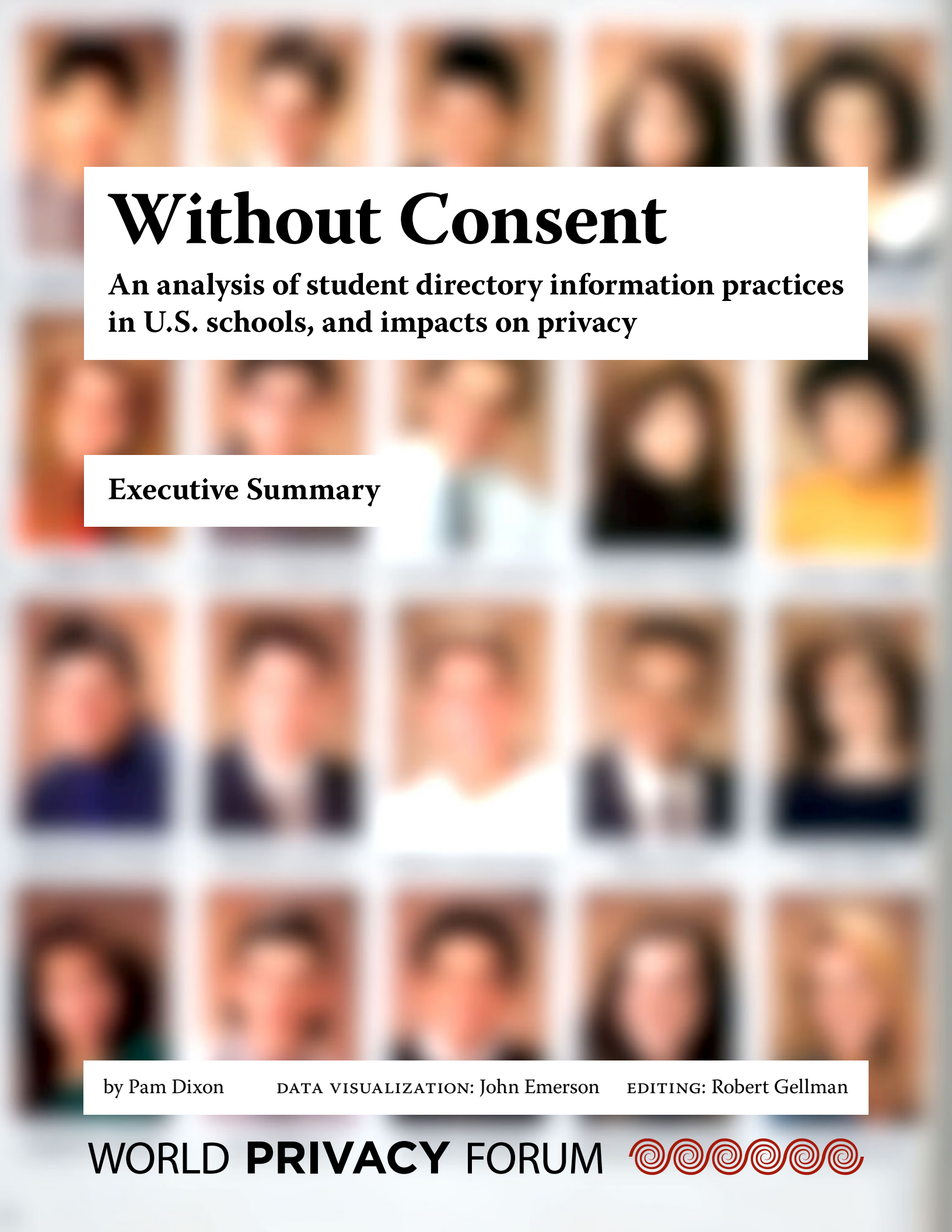

Without Consent

An analysis of student directory information practices in U.S. schools, and impacts on privacy

