COMMON CORE AND NORTH CAROLINA: PART IV—A THREAT TO STUDENT PRIVACY

The North Carolina Institute for Constitutional Law[1]
www.ncicl.org
July 23, 2013

Common Core will bring major changes to the way K-12 curriculum is set and how student data is collected, stored, and used. News reports reveal that the data collected is not always what one might associate with educational programming. For example, Reuters reported that data collection includes not just students' names and academic information but also hobbies, attitudes toward school and career goals.[2] This raises the issue of whether the student data collection required under Common Core is so pervasive and intrusive that it violates the constitutional right of privacy. This paper examines this question and concludes that Common Core undermines student privacy and requires serious reconsideration.

Privacy Rights and Student Data. The U.S. Supreme Court has not yet explicitly stated that individuals have a right to control personal data, but it has opined that under the right set of facts, it would be open to recognition of such a right in the future. In *Whalen v. Roe*, a group of patients and doctors challenged a New York state law requiring doctors to report information to a state database on patients who were prescribed certain drugs that are prone to abuse.[3] Noting the state's important interest in maintaining public health and the steps the state took to protect personal data collected under the program, the Court sustained the program.[4] But, the Court expressed reservations about the "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[5] "The right to collect and use such data for public purposes," the Court explained, "is typically accompanied by a concomitant statutory

[1] For more information, please contact executive director Jeanette Doran at doran@ncicl.org or staff attorney Tyler Younts at tyounts@ncicl.org. Either attorney may be reached at 919-838-5313.
[2] "K-12 Student Database Jazzes Tech Start-ups, Spooks Parents," Reuters, Stephanie Simon, March 3, 2013 (available at http://www.reuters.com/article/2013/03/03/us-education-database-idUSBRE92204W20130303).
[3] 429 U.S. 589 (1977).
[4] *Id.* at 598-600 (noting legal liability for breaches of data security provided for under the law).
[5] *Id*. at 605.

or regulatory duty to avoid unwarranted disclosures."[6] Since the New York statute provided protections against breaches of data security, the Court stated, "We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data - whether intentional or unintentional - or by a system that did not contain comparable security provisions."[7] Thus, while the accumulation of vast amounts of personal data does not in and of itself present constitutional problems, failure to take proper precautions against, and remedies for, unwarranted disclosures could give rise to a legal claim for breach of privacy.

Student privacy is specifically addressed by a federal statute. The Family Education Rights and Privacy Act (FERPA) is a federal law that protects the privacy interests of students. It affords parents the right to access and amend their children's education records, and gives them some control over the disclosure of the information in these records. FERPA generally prevents an education agency or institution from sharing student records, or personally identifiable information in these records, without the written consent of a parent. Amendments in 2008 and 2011 altered FERPA regulations to make re-disclosure of student data by a State Education Authority (SEA) for the purpose of conducting studies much easier. According to the Department of Education, "Interpretations of our current FERPA regulations created obstacles for States in their efforts to comply with ARRA's [American Recovery and Reinvestment Act of 2009] requirement that SLDS [State Longitudinal Data System] include the 12 elements specified in the America COMPETES Act, and thereby allow for the sharing of education data from preschool to higher education."[8]

Collection of Data Threatens Student Privacy. The extent to which personal student data will be collected by North Carolina under Common Core remains unanswered.[9] North

---

[6] *Id*.
[7] *Id.* at 605-06.
[8] Family Educational Rights and Privacy Final Rule, 76 Fed. Reg. 75604, 75609-10 (Dec. 2, 2011) (codified at 34 C.F.R. pts. 99.3, 99.35, 99.37).
[9] Critics point to the National Education Data Model (NEDM), which is a system created by the federal government for tracking P-20W (i.e., Pre-K through early workforce) data for educational research. Although the NEDM contains several hundred data points on individual pupils, the model itself is not binding on any state, but serves as a model for

Carolina, along with every other state, "committed to building longitudinal data systems by 2011 as a condition of receiving state stabilization funds,"[10] under the ARRA.[11] To qualify, the data systems had to track 12 critical data elements that are identified in the America COMPETES Act,[12] including, to name a few, test scores, transcripts, demographic, and enrollment/dropout information.[13]

