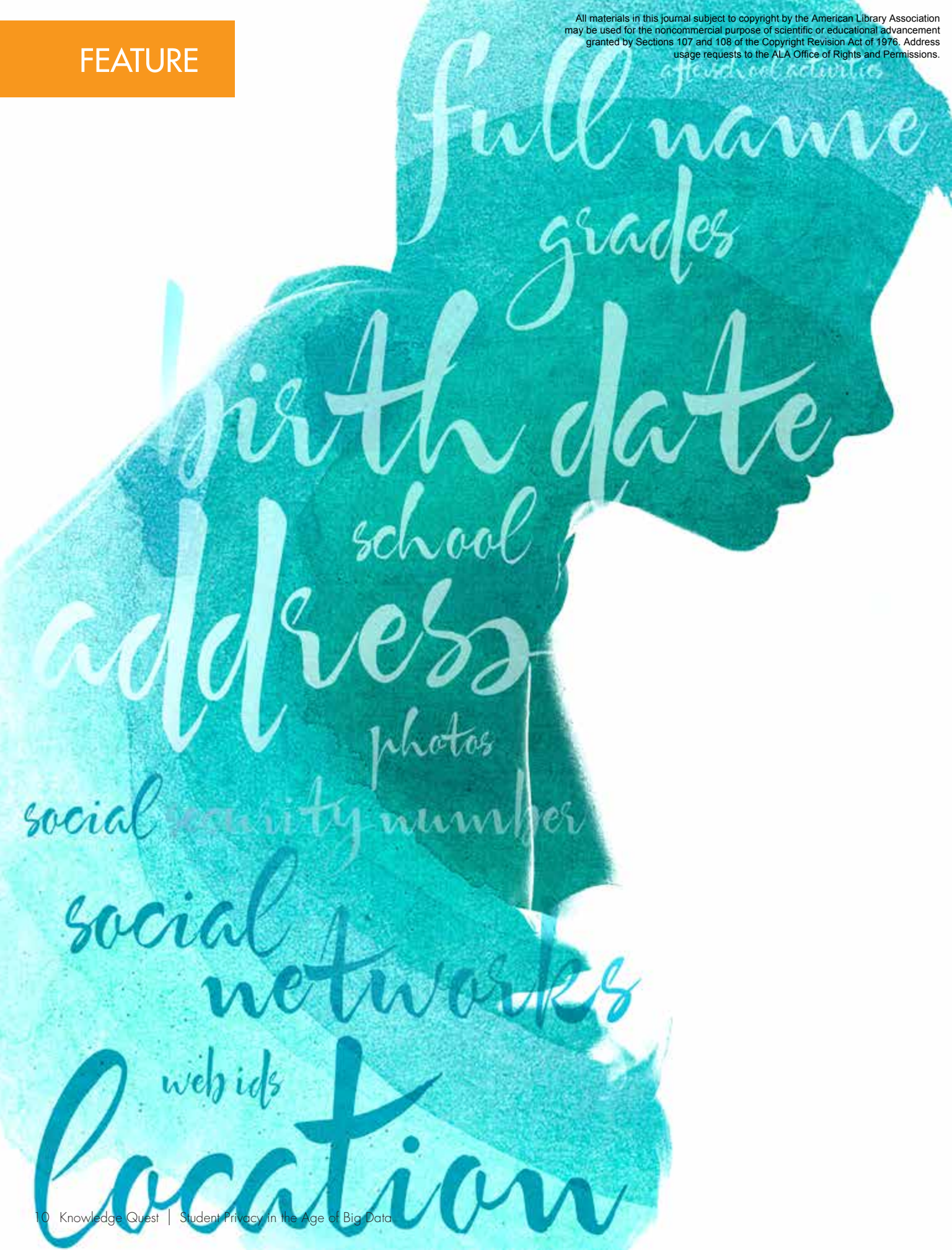
