clara Computer & High Tech. LJ* 16 (2000): 401.

Figure 16: Registrar Message Page 2



conflating these two mechanisms.

Some universities, such as the University of Wisconsin, Madison, have begun to address this problem, through providing separate exceptions in the opt out processes for the public online directories and publications, allowing students to restrict third party data and still be a part of the directory (see their platform implementation here[6]).

➔ **Tell students what data you plan to share, and with whom**: Providing students with general guidelines regarding what data the university will share with who, in a general manner, will allow students to make informed determinations.

For example, universities can set explicit policies regarding whether they will share data with:

1. *Members of the university community*
2. *Individuals outside of the university community*
3. *Scholarship organizations*
4. *Advertising companies, data brokers*
5. *Potential employers*
6. *Insurance companies, landlords, and credit card companies*

Current Implementations---Choice:

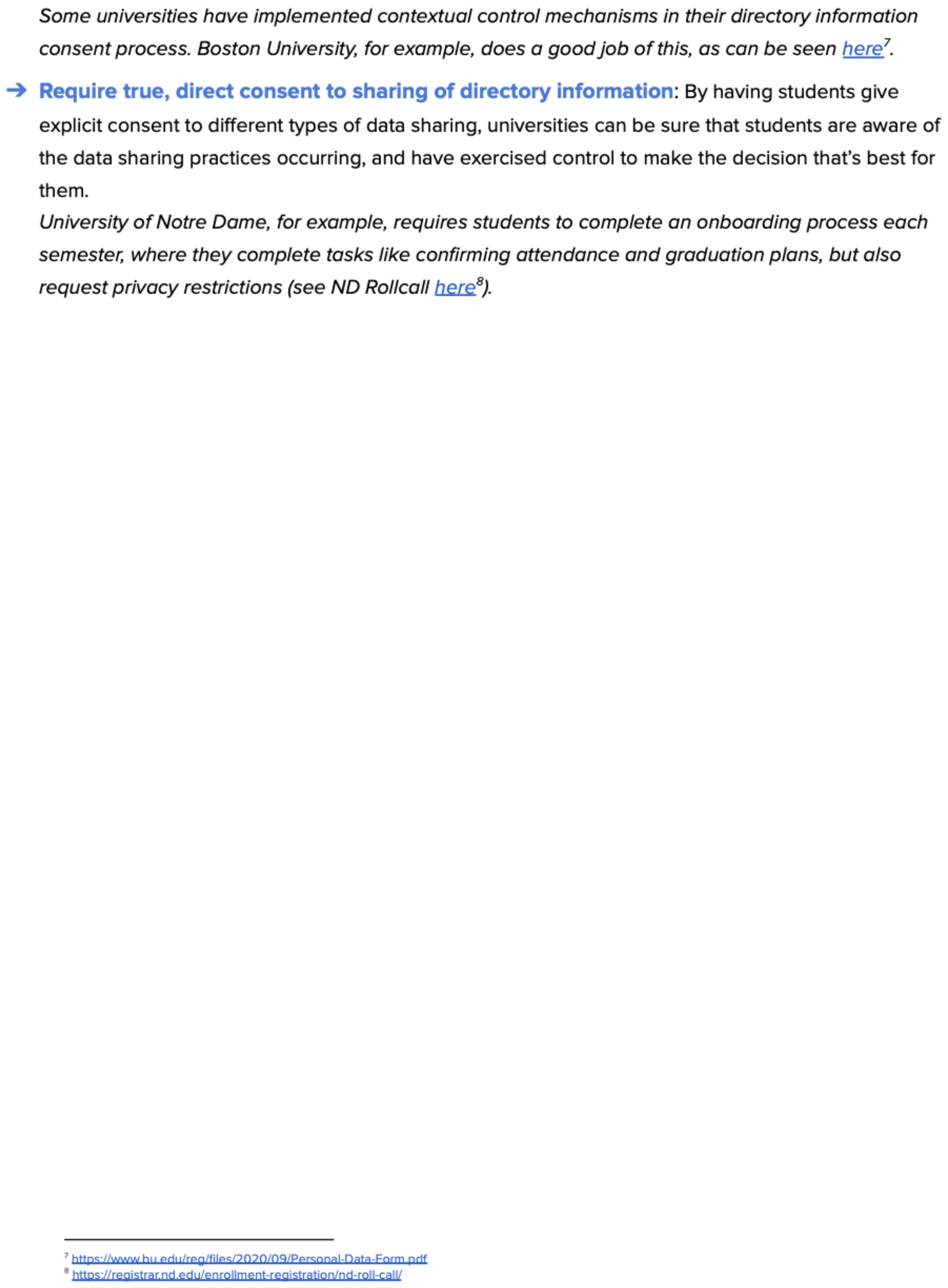
- At many universities, we see that students have very little choice surrounding the use of their data; at many universities, students only can make an "all or nothing" decision using a FERPA block. At some schools, students can make limited decisions surrounding who their data is shared with (i.e. do I want my data shared on request, but not posted online?) or what data is shared (I.e. can we give out your email address?), but very rarely are students able to make contextual decisions, answering who they want to share what data with (i.e. can we give your email to marketing agencies?). This contextual approach has been shown to be effective in representing student privacy intentions.
- Further, at almost all of the universities we heard from, no universities were obtaining true consent, but were rather opting for public notices, the lower bar set by FERPA. These public notices are typically organized in such a way that a student will not find them unless they are actively seeking it out; this means that students will not opt out, not because they don't want to, but because they don't know they can.

ACTION ITEMS:

➔ **Allow students more contextual control mechanisms**: For schools that share information with third parties outside of the institution, it would be best to allow students to make choices regarding the use of their different data in different contexts—by providing students with a comprehensive list of scenarios under which different data types may be shared, and allowing students to determine which types of access they are comfortable with.

[6] https://kb.wisc.edu/registrar/18785

Figure 17: Registrar Message Page 3



Some universities have implemented contextual control mechanisms in their directory information consent process. Boston University, for example, does a good job of this, as can be seen here[7].

➔ **Require true, direct consent to sharing of directory information**: By having students give explicit consent to different types of data sharing, universities can be sure that students are aware of the data sharing practices occurring, and have exercised control to make the decision that's best for them.
University of Notre Dame, for example, requires students to complete an onboarding process each semester, where they complete tasks like confirming attendance and graduation plans, but also request privacy restrictions (see ND Rollcall here[8]).

[7] https://www.bu.edu/reg/files/2020/09/Personal-Data-Form.pdf
[8] https://registrar.nd.edu/enrollment-registration/nd-roll-call/

Figure 18: Registrar Message Page 4