A study released in 2009 by Fordham Law School's Center for Law and Information Privacy reveals some of the privacy problems with student longitudinal databases. Following a survey of all fifty states, researchers found that educational databases across the country ignore key privacy protections for students. The report found that vast amounts of personally identifiable data and sensitive personal information about students are stored by the state departments of education in electronic warehouses or by third party vendors on behalf of the states. Researchers concluded that such data warehouses usually lack adequate privacy protections (including policies governing access, use, and retention of student data), are frequently not compliant with FERPA, and leave school children unprotected from data misuse and data breaches.[14] Although this report predates the data collection of Common Core, it is nevertheless instructive on the problems with longitudinal data systems required by ARRA and central to the Common Core Initiative's operation.

In 2012, North Carolina announced that it received a $3.64 million grant from the U.S. Department of Education to develop and implement its P-20W (i.e., Pre-K through

---

states to emulate. National Center for Education Statistics, "NEDM Frequently Asked Questions," http://nces.ed.gov/forum/datamodel/files/NEDM_FAQs.pdf.

[10] Data Quality Campaign, "Data Quality Campaign Announces Annual Progress Report on State Education Data Systems," Nov. 23, 2009, http://dataqualitycampaign.org/news-events/press-releases/data-quality-campaign-announces-annual-progress-report/.

[11] P.L. 111-5, Sec. 14005.

[12] *Id.* at Sec. 14005(d)(3). For the 12 data elements, *see* P.L. 111-358. 6401(e)(2)(D).

[13] U.S. Department of Education, "Statewide Longitudinal Data Systems Fact Sheet," July 2009, www2.ed.gov/print/programs/slds/factsheet.html. *See also* P.L. 111-358. 6401(e)(2)(D).

[14] Children's Education Records and Privacy: A Study of Elementary and secondary School State Reporting Systems, Joel R. Reidenberg, p. 24-31 (October 28, 2009) (available at http://law.fordham.edu/assets/CLIP/CLIP_Report_Childrens_Privacy_Final.pdf).

workforce) longitudinal data system.[15] Chapter 116E of the General Statutes tasks the North Carolina Longitudinal Data System Board[16] with creating an inventory of what student data will be collected and reporting it to the Joint Legislative Oversight Committee before the system is launched.[17] That inventory and report is not yet publicly available,[18] and thus the public does not know exactly what information or how many data points will be collected. However, the apparent lack of protection of personally identifiable student data is troubling. When taken together with the recent amendments relaxing FERPA regulations governing the collection and sharing of student data, the commitment to protecting student privacy under Common Core is questionable at best, and likely represents the type of shortcoming that the Court in *Whalen* identified as potentially legally deficient.[20]

Conclusion

Common Core represents a significant erosion of student privacy interests. While little is known about what student data will be collected, what we do know raises worries that student data is at risk. Steps must be taken to ensure student information is not misused—and, those steps must be taken now before the data collection begins.

---

[15] NC Dept. of Public Instruction, "NCDPI Receives Grant to Fund Statewide Longitudinal Data System," News Release, June 18, 2012, http://www.ncpublicschools.org/newsroom/news/2011-12/20120618-01.

[16] N.C. Gen. Stat. § 116E-3(a).

[17] *Id*. § 116E-4(a)(4). In addition, North Carolina has conducted a pilot test in the Guilford County Schools with a nonprofit student data and educational information organization called inBloom (formerly the Shared Learning Collaborative—an offshoot of the Council of Chief State School Officers). inBloom Press Release, "inBloom Inc. Launches to Enable Personalized Learning Through Easier Access to Information Technology," Feb. 5, 2013, https://www.inbloom.org/inbloom-launch.

[18] 2012-2013 Reports to the Joint Legislative Oversight Committee, http://www.ncleg.net/documentsites/committees/JLEOC/Reports%20Received/2012%20List%20of%20Reports%20Due%20to%20Ed%20Oversight.pdf.

[20] 429 U.S. at 605-06.