Executive Summary

by Pam Dixon DATA VISUALIZATION: John Emerson EDITING: Robert Gellman

WORLD PRIVACY FORUM

Without Consent:
An analysis of student directory information practices in U.S. schools,
and impacts on privacy

World Privacy Forum
www.worldprivacyforum.org

Cover and design by John Emerson

EBook/Digital: ISBN: 978-0-9914500-1-5
Publication Date: April 2020

Brief Summary of Report

If data is the new oil, then student data is among the most desirable data wells of all. While some states have enacted laws to better protect students and their privacy, policymakers have left a formidable front door open: that is, the ability for detailed student information to be made public by schools under an exemption in the federal student privacy law, the Family Educational Rights and Privacy Act.

This exemption is called the *Directory Information* exemption. When schools choose to, they can designate certain student information of their choice to be made public without prior consent. This information becomes *directory information*. To provide a balance, Congress provided a right that students and parents can restrict unconsented public disclosure of their directory information. Eligible students can place this restriction on their *directory information* by submitting an opt out request at the school. Parents or guardians of students under 18 will have to place the restriction for the student. This right to restrict disclosure is an essential one, but students, parents and others may not be aware of the importance and profound privacy impact of this information.

Directory information at schools is not like information in a phone book; it can be much more extensive. Information such as legal name, exact date and place of birth, home address, photographs, gender, social media handles, parent or guardian home address, and primary language spoken are among the many categories of directory information that schools could — and do — choose to release. In our modern world this kind of information can and does create safety, privacy, and other risks for students, particularly those who are victims of crime or have other vulnerabilities, including economic vulnerabilities.

The default privacy setting of students' directory information under FERPA is set to allow schools to "publish without prior consent." In theory, the right to opt out should provide privacy checks and balances. But this report finds that many schools, while technically compliant, have not done enough to encourage students and parents to effectuate their FERPA opt out rights. In some cases, notices of FERPA opt out rights are not prominently posted on school web sites. In others, the very notices that students need for learning about how to activate their opt out rights are the same notices that may nudge them to do the opposite by using discouraging language that facilitates inaction or makes opting out of directory information sharing look like an unattractive option.

The research for this report examined directory information practices and related issues in a multi-year study across more than 5,000 schools at the primary, secondary, and postsecondary levels. The research found troubling and challenging student privacy problems that need to be urgently addressed. The report includes detailed findings and recommendations based on the research. In brief, the research found:

- It is completely possible for schools to meet the FERPA minimum standards for FERPA notice and at the same time make FERPA opt out difficult or undesirable for students and parents.
- FERPA directory information notice and opt out is not being consistently implemented in modern, updated ways at schools.
    - Not all schools post FERPA opt out forms for students online. For example, 39 percent of studied primary and secondary schools make FERPA opt out forms online and available to the public.
    - Some schools require students to write a letter to opt out.
    - Some schools give a year for students to opt out; some schools give 10 days.
- The information designated as *directory information* by many schools can, in our modern world, be invasive of privacy and cause harm. Exact date of birth, home address, gender, and

photographs of students released as public information is no longer acceptable and poses demonstrable risk to students.

- Few schools have developed a culture of fostering and promoting students' rights under FERPA to opt out of directory information sharing.
- WPF research documented a troubling pattern of the brokering of information of minors online.
    - In one case, a company registered as a data broker acquired student *directory information*.
    - A facial recognition company disclosed it has been brokering the information of minors by collecting the publicly available images of minors for use in its facial recognition product.
    - Among data brokers that stated that they had actual knowledge that they possess the brokered personal information of minors, two companies said they used the information of minors to create predictive scores regarding their parents for commercial purposes.
- Language that schools use to communicate with students and parents about FERPA opt out rights is not always encouraging of pro-privacy choices, and may contain negative nudges that discourage parents and eligible students from opting out.

WPF research found best practice exemplars of modern FERPA implementations at all levels. These best practices have the hallmarks of modern privacy thought, which is a focus on implementing FERPA in a way that creates transparency, accountability, fairness, equality of opportunity to opt out, and an environment that supports student privacy, safety and student thriving for all students and parents.