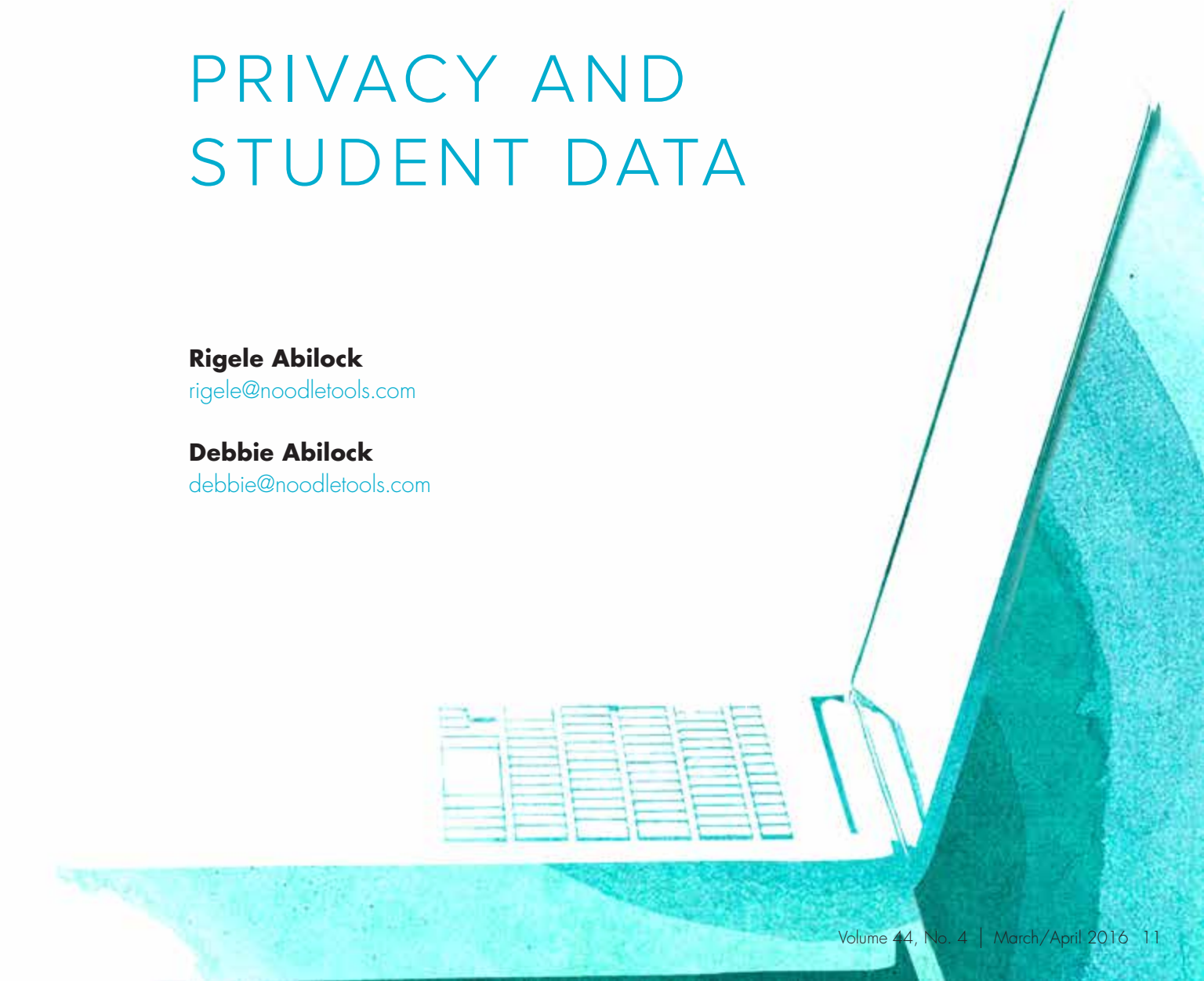


