

November 20, 2009

The Honorable Tom Harkin
Chair,
Committee on Health, Education, Labor, and Pensions
U.S. Senate
Washington, DC 20510

The Honorable Michael Enzi
Ranking Member,
Committee on Health, Education, Labor, and Pensions
U.S. Senate
Washington, DC 20510

Dear Chair Harkin and Ranking Member Enzi,

We, the undersigned organizations, are writing regarding the Children's Educational Records and Privacy report published by Fordham Law School's Center on Law and Information Policy.¹ Our concern that information on school children collected by the States is increasingly pervasive and intrusive, and if not properly protected from distribution will seriously impair children's future reputations and career possibilities. This information includes:

- 32% of states collect children's social security numbers.
- 22% of states record student pregnancies.
- 46% of states have a mechanism in place to track children's mental health, illnesses and jail sentences.
- 72% of states collect children's family wealth indicators.

In addition to these areas, some states collect information on a student's birth order, birth weight of a student's baby, whether a student is home schooled, if a student has been a victim of peer violence, medical test results, as well as information on the student's parents' education level.

For these reasons, privacy protection for data held by these systems of records must be addressed. One can obtain significant (though far from foolproof) protection by mandating that the main identifying information be stored in a separate database from the more public information, and that there be adequate use limitations; data retention policy; access controls; security; and auditing transactions that do retrieve individual identities.

¹ http://law.fordham.edu/assets/CLIP/CLIP_Report_Childrens_Privacy_Final.pdf.

We are writing to alert you to the findings of an important new report on children's privacy, which include the following:

- Only six states appear to use a third party who restricts the state's access to the student ID numbers, i.e. prevents state access to individual student data.
- Only eighteen states have detailed access and use restrictions.
- Only eighteen states require database users to enter into confidentiality agreements.
- Only ten states have data retention policies.
- Forty-nine states make FERPA information accessible on the internet, but for many the information is hard to find, vague, or incomprehensible.

We endorse an aggressive stance on limiting the collection, retention, use, or reuse of information on school-aged children. However, when data is necessary to further the education, health, safety, or welfare of children, then measures—both regulatory and procedural—should be implemented based on the following report recommendations:

- States should implement Dual Database Architecture to separate unique student identifiers from personally identifiable data, which would permit local access to needed information while minimizing the privacy risks that arise when personally identifiable information is further distributed to individuals on the state level. The two major purposes for state level collection and review of children's education records are limited to: (1) compliance with NCLB reporting requirements, and (2) audit and performance evaluation of schools.
- States that outsource data processing should have comprehensive agreements that explicitly address privacy obligations, which should include data collection limitations, use restrictions, retention limitations, role based access control, and contractual agreements that should privacy be violated notice must be provided to the institution and to the guardian or parent of each affected child.
- States should limit data collection to necessary information for clearly specified purposes.
- States should have specific data retention policies and procedures, including a clear policy for the deletion of personally identifiable student records after students exit the school system or after the records are no longer necessary for the purpose giving rise to the initial data collection.
- States should explicitly provide for limited access and use of both the local level database and the state level database.
- States should maintain audit logs that track system use of the database and access to student information.

- States should appoint a Chief Privacy Officer within the state’s Department of Education to assure the respect for children’s privacy in educational records and to oversee compliance with federal and state privacy laws.

We strongly endorse the recommendations of the report because they outline the sensible and necessary establishment of minimum baseline standards for entities and institutions responsible for implementing longitudinal databases. Furthermore, should Congress determine that action is warranted, it is imperative that they do not limit the role states can play in raising the bar on privacy protections offered to their youngest residents. Federal efforts should seek to establish minimum standards to assure that school-aged children have sufficient protection of their personal information. It is our collective recommendation that solutions address the need to more clearly define permissible reasons for data collection, create specific data retention limitations, and implement a mandatory oversight mechanism in the form of an independent Chief Privacy Officer for privacy at the state level in connection with the collection and use of children’s education data.

The practice of collecting data from students is increasing in K-12 educational systems and post-secondary education systems. There are also proposals to include data collection from pre-birth through attainment of the first job. The breadth and depth of collection of information on the very young may exceed the experience of any previous generation. Therefore, it is important to recognize the privacy risks associated with these longitudinal databases, so that children’s personal information will be properly safeguarded. Thank you.

Sincerely,

1. American Association of Collegiate Registrars and Admissions Officers
2. American Civil Liberties Union
3. Arab Community Center for Economic and Social Services
4. Center for Digital Democracy
5. Center for Financial Privacy and Human Rights
6. Coalition for Alternatives to Militarism in Our Schools
7. Consumer Action
8. Electronic Privacy Information Center
9. Gun Owners of America
10. Learning Not Recruiting (Toledo, Ohio)
11. Liberty Coalition
12. National Center for Transgender Equality
13. National Network to End Domestic Violence
14. National Workrights Institute
15. Patient Privacy Rights

16. Privacy Journal
17. Privacy Rights Clearinghouse
18. Remar Sutton, Privacy Rights Now Coalition
19. Rutherford Institute
20. The Multiracial Activist
21. World Privacy Forum