There is much that can and must be done to improve student privacy outcomes. Some solutions are simple, such as updated guidance requiring schools to post annual FERPA notices, and ideally, opt out forms, on school websites. Some solutions require legislative and regulatory attention, such as ensuring students' *directory information* does not get passed to data brokers. Ensuring students' photographs or digital images are not available on school websites to be scraped for use in test databases for biometric or other systems also requires attention. And ensuring that all students, from all walks of life, including those who are homeless or living in poverty, have the ability to learn about their privacy rights and take advantage of those rights is of utmost importance.

The days of schools designating and releasing broad swaths of *directory information* publicly as a "default setting" of FERPA privacy rights needs to be behind us. Advances in modern privacy thought and laws demonstrate that *directory information* is no longer just a dusty right consigned to dense legal notices few understand the full significance of. The COVID-19 pandemic that has so deeply impacted all schools, parents, and students shows the urgent need to ensure that FERPA notices and opt outs are online, available all year, and can utilized without resorting to paper handouts or in-person office visits. The U.S. Department of Education, states, local school boards, and local schools need to do much more to update their approach to how *directory information* is handled at every level. The current default settings for directory information under FERPA need to be re-examined and the procedures need to be re-evaluated and refitted to a more modern understanding of data privacy. The safety and privacy and thriving of all students depends on it.

Key Recommendations

We can and must do more to protect the information of students, and minors. FERPA-covered educational institutions and agencies have an important role in taking affirmative and decisive steps to protect students and minors. Some specific recommendations regarding directory information include:

- Educational institutions covered under FERPA must provide a prominent, publicly accessible FERPA notice online *and* a FERPA opt out form online at a minimum. This information should be

made available online on an ongoing basis all year. Ideally, this notice will be viewable on multiple types of devices, including mobile phones. Ideally, FERPA opt outs can be viewed, filled out, and submitted via online and mobile means.

- The Department of Education, State educational agencies, local school boards, and educational institutions need to review and revise FERPA notice and opt out methods for accessibility and inclusiveness and for all students and parents, across delivery methods from online to offline, inclusive of mobile, audio, and multiple forms (and languages) of notice.
- Educational institutions covered under FERPA must allow for student opt out on an ongoing basis and not just in the beginning of the school year or upon enrollment.
- Educational institutions must stop brokering student directory information to data brokers, or allowing passive collection of student directory information by data brokers.
- Educational institutions should adopt a **minimum necessary rule** when deciding which kinds of data to designate as FERPA directory information.
- All FERPA-covered institutions should conduct a **safety and privacy review** prior to designating categories of information as directory information.
- There should be an express prohibition on the use of photographs of minors released by schools without prior consent under the directory information exemption for training face recognition or biometric systems. This includes yearbooks made using facial recognition. Schools should require yearbook companies using facial recognition in their process to never sell or share that information, and should require specific consent for the use of facial recognition.
- Schools using "platforms" or student information systems, must provide publicly available FERPA annual notices, opt outs, and other information outside of those systems in a way that is accessible to members of the public, including via online access.

Report Acknowledgements

With thanks to the research team at WPF who contributed significant amounts of time over the course of four years to the detailed and extensive research and fact-checking that went into this report.

Thanks to Jack Bolen, WPF Research Fellow, who assisted with research, fact checking and also aspects of integrated student information systems.

Thanks to the legal, educational, technical, and policy experts who contributed their time and knowledge to this report. Among them, particular thanks to Robert Gellman, Professor Jane K. Winn, Timothy Sparapani, and Professor Joel Reidenberg.

We want to further acknowledge Fordham University School of Law Professor Joel Reidenberg for his decades-long work on student privacy. His work, and those of his colleagues at Fordham CLIP, have created greater transparency in challenging areas of research. Their work created a path that facilitated the research conducted for this report.