i agree, but do i KNOW?

PRIVACY AND STUDENT DATA

Rigele Abilock
rigele@noodletools.com

Debbie Abilock
debbie@noodletools.com



School librarians are champions of online learning. They select databases, use instructional software, and promote intellectual freedom including student access to the Internet. Propelled by the significant benefits of learning, engagement, and personalized instruction, many of their schools and districts have rapidly adopted online services without establishing standardized controls or protections for the massive amounts of student data being collected and shared. A 2013 study by Fordham Law School's Center on Law and Information Policy found that, while cloud services were deployed for wide-ranging functions in 95 percent of the six demographically and geographically diverse districts surveyed, they were "poorly understood, non-transparent, and weakly governed." The study noted "rampant gaps" in vendor-school contract documentation, an absence of policies governing privacy, and a failure to inform parents about their children's exposure to online services (Reidenberg et al. 2013, 5).

The situation is changing quickly. Some large districts now employ teams of in-house legal and policy experts who are charged with protecting student data and specifying measurable characteristics of "safe" online products. Most schools are in the process of developing privacy protocols and priorities. A strategic opportunity exists for school librarians to become leaders in shaping school privacy practices by guiding students, families, and faculty in wise and safe technology use while advocating for privacy rights. As advocates for thoughtful online learning, we must, at the very least, examine data confidentiality policies for the products we select and disseminate. More strategically, in our role as digital citizenship educators we must participate in our institutional decision-making process. We hold in our hands a fundamental responsibility to students as learners and citizens in a democracy guided by our profession's core values, which state that "Protecting user privacy and confidentiality is necessary for intellectual freedom and fundamental to the ethics and practice of librarianship" (ALA 2004).

As advocates for thoughtful online learning, we must examine data confidentiality policies for the products we select and disseminate.

Do You Sign (and Read) the Contract?

To balance student privacy with educational objectives, a district or school must develop transparent guidelines and metrics to evaluate the policies and contracts of its online vendors. In support of these goals, the U.S. Department of Education's Privacy Technical Assistance Center provides resources that include "Warning signs and potential illegal practices to look out for" when using cloud-based services, recommendations for practices and policies to protect student data, and a checklist for evaluating how a vendor's Terms of Service (ToS) handles data in "a safe and secure manner" (PTAC 2015).

The ToS document is a formal contractual agreement between the school and the vendor; it governs the vendor's obligations and limits its liabilities. Especially significant are terms concerning data storage, data retention, data handling, liability for data breach, and contract termination. Once a school or district representative clicks "I agree," typically by click-wrap or click-through signature, the school has accepted the vendor's terms, regardless of whether those terms are in alignment with the Family Educational Rights and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA), and other federal and state laws.

The school board or a selected designee such as the superintendent or assistant superintendent is authorized to contract for a district. By most states' laws, teachers in a district do not individually possess the legal right to bind a district or school to a contract, while school librarians who negotiate contracts with vendors, network providers, and other licensors may have that right.

However, authorized or not, when teachers or librarians click through a ToS display they may expose the school or district to liability if student data flows out of the school. Melissa Tebbenkamp, Raytown (MO) District director of instructional technology, acknowledges this vulnerability: "We have a problem with sites targeting our teachers… [who are] not being responsible with our data. For school technology directors around the country, it is a can of worms" (Singer 2015b).

Do You Read the Privacy Policy?

While the ToS document is a formal two-way agreement between vendor and school, a vendor's privacy policy is a working picture of the company's current and expected practices related to data use, collection, and sharing, as well as marketing, advertising, access, and security controls. As an on-the-ground description of how the vendor operates its site, the privacy policy should be read in conjunction with the ToS. While a policy lacks the contractual element of a click-through signature, it remains the primary declaration of the company's privacy practices, and thus may be enforceable against a vendor that breaches those stated practices.

A direct link to a provider's privacy policy must be displayed at the bottom of its homepage. Read the entire privacy policy closely. For example, the introduction to Khan Academy's Privacy Notice (2014) states: "We established ourselves as a not-for-profit organization so that our mission of education and your trust will not be in conflict with a for-profit motive." However, a later clause reads: "We may allow third-party service providers to place and read their own cookies, web beacons, and similar technologies to collect information through the Website."

