Amassing Student Data and Dissipating Privacy Rights

From test-performance scores to student financial data to statewide longitudinal data systems, there has been a dramatic increase in the collection of students' sensitive information over the last decade. Both the U.S. Congress and the presidential administrations have touted the amassing of student data as beneficial and necessary to a successful education system. However, the increase in the collection of student data has led to a marked decrease in student data protection. Changes to student privacy regulations and government programs such as the Education Data Initiative underscore the need for meaningful oversight for the protection of student data.

The Education Department and Privacy Safeguards

In 2008 and 2011, the U.S. Education Department amended the regulations for the Family Educational Rights and Privacy Act (FERPA). These amendments increased private company and third-party access to student data. The 2008 changes expanded the definition of "school officials" to include "contractors, consultants, volunteers, and other parties to whom an educational agency or institution has outsourced institutional services or functions it would otherwise use employees to perform."[1] This amendment gives companies like Google and Parchment access to education records and other private student information.

> The increase in the collection of student data has led to a marked decrease in student data protection.

Google Apps for Education offers "free Web-based email, calendar, and documents" to "millions of students and educators worldwide."[2] Arizona State University, the University of Michigan, Brown University, and other higher education institutions use Google Apps for Education to provide many of the services that colleges and universities had typically provided directly to students and faculty—resources for research, e-mail, and document production.[3] Because higher education can spend hundreds of thousands of dollars to provide e-mail servers to students and faculty, the allure of "free" e-mail service is obvious.[4] Less obvious, however, is that students are paying the cost to use Google's "free" servers by providing access to their sensitive data and communications.

Google states: "To the extent that Customer Data includes FERPA Records, Google will be considered a 'School Official' . . . and will comply with FERPA."[5] Presumably, "FERPA Records" mean "education records," including test scores, transcripts, and disciplinary infractions. Other Google representations raise real concerns about how the student information, now in control of private companies, will be used. For instance, Google will disclose student information from its Apps for Education if it has a "good-faith belief" that such disclosure is "reasonably necessary" to comply with law enforcement requests and to protect "the rights, property or safety of Google, [Google] users or the public as required or permitted by law."[6] This means that Google, and not the educational institution, will be making decisions about when to disclose sensitive student (and faculty) information to law enforcement agencies.

Parchment is another popular third-party entity to which colleges and universities routinely outsource students' most prized commodity: transcripts. Parchment is a web-based service that permits colleges to "receive, request, and analyze electronic transcripts."[7] Despite Parchment's claim that its services are "fully secure and FERPA compliant," the company's terms of use reveal that to the extent permissible by law, Parchment disclaims any representation or warranty that its site is secure and disclaims any liability for lost data.[8] In an era of rampant security breaches, a company's failure to carry the responsibility for safeguarding students' transcripts is hardly reassuring.

Surprisingly, in 2011, the Education Department again loosened the safeguards for student records by modifying the key terms "education programs" and "authorized representatives" to permit greater disclosure of student data. Under FERPA, "authorized representatives" of the U.S. comptroller general, the secretary of education, and state educational authorities may access student records to audit or evaluate federally supported "education programs."[9] The new regulations broadly define "education programs" to encompass programs not only focused on "improving academic outcomes" but also related to "bullying prevention, cyber-security education, and substance abuse and violence prevention" regardless of whether the program is administered by an educational agency or institution.[10] And previously, "authorized representatives" were exclusively entities over which educational authorities had "direct control, such as an employee or a contractor of the authority."[11] Now, autho-

rized representatives can be any individual or entity that educational authorities select as an authorized representative.[12]

By amplifying "education programs" and "authorized representatives," the Education Department has taken very narrow circumstances that permit the disclosure of education records and has expanded those circumstances to the point that the disclosure of student data is no longer the exception but is increasingly becoming the rule.

Wider Disclosure, Fewer Safeguards

In January 2012 the Education Department, working with the Office of Science and Technology Policy (OSTP), announced the Education Data Initiative, a public-private partnership that collects and disseminates student data.[13] The Education Data Initiative involves several public-sector entities that gather student data and then disclose it to the private sector. For instance, under the Education Data Initiative, federal student aid websites feature "a 'MyData' download button to allow students to download their own data [and] . . . share . . . with third parties that develop helpful consumer tools."[14]

Although the Education Department and OSTP are pushing for an increase in aggregating data, these agencies do not explicitly describe how the Education Data Initiative will protect students' privacy or safeguard against security breaches. The absence of a breach policy is ironic in light of security breaches that affected an Education Department website in October 2011. The Education Department's Federal Student Loan Servicing website (http://www.myedaccount.com) exposed "the personal financial details of as many as 5,000 college students" to borrowers who had logged into the website. Although the department shut down the website while it resolved the problem and "notified and offered credit monitoring services" to those affected,[15] this is an unfortunate example of the Education Department's failure to establish appropriate technical safeguards that ensure confidentiality of personal records as required by the Privacy Act, which, like FERPA, is another landmark federal privacy law.[16]

The Education Data Initiative reflects a growing trend with student data: government agencies are taking personal information that students are required to provide, skirting federal regulations, and turning student data over to the private sector with few, if any, safeguards for privacy and security.