We thank the state of Vermont for leading the nation in passing a data broker registry law that requires disclosure of the brokering of the data of minors. Without this law, and without the specific provisions that makes brokering the data of minors more transparent, WPF would not have learned about significant data broker activities regarding student directory information and the data of minors.

This work was supported by a grant from the Kaplan Foundation and an individual grant from S. Kaplan. We thank them for their support of this project.

About the World Privacy Forum

The World Privacy Forum[1] is a non-profit public interest research and consumer education group focused on the research and analysis of privacy-related issues and consumer education. The Forum was founded in 2003 and has published significant, groundbreaking privacy research and policy studies, including major multi-year research studies. Among these include *Medical Identity Theft: The information crime that can kill you*, the first public report on medical identity theft, *The Scoring of America*, the first major report regarding predictive analytics and privacy, and *A Failure to Do No Harm, India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, a multiyear peer-reviewed report regarding large scale identity and biometric systems, published in Springer-Nature and co-published at the Harvard-based Technology Journal. Each of these reports has had significant, demonstrable, and positive real-world impacts on consumer privacy.

WPF engaged substantively in the 2008 and 2011 FERPA rulemakings and the 2015 Department of Education's *Dear Colleague* letter[2] on student health privacy at institutions of higher education. WPF maintains educational material about student privacy, the Family Educational Rights and Privacy Act, and material about the intersection between health privacy law and student privacy law See: *A Patient's Guide to HIPAA*, the *Student Privacy 101* series, and additional materials at www.worldprivacyforum.org.

1 World Privacy Forum's home page includes information about our activities, as well as numerous privacy research, data visualizations, and data privacy resources. Available at: https://www.worldprivacyforum.org.

2 *World Privacy Forum Letter to DOE regarding Dear Colleague Letter about student health privacy*, October 1, 2015. Available at: http://www.worldprivacyforum.org/wp-content/uploads/2015/10/WPF_comments_Edu_Medprivacy_Guidance_30Sept2015_fs.pdf. *Final, Dear Colleague Letter to School Officials at Institutions of Higher Education*, U.S. Department of Education, Aug. 24, 2016. This letter is "significant guidance" per OMB Good Guidance Practices. Letter available at: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/DCL_Medical%20Records_Final%20Signed_dated_9-2.pdf.

Methodology for this report

This report focuses on the privacy of student directory information at FERPA-covered educational institutions, and on students' ability to learn about and effectuate their FERPA rights. WPF conducted a detailed, multi-year research study on FERPA and directory information-related issues at more than 5,000 primary and secondary schools in 101 U.S. school districts. At the postsecondary level, we studied 102 postsecondary schools in the U.S. The methodologies for the selection of the schools and other aspects of this research are detailed in the appendices of this report.

This report studies implementations of FERPA in regards to student directory information, and examines key risks to student privacy relative to directory information, and what practices or changes would create improved privacy outcomes for students. Because this is not a compliance report, in reporting and discussing the results of our work we have reported our data in aggregate form without identifying schools by name. If and when we identify a specific school in the main report text by name, it is because we are using one or more practices of that school as an exemplar of a good practice.

For some of the results for primary and secondary schools, we have reported results at the district level. When we have done this, it is to understand district-level policies between urban and rural school districts, and in some cases to balance the statistical effects of very large urban school districts on the results in total. For example, some large urban school districts may have 1,000 or more schools. A rural district may contain 50 or fewer schools. We have listed the primary / secondary schools studied in an appendix of this report for transparency. We have not listed the roster of postsecondary institutions we studied, as we were unable to provide results for postsecondary institutions at a high enough level of aggregation to de-identify the results.

Part IV. Conclusion: Towards Creating a Culture of Privacy in FERPA- Covered Institutions

A lesson learned from other areas of data privacy is that law on the books is one thing, but law in practice can be something else entirely. Laws are only as effective as their implementation, and the best implementation should nurture a way of thinking that embodies the needs of students, even if those needs go beyond the words of a law, whether it is out of date or not.