Unless you negotiate a contract that specifically prohibits certain practices, your students' data privacy can be compromised. Diane Savage, an attorney in the Technology Transactions Group of the prominent Silicon Valley law firm Cooley, LLP, observes:

> "Given the concern about the sharing of personal information of children evidenced by the Children's Online Privacy Protection Act, it is surprising that FERPA—the most well-known educational privacy law—is generally only enforceable against educational institutions that receive federal funds, and not directly against the vendors that actually cause the FERPA violation. While a few states, notably California, have or are in the process of enacting laws directly restricting vendor use of student information, for the most part the only liability vendors face for FERPA violations is liability that they are required to assume by schools that impose such liability in their contracts with these vendors." (Savage 2015)

To balance student privacy with educational objectives, a district or school must develop transparent guidelines and metrics to evaluate the policies and contracts of its online vendors.

CURRENT STATE OF AFFAIRS

In April 2015 U.S. House Representatives Luke Messer and Jared Polis introduced the bipartisan Student Digital Privacy and Parental Rights Act of 2015, designed to significantly restrict how online education vendors can exploit the personal data of students who use their products. For some, the bill does not go far enough. Parents and privacy advocates identified weaknesses in the proposed bill:

> "It allows school services to make unilateral changes to their contracts and privacy policies. It permits them to disclose student information for purposes like preparing for 'employment opportunities'...The bill is also unlikely to prohibit companies like Pearson from monitoring the social media posts of students if those activities are performed on behalf of state educational agencies." (Singer 2015a)

It is evident that future prospects for student online privacy regulation hinge on many political debates to come—and encompass innovation, education, society, corporations, and democracy.

News reports, parent concerns, and information from professional organizations like the International Society for Technology in Education (ISTE) and the Consortium for School Networking (CoSN) have raised the bar on online student privacy protection. Common Sense Media reports that there is bipartisan national support among adults, even those without children in school, for "tighter regulations on student data...to ensure their private information is not exploited for commercial purposes and stays out of the hands of the wrong people" (2014).

With U.S. policy in flux—and schools, vendors, and parents all responsible parties—here's what you need to know about the current federal regulations governing school data privacy.

FERPA, PPRA, and the Accountability of Schools (and Parents)

School accountability is governed through two federal statutes issued by the U.S. Department of Education. Both FERPA (Family Educational Rights and Privacy Act) and PPRA (Protection of Pupil Rights Amendment) regulate how public schools can collect and use their

students' personal information and records. FERPA and PPRA aim to protect all student records, data, and directory information as "school confidential" barring specific parental consent or opt-out.

However, the boundaries can be blurry. For example, although the burden of confidentiality remains with the school, FERPA provides exceptions for information flow to school officials, who can, in turn, include outsourced contractors. Thus, FERPA permits certain re-disclosures of student data to outside vendors, contractors, nonprofits, and businesses. The U.S. Department of Education has established the Privacy Technical Assistance Center (PTAC) <http://ptac.ed.gov> as a resource for education stakeholders and families seeking current information about student-level data privacy, security practices, and implementation of FERPA.

COPPA and the Accountability of Vendors (and Schools and Parents)

Unlike FERPA and PPRA, which together define schools' obligations, the Children's Online Privacy Protection Act (COPPA) directly regulates online vendors. Enforced by the Federal Trade Commission, COPPA endeavors to align for-profit vendors with educational goals. It elevates the consent requirements of any commercial vendor that knowingly chooses to collect, use, or disclose the personally identifiable information of children under thirteen.

If the vendor collects and uses the students' personal information for the benefit of the school alone, the school may consent on behalf of all children. However, if the vendor wishes to collect and/or exploit personal information for purposes beyond the benefit of the school, parental consent is required. Since a majority of online educational services do require parental consent, it seems clear that children's identifiable information is often being collected and used for commercial purposes. While COPPA is an important step in naming vendors as accountable for their educational products and services, it has resulted in significant responsibility being transferred to parents.

Do You Trust—And Verify?

Close reading of a ToS agreement and privacy policy should be augmented by common-sense evaluation of a vendor's corporate or organizational intention. A few online education platforms have been proactively designed as safe havens for student privacy. As models of ethical practices, they demonstrate that it is possible for a profit-making corporation to provide online services with "sufficient flexibility to accommodate a wide variance of circumstances, including types of technologies, types of data, and local needs [in order to provide schools with] a privacy and security floor…without a digital learning ceiling" (Schneiderman 2015, 4). Although certain monetary benefits are forfeited as a result, district purchasing decisions are simplified and the committed focus to educational goals earns subscribers' trust.

