WASHINGTON
LEGISLATIVE OFFICE


May 23, 2011

Regina Miles
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202

Re: **Family Educational Rights and Privacy Act (FERPA) regulatory changes, Docket ID ED-2011-OM-0002**

**AMERICAN CIVIL LIBERTIES UNION**
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
*DIRECTOR*

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500



Dear Ms. Miles

On behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, and its more than half a million members, countless additional supporters and activists, and 53 affiliates across the country, we write to express our concerns regarding the Department of Education's changes to the existing regulations implementing the Family Educational Rights and Privacy Act (FERPA). 76 Fed. Reg. 19726. FERPA was passed in 1974 to protect the privacy of American students control information sharing among primary, secondary and post secondary institutions.

This notice of proposed rulemaking (NPRM) represents a significant new privacy invasion. The rules allow much greater access to students' personal information by state officials not working directly on education and by other governmental and private entities that are not traditional education providers. They may allow for the sharing of personal information between states – paving the way for a national database of student records and substantially increasing the risk of lost records and identity theft. All of this information sharing occurs without a parent or student's consent and beyond their control. Final regulations must express more clearly a commitment to keeping personally identifiable information confidential and barring access to that information by those who might otherwise have access to the aggregated information. When it is necessary to share personal student information the reasons for that sharing and restrictions on information must be very clearly articulated. There must be no creation of a national student database.

All of the concerns in this comment are directed at the sharing of personally identifiable information about students such as identifiable records of student grades, discipline and other personal and private information. We do not oppose general collection of information about students and its use in a non-identifiable form. In fact we believe that the collection of aggregate information on students is a critical tool for civil rights enforcement and in assuring that every student receives equal access to a high quality education.

For example, school discipline and academic success are inherently linked. To better support student achievement, educators, parents, and policy makers must be able to review information on the health of a school's climate. Therefore we support collection and public reporting of information to inform policy makers and advocates about racial disparities in school discipline and other punitive measure that may work to push kids out of school, such as suspensions, expulsions, instances of corporal punishment, school-based arrests, referrals to law enforcement agencies, and referrals to disciplinary alternative schools. To allow for a greater insight, the data should be disaggregated by race, gender, special educational status, socio-economic status, and English proficiency, and cross-tabulated. However, this information should be reported in an anonymous way that allows for accountability while protecting student privacy.

## I. Background

In order to understand the privacy implications of sharing student personal information, one must recognize two core facts:

- Educational records are very detailed and sensitive and
- Increased access to records inevitably leads to increased risk of data breaches and data loss.

### *a. Sensitive Records*

Teachers and schools are intimately involved with students' lives for years. Beyond class attendance and grades they track discipline problems, report on home life and offer detailed evaluations of students. A teacher may need to know much of this information but it is difficult to justify sharing it with a wide range of state officials.

Compounding this problem is the fact that schools are also collecting unnecessary and extraneous information. According to the Fordham Center on Law and Information Policy, which reviewed the state data collection practices on K-12 students in all 50 states, data collected by particular states includes pregnancy, mental health information, criminal history, birth order, victims of peer violence, parental education, medical test results, and birth weight.[1] The study also found that information was not being handled in compliance with current law, and that there were no clear rules for accessing the information. All of this makes any increased disclosure of personally identifiable information a significant privacy problem.

### *b. Data Breach*

Expanding access to educational records is almost certain to lead to an increase in the number of lost or misused records containing personal information on students. The more individuals who access and use personally identifiable student data, the more opportunities there will be for inadvertent disclosures, loss of information from poor security practices, and misuse by individuals within the system.

This problem has already reached epidemic proportions. According to the Privacy Rights Clearinghouse, which monitors data breaches, 8,584,571 student records have been lost from 543

[1] Fordham Center on Law and Information Policy, October 2009: *A Study of Elementary and Secondary School State Reporting Systems*, Available at: http://law.fordham.edu/center-on-law-and-information-policy/14769.htm

different breaches since 2005. [2] These breaches represent a staggering loss of personal information, one that is ongoing. Consider these worrisome headlines from just the last few months:

- *Student Records Found Dumped in Trash Bins* – The personal files from Huntington Learning Center in East Northport, Long Island, were found tossed in a dumpster behind a strip mall. March 28, 2011.[3]

