NEPC
NATIONAL EDUCATION POLICY CENTER

Tuesday, August 28, 2018

**Newsletter**

# NEPC Resources on Protecting Student Privacy in Schools

In New York, the Lockport school district plans to use $2.75 million in state bond money to purchase a new facial-recognition system. In Massachusetts, 3,000 high school students from all over the United States attended a technology leadership event with $985 tuition, later learning that the event's sponsors had targeted them on the basis of online surveys with personal details they'd filled out under the mistaken belief that the surveys would do nothing more than inform them about college and college scholarships. In Huntsville, Alabama, ed-tech consultant Douglas Levin found evidence that three different data brokers were using the district's website to collect information on visitors, including students.

All three examples illustrate the diverse and increasingly sophisticated threats to K-12 students' privacy at school. These threats raise numerous questions. What if facial recognition data ends up in databases accessed by marketers or even law enforcement or immigration officials? What happens when student data are sold to organizations that target products or propaganda to children? How do seemingly harmless activities such as using G-Suite for Education manipulate students in unseen ways by encouraging a culture of consumerism that prioritizes materialism over the civic and academic objectives that should be central to the mission of K-12 education?

The National Education Policy Center's Commercialism in Education Research Unit (CERU) has been examining questions like these now for decades. In *Asleep at the Switch: Schoolhouse Commercialism, Student Privacy, and the Failure of Policymaking*, CERU co-directors Faith Boninger and Alex Molnar make five recommendations designed to prevent new technologies from violating student privacy and causing other negative consequences in schools:

1. Prohibit schools from collecting student personal data unless rigorous, easily understood safeguards for the appropriate use, protection, and final disposition of those

data are in place.

2. Hold schools, districts, and companies with access to student data accountable for violations of student privacy.

3. Require algorithms powering education software to be openly available for examination by educators and researchers.

4. Prohibit adoption of educational software applications that rely on algorithms unless a disinterested third party has examined the algorithms for bias and error; and valid data have shown that the algorithms produce intended results.

5. Require independent third-party assessments of the validity and utility of technologies, and the potential threats they pose to students' well-being, to be conducted and addressed prior to adoption.

"In addition," Boninger and Molnar write, "parents, teachers, and administrators—as individuals and through their organizations—should work to publicize both the threats that unregulated educational technologies pose to children and the importance of allowing access to the algorithms powering educational software."

## NEPC Resources on School Commercialism

The National Education Policy Center (NEPC), housed at the University of Colorado Boulder School of Education, produces and disseminates high-quality, peer-reviewed research to inform education policy discussions. Visit us at: http://nepc.colorado.edu