In contrast, companies with ads for online shoe stores and insurance companies plastered on their webpages should raise red flags about corporate intention and the likely prioritization of corporate versus educational goals. To help you assess a company's data-handling practices, Me and My Shadow reviews a number of tools that you can use (Tactical Technology Collective n.d.). For example, a browser add-on like Ghostery (see figure 1) or Mozilla's Lightbeam can expose the embedded but invisible code that continually collects data and tracks users' behavior as they navigate within and across sites.

Who Should Be Responsible?

Drilling down to the functional level, technology purchases must serve an educational purpose. Elizabeth Calhoun-Brumbaugh, who manages Educational Technology Services for California's Santa Clara County Office of Education, criticizes districts that develop tunnel vision for technology as a stopgap solution without a clear, justifiable learning rationale:

> "Privacy policies for technology products are an anomaly in public education. Previously, schools would create device-specific policies—iPad policies, Facebook policies—and set up learning management systems, but they haven't had the time or resources to explore the underlying behaviors—how to evaluate individual pieces of technology for educational value in direct support of the curriculum." (Calhoun-Brumbaugh 2015)

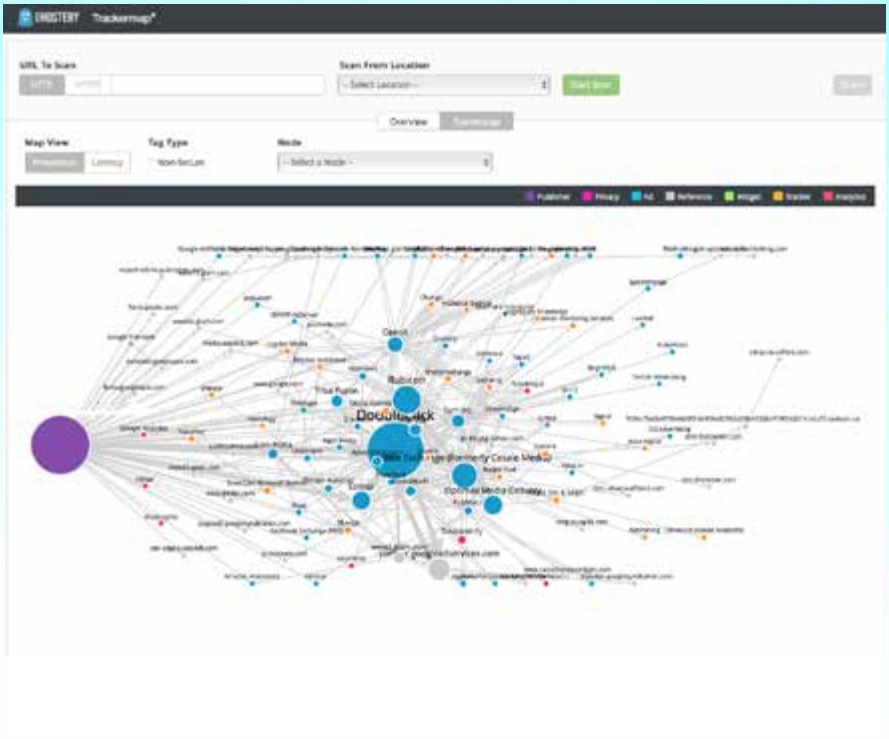
A new industry has arisen to consolidate decision-making about "safe" online products. Companies like Clever, IKeepSafe, Common Sense Media, and Google Apps for Education offer differing solutions, but each organization has its own agenda. It's unlikely that a single system for managing and securing applications can serve as a one-size-fits-all solution for a school's unique blend of teaching styles, curriculum, culture, and community values. With this reality in mind, it's imperative to create formal but accessible channels so that teachers and librarians can choose software and services to support specific learning goals while also meeting the school's stated privacy goals.