- *Hackers may have accessed thousands of South Carolina students' information* – In the Lancaster County School District hackers were able to hack into the district's system by monitoring district computers and capturing keystrokes to get passwords. Those passwords gave the hackers access into the records on the state system of more than 25,000 students and more than 2,500 school district employees. April 18, 2011.[4]

- *Central Ohio Technical College students' personal information left unsecured* - 600 students' personal information was left unsecured after sent to storage at Apple Tree Auction Center, where they were left unsecured for less than 24 hours. April 19, 2011.[5]

- *Pennsylvania College laptop stolen* - Albright College's financial aid office had a laptop stolen containing personal information on 10,000 current, former and prospective students, by an employee who sold the computer for to pay for drugs. April 16, 2011.[6]

- *Information on top Texas high school graduates mishandled* - The Social Security numbers of 164,406 students who graduated in the top 10 percent of their class over the past two decades were placed at risk for identity theft because they were sent unencrypted via the mail. April 7, 2011.[7]

In many of these cases, the data loss was not intentional. But the more people that access and handle information on individual students, the greater risk of a data breach.

## II. Expanded Access for State Officials

The NPRM expands non-consensual access to student records in at least four ways:

- By increasing the number of officials who can access information on individual students;
- Through inadequate controls on that access; and

---

[2] Privacy Rights Clearinghouse, *Chronology of Data Breaches: Security Breaches 2005-Present*. Available at: http://www.privacyrights.org/data-breach

[3] Day, Andrea. "Student Records Found Dumped in Trash Bins." *Fox News New York*, March 2011. Accessed May 19, 2011 at: http://www.myfoxny.com/dpp/news/student-records-found-dumped-in-trash-bins-20110328

[4] "Hackers May Have Accessed Thousands of SC Students' Information." *Channel 5 News*, April 2011. Accessed May 18, 2011 at: http://www.live5news.com/story/14468839/hackers-may-have-accessed-thousands-of-students-information

[5] Balmert, Jessie. "COTC Students' Personal Information Left Unsecured." *Newark Advocate*, April 19, 2011, Accessed May 19, 2011 at: http://www.newarkadvocate.com/article/20110419/NEWS01/104190308

[6] Henshaw, Steve. "1 Stolen Albright Laptop found; 1 still Missing." *Reading Eagle*, April 16, Accessed May 19 2011 at: http://readingeagle.com/article.aspx?id=301685

[7] Scott, Robert. "More Student SSNs Were at Risk, TEA Says." *The Texas Tribune*, April 7, 2011, Accessed May 19, 2011 at: http://www.texastribune.org/texas-education/public-education/more-student-ssns-were-at-risk-tea-says/

- By eliminating the need for express authority to conduct audits of personally identifiable student records.

*a. Access by state officials to records on individual students*

The NPRM expands the definition of "authorized representatives" to:

> any entity or individual designated by a State or local educational authority or agency headed by an official listed in § 99.31(a)(3) [Comptroller General of the US, the AG of the US, The Secretary, state and local educational officials], to conduct—with respect to Federal or State supported education programs— any audit, evaluation, or compliance or enforcement activity in connection with Federal legal requirements that relate to those programs. 76 Fed. Reg. 19728.

The practical result of this change is that state educational officials can designate any state official to access personal information on students without the student or parent's consent for an almost unlimited spectrum of activities. In fact, this is the precise intent of the language. The Department envisions:

> There is no reason why a State health and human services or labor department, for example, should be precluded from serving as the authority's authorized representative and **receiving non-consensual disclosures of PII to link education, workforce, health, family services, and other data** for the purpose of evaluating, auditing, or enforcing Federal legal requirements related to, Federal or State supported education programs 76 Fed. Reg. 19729 (emphasis added).

While the NPRM requires this access to be limited by a written agreement (discussed below), this protection will be of little comfort to students and parents. This information describes individual students and is both detailed and sensitive. Further, the information was collected for a specific purpose and using it for other purposes is contrary to the expectations of students and their parents and a violation of their privacy.

