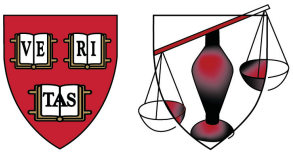


Research Publication No. 2014-10
June 3, 2014

Framing the Law & Policy Picture: A Snapshot of K-12 Cloud-Based Ed Tech & Student Privacy in Early 2014

Leah Plunkett
Alicia Solow-Niederman
Urs Gasser

23 Everett Street • Second Floor • Cambridge, Massachusetts 02138
+1 617.495.7547 • +1 617.495.7641 (fax) • http://cyber.law.harvard.edu •
cyber@law.harvard.edu

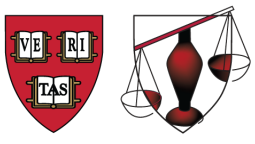
STUDENT PRIVACY INITIATIVE

Berkman Center for Internet & Society

Framing the Law & Policy Picture: A Snapshot of K-12 Cloud-Based Ed Tech & Student Privacy in Early 2014

June 2014

Leah Plunkett, Alicia Solow-Niederman, and Urs Gasser



Berkman

The Berkman Center for Internet & Society at Harvard University

23 Everett Street • Second Floor • Cambridge, MA 02138
• +1 617.495.7547 • www.cyber.law.harvard.edu/ •

ABSTRACT

A growing number of primary and secondary (K-12) school systems nationwide are adopting cloud-based educational technologies ("ed tech"), tools which "enable the transition of computing resources—including information processing, collection, storage, and analysis—away from localized systems (i.e., on an end user's desktop or laptop computer) to shared, remote systems (i.e., on servers located at a data center away from the end user accessible through a network)" in the course of educational and / or academic administrative work. Cloud-based ed tech possesses unique innovative potential that can best be unlocked when the opportunities it presents are considered alongside the importance of protecting student privacy.

This paper, building upon findings of the ongoing Student Privacy Initiative under the auspices of the Berkman Center for Internet & Society at Harvard University, provides a snapshot of key aspects of a diverse—and heated—law, policy, and implementation debate that is taking place in the rapidly evolving cloud-based ed tech landscape. It aims to provide policy and decision-makers at the school district, local government, state government, and federal government levels with greater information about and clarity around the avenues available to them in evaluating privacy options. This analysis focuses on three overarching questions: who in the educational system should make cloud-based ed tech decisions; when is parental consent needed for the adoption of these technologies; and how can data transferred, stored, and analyzed through these products be kept secure and, as necessary, de-identified?

Though there is often no bright line rule that can strike an ideal balance of these and other imperatives—including normative commitments, innovative educational opportunities, and evolving privacy attitudes and expectations—the authors offer the following pragmatic recommendations based on the cloud ed tech landscape at this moment in time:

(1) Employing (temporary) centralization of cloud-based ed tech decision-making at the district level to foster the legal, technical, and other expert oversight necessary in this complex space without stifling capacity for local experimentation;
(2) Examining the adoption of user-friendly labeling of cloud-based ed tech products to increase transparency and encourage compliance with parental consent and other legal requirements; and
(3) Adopting FIPPs (Fair Information Practice Principles) and other best practice standards by industry providers to increase data security and protection.

Critically, any such recommendations must preserve room for future development as the student privacy and ed tech picture continues to evolve. The authors also recognize that the proposed practices are in flux and have to be read as a supplement rather than a substitute for careful consideration of more fundamental reform of the current student privacy framework.

INTRODUCTION

In February 2014, President Barack Obama pledged billions of dollars in new support for educational technologies to "put the world and outer space at every child's fingertips."[1] Whether students themselves get online or not, however, data about them is likely already there. The widespread adoption of cloud technologies by educational institutions indicates a fundamental transformation of primary and secondary (K-12) education in which "data" plays an increasingly important role.[2] Indeed, a recent study of K-12 public school districts found that 95% of districts in a nationally representative sample are currently using one or more forms of cloud-based educational technologies ("ed tech").[3] Yet such widespread adoption belies a more complex reality. Much of the popular media coverage suggests that policy and decision-makers are experiencing significant turbulence as they address unprecedented questions about the proper interplay between student privacy, educational and administrative autonomy, and cloud-based technological innovation—with the metaphorical space shuttle already out of the station.[4]

In recent months, stories about cloud-based ed tech—its uses, abuses, promises, pitfalls, and beyond—have featured frequently in the news and in the materials of advocacy, industry, or governmental groups.[5] This widespread public interest in cloud-based ed tech contributes to a robust societal dialogue on the topic; however, the conversations in this space are often narrow in focus—for instance, drawing on the latest headline or responding to a particular ed tech service—or emotional in tone.[6] The preponderance of event-driven and expressive coverage in many cases threatens to eclipse substantive discussion of important legal, policy, and regulatory issues, and also may impede balanced consideration of innovative technological and educational

---

[1] Allie Bidwell, *Obama Announces Nearly $3 Billion in Education Technology Commitments*, U.S. NEWS & WORLD REPORT (Feb. 4, 2014), http://www.usnews.com/news/articles/2014/02/04/obama-to-announce-nearly-3-billion-in-education-technology-commitments.

[2] *Cf.* Urs Gasser, *Cloud Innovation and the Law: Issues, Approaches, and Interplay,* BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY 2 (March 17, 2014), http://cyber.law.harvard.edu/node/9070 ("Many of today's trends and developments in the ICT [information and communication technology] space are powered by a less visible and arguably more evolutionary innovation at the lower layers of the ICT infrastructure.")