Conclusion

In February 2012, the Electronic Privacy Information Center (EPIC) filed suit against the Education Department regarding the changes to the federal student privacy regulations under FERPA. At EPIC, we believe the agency exceeded its authority when it revised the federal privacy law to make student data more available. And we disagree with the agency's decision to loosen the key definitions that help safeguard student records. Our case, *EPIC v. Department of Education*, is pending in federal district court in Washington, D.C.

When FERPA was enacted almost forty years ago, Congress made it clear that students' personal information should not be made widely available. Congress was particularly concerned that if student records fell into the hands of private parties, these records could hurt students later in life when, for example, students were seeking jobs. Although the pressures have increased over the years to access student data, Congress and the Education Department should work to strengthen student privacy rights and provide oversight on student data disclosure. ■

Notes

1. Family Educational Rights and Privacy Regulations Notice of Proposed Rulemaking, 73 Fed. Reg. 15,574, 15,578 (March 24, 2008); see also Family Educational Rights and Privacy Regulations, 73 Fed. Reg. 74,806, 74,852 (December 9, 2008).
2. Google Apps for Education, accessed December 12, 2012, http://www.google.com/enterprise/apps/education/.
3. "Customer Stories," Google Apps for Education, accessed December 12, 2012, http://www.google.com/enterprise/apps/education/customers.html.
4. "Arizona State University Success Story," Google Apps for Education Case Study, October 10, 2006, http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/en/edu/customers/pdfs/asu_success_story.pdf.
5. "Google Apps for Education Agreement," Google Apps, accessed December 12, 2012, http://www.google.com/apps/intl/en/terms/education_terms.html.
6. "Privacy Policy," Google, July 27, 2012, http://www.google.com/policies/privacy/#infosharing. See also "Security and Privacy," Google Apps for Education, accessed December 12, 2012, http://www.google.com/apps/intl/en/edu/privacy.html.
7. "Docufide Receiver," Docufide by Parchment, accessed December 12, 2012, http://www.docufide.com/products/docufide-receiver.
8. "Terms of Use," Docufide by Parchment, accessed December 12, 2012, http://www.docufide.com/terms-of-use.
9. 20 U.S.C. § 1232g(b)(3) (2012).
10. Family Educational Rights and Privacy Regulations, 76 Fed. Reg. 75,604, 75,614 (December 2, 2011).
11. Family Educational Rights and Privacy Regulations Notice of Proposed Rulemaking, 76 Fed. Reg. 19,726, 19,734 (April 8, 2011).
12. 34 C.F.R. § 99.3 (2012).
13. Aneesh Chopra and Zakiya Smith, "Unlocking the Power of Education Data for All Americans," *Office of Science and Technology Policy Blog*, January 19, 2012, http://www.whitehouse.gov/blog/2012/01/19/unlocking-power-education-data-all-americans.
14. Office of Science and Technology Policy, Executive Office of the President, "Fact Sheet: Unlocking the Power of Education Data for All Americans," January 19, 2012, p. 1, http://www.whitehouse.gov/sites/default/files/microsites/ostp/ed_data_commitments_1-19-12.pdf.
15. "Government Site Exposes Financial Info of Thousands of College Students," *CBS Local Media*, October 26, 2011, http://washington.cbslocal.com/2011/10/26/government-site-exposes-financial-info-of-thousands-of-college-students/. See also Alice Lipowicz, "Education Dept.'s New Website Suffers Data Leak, Malfunctions," *Federal Computer Week*, October 31, 2011, http://fcw.com/articles/2011/10/31/education-dept-experiencing-data-leak-glitches-on-new-student-loan-website.aspx.
16. 5 U.S.C. § 552a(e)(10) (2012).

Marc Rotenberg (rotenberg@epic.org) is Executive Director of the Electronic Privacy Information Center (EPIC) in Washington, D.C. He teaches Information Privacy Law at Georgetown University Law Center. **Khaliah Barnes** (barnes@epic.org) is Administrative Law Counsel at EPIC.