School librarians can develop the necessary strategic alliances and nurture the transparency that will build community trust around this contentious issue. Become familiar with the "Protecting Privacy in Connected Learning" toolkit (Consortium for School Networking and Harvard Law School's Cyberlaw Clinic 2014) and the foundational principles for safeguarding student data that are supported by a number of professional associations ("Student Data Principles" n.d.). On your library website, include information about online privacy policies and terms of service for products you purchase or promote. In advance of any issues, approach your administration with a proposal for a privacy advisory committee—or cultivate that skill set within your existing technology acquisitions group. Seek mentors within your district and authorities in educational services cooperatives or county offices of education, and then weave discussions of these topics into staff meetings and professional development workshops, as well as your digital citizenship lessons.

Be prepared to articulate the learning benefits and quality of online product choices to your community. Parental consent should be an informed consent, not an empty formality. Rather than counseling parents to perfunctorily sign a blanket consent provided by the school so their children are not "left out" of

Figure 1. Examples of tools that make data tracking visible to Web users.

Ghostery's add-on identifies 25 trackers on a website, which you can choose to block.



Ghostery Tracker shows that ads and trackers from 80 unique vendors have been coded into one educational site's homepage (purple).

Rather than counseling parents to perfunctorily sign a blanket consent provided by the school so their children are not "left out" of classroom activities, present a rationale with specific information about the quality and benefits of your online learning choices in language that everyone can

understand and respect.

Without being defensive, be ready to explain the trade-offs between privacy and unique learning or information opportunities, and the specific decision-making process employed at your school.

classroom activities, present a rationale with specific information about your online learning choices in language that everyone can understand and respect. Parents with professional careers in technology are astute about the inner workings of online data tracking and the use of their own children's personal data (Singer 2015c). Without being defensive, be ready to explain the trade-offs between privacy and unique learning or information opportunities, and the specific decision-making process employed at your school.

Our total digital footprint doubles every two years, over half of which is not the data we actively manage nor the personae we intentionally craft for social media (Aiden and Michel 2013, 246). This "invisible" data consists of traces left behind from our Web search histories, app use, e-mail and other online correspondence, credit card purchases, locational and IP tracking, and images taken by surveillance cameras—data often collected without our knowledge or consent. How will this web of data play out in our future? Thomas H. Davenport, author of *Big Data @ Work: Dispelling the Myths, Uncovering the Opportunities*, sums up the uncertainties of the future of big data as "What we don't know—and won't for a while" (2014, 26).

Computing pioneer Alan Kay has said, "The best way to predict the future is to invent it" (TED Conferences n. d.). We agree. Rather than wait for others to define that future, the librarian who embraces a leadership role regarding school privacy practices can shape a future in which vibrant and safe student learning is possible. The U.S. Secretary of Education has characterized privacy as an issue of keeping kids safe: "Privacy rules may well be the seatbelts of this generation" (Duncan 2014). True, for the moment. However, just as we counsel students to be savvy digital citizens, safe Internet users, and critical thinkers—and just as we urge them to be personally responsible for their online choices—we have a responsibility to protect them *in loco parentis*. The underpinnings of democracy rest on each citizen's access to opportunity and the assurance of privacy protection *from both corporate infringement and government surveillance*. While "privacy is essential to the exercise of free speech, free thought, and free association and, therefore, essential to democracy" (Krug 2005, ix), it is equally true that our free choices are threatened when companies track and use our personal data to engineer behavior for their own gain or for some paternalistic goal (Belluz 2014; Meyer 2014; Segran 2014; Thaler and Sunstein 2009).

Ultimately, the stakes for society are high. We hold in our hands a fundamental responsibility—shaped by democracy—that will have a profound impact on our students and future citizens, above and beyond the reach of our school's resources and services.

Rigele Abilock *is President of Corporate Strategy and Operations for NoodleTools, an online research management platform in Palo Alto, California. Her expertise spans over 20 years of working with technology-based companies on their business strategies and contractual relationships.*

Debbie Abilock, *NoodleTools' cofounder responsible for education vision, serves on the board of the ALA Center for Civic Life and has been a member of AASL for 33 years. An award-winning educator and* Library Journal *Mover and Shaker, she writes "Friction," a column on teaching slow thinking and intentionality in research, for* School Library Connection *magazine, and coauthored the article "Recipe for an Infographic" in the November/December 2014 issue of* Knowledge Quest.