FERPA, with its important protections for student data, is an important cornerstone of student privacy in the U.S. When implemented properly, FERPA can give students some degree of autonomy and choice over information that can affect their lives and opportunities in meaningful ways. Understanding and exercising privacy controls can also give students an education that will serve them well as they navigate privacy issues throughout their lives.

FERPA-covered schools need to develop good, thoughtful, and useful FERPA notices, policies, and opt out forms. These are essential — but these tools operate best in an environment that fosters a "culture of privacy." This means that privacy is a value that is respected and nurtured within the entire culture of educational institutions. One of the first steps toward creating a culture of privacy is to embrace privacy protection as a positive feature, not to treat it as a bug in the system.

In our modern era, students (and parents) may have many reasons for wanting or needing to utilize FERPA directory information opt out rights. Students may want their personal information such as home address or weight shielded from public eyes. Students who are victims of domestic violence may need enhanced privacy and "data safety," and restricting information may be essential for them. Parents of students who are active members of law enforcement or the judiciary may also want a FERPA opt out in place.

A culture of privacy will assist and understand the many reasons (or no particular reason) that, in our incredibly complex digital environment, people want to remove personal information from public disclosures. Modern data systems collect personal information and can use it to predict and affect how individuals are treated in the educational, vocational, economic, and other marketplaces. In some cases, this information can affect individuals for the rest of their lives.

FERPA provides local educational institutions with broad discretion to implement certain aspects of the federal privacy rules. For example, a school can limit directory information beyond that allowed by FERPA. In an ideal world, the FERPA framework has the possibility of being flexible and effective, both essential qualities. But in the absence of clear, modern guidance and vigorous leadership focused on student privacy and school privacy concerns, the broad discretion that FERPA allows can and in many cases has devolved, creating significant inconsistencies in local FERPA implementations. For parents and students who are involved with more than one school during the course of a student's academic life, the diversity in FERPA protections is an additional challenge.

The Department of Education needs to update FERPA policy to reflect the modern understanding that the release of a student's home address represents a profound safety risk for all children, but especially for vulnerable populations, including victims of crime, survivors of domestic violence, and students who are children of members of law enforcement and the judiciary. Releasing the photographs of minors publicly online without prior consent is also problematic, and this practice needs to be curtailed. These are starting points — additional items such as rewriting model notices and asking schools to post FERPA notices and opt out forms online and without requirements for registration to see these policies would be welcome updates.

FERPA policy must be proactive and smart about ensuring that data scrapers, data brokers, data profilers, and those seeking to cull the data of a new generation cannot do so unless and until parents and eligible students who are well and truly fully aware of all FERPA directory information rules and policies at their local schools choose for the information to be public. And schools, for their part, need to assertively assist parents and students in opting out of directory information sharing when so requested. Schools that make FERPA opt outs difficult for students do not support a culture of privacy.

Solutions to the problems identified in this report exist. And the solutions in many cases are inexpensive and achievable. It is not expensive to post a FERPA policy and a FERPA opt out policy on a school web site. It is not impossible to make it easy for a student or parent to exercise opt out rights by providing a FERPA opt out form and allowing for that form to be turned in throughout the academic year.

What is going to be challenging is to find the willingness and the attention needed to make the changes that can bring modern privacy protections into the educational institutions in the United States. In the past decade, there has been little discussion of the effects of educational institutions' directory information policies in the modern educational digital ecosystems. It is time to remedy that gap.

To do this, schools can begin by convening parents, students, and other stakeholders to discuss how to update privacy policies in a way that serves the needs of students and parents first and foremost. Schools can survey parents and ask what kind of opt outs are effective for them, and how much time they need to opt out. Schools can listen to the privacy concerns of students and parents who have been touched by crime or who have been made vulnerable in other ways, and can begin to craft FERPA policies at the local level that are sensitive to the real-world privacy problems that parents and students are facing. In doing so, educators can begin to fulfill their obligation to do no harm in the area of student privacy, and to create a safe place for student flourishing by modeling the dignity of treatment of others educators most want to see in their students.