*b. Inadequate controls*

The written agreements established by the NPRM to protect personal information are necessary but insufficient. The NPRM usefully describes a number of areas that must be covered by these agreements including designating a particular representative, limiting information disclosures and retention times, and a variety of other protections. We believe additional mandatory requirements must address in more concrete turns the consequences for data breaches. Specifically, contracts should include requirements of liquidated damages, a third party beneficiary clause for data subjects (so students and parents can hold officials liable), a clearly delineated audit provision, and descriptions of notification and other responsibilities when personal information is lost. Written agreements should also be public documents, and they should specify the legal authority for any disclosures.

Even a perfect data sharing agreement would not solve the main problem at issue. This agreement will be useful in providing accountability after breaches and alerting responsible officials to their duties, but it will do little to stop inadvertent breaches or officials acting in bad faith.

*c. Eliminating the need for express authority to conduct audits*

Much of the authority necessary to access student records is based on the need to perform "audit, evaluation, or compliance or enforcement activity". Previous regulation has required that such authority must be grounded in some other federal, state or local authority. The Department has stated that "[l]ack of such explicit State or local authority has hindered the use of data in some States." 76 Fed. Reg. 19735. Therefore under this new regulatory guidance, state and local officials do not require express legal authority to conduct audits of individual student records and these other activities, but rather may "obtain PII when they have implied authority to conduct evaluation, audit, and compliance activities of their own programs." 76 Fed. Reg. 19735.

Given the amount of personally identifiable information accessible under this new regulation, such an exemption is striking. Officials will no longer have to describe their actual legal authority to conduct and audit. Instead they will simply be able to describe something as an evaluation, audit or compliance activity and gain access to significant amounts of the personal data stored in student records.

## III. Sharing personally identifiable student records with outside education groups

The NPRM also greatly increases access to personally identifiable student records for entities outside the formal K-12 and secondary education systems. Specifically, it broadens the definition of "educational program" to:

> any program that is principally engaged in the provision of education, including, but not limited to early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education and adult education, regardless of whether the program is administered by an educational authority. 76 Fed. Reg. 19729, 19730.

This definition would allow an extremely wide variety of parties to be classified as 'educational programs' and give those same parties access to the sensitive information contained in individual student records without the student's or parent's consent. As previous regulations have made clear currently the definition of educational program is quite limited. 34 C.F.R. 99.1 This change would enable any program that described itself as an educational program to access these records. This could include adult education classes, private tutoring services, day care providers or workforce training course. It is so unbounded that it could extend to websites that promise to "teach you how to make money online from home." All of these programs would be able access personally identifiable student records for the purpose of evaluating their own educational outcomes. There would be no consent required and no ability to limit this sharing.

The NPRM makes this intention clear, stating that "[t]he potential benefits of this proposed change are substantial, including the benefits of non-educational agencies that are administering ''education programs'' being able to conduct their own analyses without incurring the prohibitive costs of obtaining consent for access to individual student records. " 76 Fed. Reg. 19734. It is striking that a regulation nominally aimed at protecting student privacy would concern itself with helping additional parties to gain access to private records and avoid the prohibitive cost of obtaining consent.

Ultimately the combination of these two overarching goals – increased sharing with state officials and increased sharing with outside entities – raise another possibility which might be

permitted under these new rules: the sharing of personally identifiable student information between state systems. Such sharing is a logical progression from these widespread new sharing rules and would pave the way for a national database of student records. Such a system would have all of the same problems of improper access and data breach, but would be magnified by vast number of new users. There would also be an almost irresistible temptation to build on this database for other uses since it would represent a database of almost every American of a certain age, one that would grow over time to become a database of almost all Americans.

**Conclusion**

The NPRM poses serious privacy concerns. Personally identifiable student records include extremely sensitive information about individuals, yet these rules significantly expand the number of parties who can access a record without requiring consent from the parent or the student. These new parties include state officials not working directly on education as well as private entities that would not traditionally be able to access government educational records. Furthermore, the expansion of access to student records could eventually lead to sharing among states. If this were to happen, it could lead to the creation of an immense database holding sensitive information about most Americans.

Final regulations must express more clearly a commitment to keeping personally identifiable information confidential and barring access to that information by those who might otherwise have access to the aggregated information. When it is necessary to share personal student information the reasons for that sharing and restrictions on information must be very clearly articulated. There must be no creation of a national student database.

Sincerely,

Laura W. Murphy
Director, Washington Legislative Office

Christopher R. Calabrese
Legislative Counsel