Works Cited:

Aiden, Erez, and Jean-Baptiste Michel. 2013. *Uncharted: Big Data as a Lens on Human Culture*. New York: Riverhead.

American Library Association. 2004. "Core Values of Librarianship." <www.ala.org/advocacy/intfreedom/statementspols/corevalues> (accessed November 1, 2015).

Belluz, Julia. 2014. "The Insidious New Ways Big Pharma Is Manipulating Your Doctors' Drug Choices." *Vox* (November 13). <www.vox.com/2014/11/13/7197729/phamaceutical-digital-marketing> (accessed April 7, 2015).

Calhoun-Brumbaugh, Elizabeth. 2015. Interview with Rigele Abilock. May 18.

Common Sense Media. 2014. "Student Privacy Survey." <www.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf> (April 7, 2015).

Consortium for School Networking, and Harvard Law School's Cyberlaw Clinic. 2014. *Protecting Privacy in Connected Learning Toolkit*. Washington, DC: CoSN. <http://cosn.org/sites/default/files/Protecting%20Privacy%20in%20Connected%20Learning%20Toolkit%202014_0.pdf> (accessed April 7, 2015).

Davenport, Thomas H. 2014. *Big Data @ Work: Dispelling the Myths, Uncovering the Opportunities*. Boston: Harvard Business Press.

Duncan, Arne. 2014. "Technology in Education: Privacy and Progress." <www.ed.gov/news/speeches/technology-education-privacy-and-progress> (access April 7, 2015).

Khan Academy. 2014. "Khan Academy Privacy Notice." <www.khanacademy.org/about/privacy-policy> (accessed April 13, 2015).

Krug, Judith. 2005. "Foreword." In *Privacy in the 21st Century: Issues for Public, School, and Academic Libraries*, by Helen R. Adams, et al., ix–x. Westport, CT: Libraries Unlimited.

Meyer, Robinson. 2014. "Everything We Know about Facebook's Secret Mood Manipulation Experiment." *Atlantic* (June 28). <www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648> (accessed April 7, 2015).

Privacy Technical Assistance Center. 2015. "Protecting Student Privacy While Using Online Educational Services: Model Terms of Service." <http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf> (April 7, 2015).

Reidenberg, Joel N., et al. 2013. *Privacy and Cloud Computing in Public Schools*. New York: Center on Law and Information Policy, Fordham University School of Law. <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip> (accessed April 7, 2015).

Savage, Diane. 2015. Interview with Rigele Abilock. May 27.

Schneiderman, Mark. 2015. "Security and Communication Improve Community Trust." *Phi Delta Kappan* 96 (5) 29–34.

Segran, Elizabeth. 2014. "Keeping Down with the Jones: How You're Being Manipulated to Save the Environment." *Fast Company* (December 2). <www.fastcompany.com/3039203/elasticity/keeping-down-with-the-joneses-how-youre-being-manipulated-to-save-the-environment> (April 7, 2015).

Singer, Natasha. 2015a. "Bill Would Limit Use of Student Data." *New York Times* (March 22). <http://nyti.ms/1G1564z> (accessed April 7, 2015).

———. 2015b. "Privacy Pitfalls as Education Apps Spread Haphazardly." *New York Times* (March 11). <http://nyti.ms/19csX4Z> (accessed April 7, 2015).

———. 2015c. "Uncovering Security Flaws in Digital Education Products for Schoolchildren." *New York Times* (February 8). <http://nyti.ms/16CM469> (accessed April 7, 2015).

"Student Data Principles: 10 Foundational Principles for Using and Safeguarding Students' Personal Information." n.d. <http://studentdataprinciples.org/the-principles> (accessed April 13, 2015).

Tactical Technology Collective. n.d. "Useful Tools to Help You Defend Your Privacy." <https://myshadow.org/resources> (accessed April 6, 2015).

TED Conferences n. d. "Alan Kay." <www.ted.com/speakers/alan_kay> (accessed December 12, 2015).

Thaler, Richard H., and Cass R. Sunstein. 2009. *Nudge: Improving Decisions about Health, Wealth, and Happiness*, revised and expanded ed. New York: Penguin.