[3] Joel Reidenberg *et al.*, *Privacy and Cloud Computing in Public Schools*, CENTER ON LAW AND INFORMATION POLICY, FORDHAM LAW SCHOOL 11-12, 19 (Dec. 13, 2013), http://ir.lawnet.fordham.edu/clip/2/ [hereinafter *CLIP Report*] (defining "ed tech" as "any computing activity that collect[s] or transfer[s] student information for processing by third parties over the Internet").

[4] *See*, *e.g.*, Elizabeth Dwoskin, *Student Data Company to Shut Down Over Privacy Concerns*, WALL ST. J. (Apr. 21, 2014), http://blogs.wsj.com/digits/2014/04/21/student-data-company-to-shut-down-over-privacy-concerns/; Jo Napolitano, *Data Service inBloom Calls It Quits*, NEWSDAY (Apr. 21, 2014), http://www.newsday.com/long-island/data-service-inbloom-calls-it-quits-1.7780439 (tracing how concerns about student privacy led schools in five states to halt their relationship with inBloom, a cloud-based ed tech company with major financial backing, and ultimately to inBloom's decision to close).

[5] *See*, *e.g.*, Kenneth Cukier, *Big Data at School: Open Learning*, ECONOMIST.COM (Apr. 22, 2014), http://www.economist.com/blogs/prospero/2014/04/big-data-school-0 (explaining that education sector is relative newcomer to use of tech and big data); *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, PRIVACY TECHNICAL ASSISTANCE CENTER, U.S. DEPT. EDUCATION (Feb. 2014), http://educationnewyork.com/files/Student_Privacy_and_Online_Educational_Services_%28February_2014%29.pdf [hereinafter PTAC, *Best Practices*] (giving updated federal guidance for school systems on how to use ed tech while protecting privacy).

[6] *See*, *e.g.*, Natasha Singer, *Deciding Who Sees Students' Data*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?_r=0 (describing some parents' negative reaction to a Colorado school district's adoption of inBloom).

opportunities. Moreover, it is often unclear in these conversations whether different actors share the same understandings of the technologies at play, especially since there is not a universal definition of cloud technologies across education or other sectors.[7]

This analysis, which emerged from a collaboration among the authors under the umbrella of the Student Privacy Initiative ("SPI") at the Berkman Center for Internet & Society at Harvard University, understands cloud-based ed tech as technologies that "enable the transition of computing resources—including information processing, collection, storage, and analysis—away from localized systems (i.e., on an end user's desktop or laptop computer) to shared, remote systems (i.e., on servers located at a data center away from the end user accessible through a network)" in the course of educational and / or academic administrative work.[8] The goal of this paper is to explore and elevate key public discussions regarding student privacy in federal law, policy, and implementation that are currently taking place in the United States' K-12 cloud-based ed tech landscape so that ed tech policymakers and decision-makers at the school district, local government, state government, and federal government levels can gain a deeper understanding of the privacy options available to them.[9] To that end, the paper focuses on three overarching questions facing policymakers and decision-makers: who in the educational system should make cloud-based ed tech decisions; when is parental consent needed for the adoption of these technologies; and how can data transferred, stored, and analyzed through these products be kept secure and, as necessary, de-identified?

This paper explores the answers to these questions by using a hypothetical cloud ed tech product, Scholair. Where appropriate, the paper identifies areas in which there appears to be rough consensus among various stakeholders—including academics, non-profit organizations, district and government officials, and industry partners—regarding a desirable course of action at this moment in time, as well as those where there appears to be greater disconnect. In identifying these junctures, the paper draws significantly on a series of on-going Berkman Center hosted working group meetings.[10]

---

[7] *See*, *e.g.*, Nabil Sultan, *Cloud Computing for Education: A New Dawn?*, 30 INTERNAT'L J. INFO MGMT 109, 110 (2010) ("A study by McKinsey . . . found that there are 22 possible separate definitions of cloud computing . . . no common standard or definition for cloud computing seems to exist.")

[8] *See* Gasser, *Cloud Innovation* at 3 (defining cloud computing across contexts).

[9] There are of course many other important constituencies in the ed tech space, including—but not limited to—teachers, parents, students, and industry representatives. A growing number of resources exist to support the efforts of these and other groups to navigate the ed tech terrain. *See*, *e.g.*, Consortium on School Networking ("CoSN"), *Protecting Privacy in Connected Learning Toolkit* (Version 1, March 2014), http://www.cosn.org/about/news/cosn-issues-k-12-privacy-toolkit-school-leaders [hereinafter "CoSN, *Toolkit*"]. State legislatures are also very active in the ed tech arena; however, due to the heterogeneity of efforts at the state level, this paper has chosen not to include state laws in this analysis so that a coherent national level snapshot may be presented. *Cf. generally State Analysis*, DATA QUALITY CAMPAIGN, http://www.dataqualitycampaign.org/your-states-progress/by-state/overview/ (last visited on May 2, 2014) (evaluating each state's progress toward achieving a certain set of ed tech data quality standards, as set by DQC); EducationCounsel LLC, *Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers* 2 & Appx. B (Mar. 2014), http://educationcounsel.com/docudepot/articles/EducationCounsel%20Guidance%20on%20State%20Student%20Privacy%20and%20Security%20Policies%20-%204838-6763-1641%20v%201.pdf (articulating set of "foundational components" for state laws, as well as model legislative language).

[10] This identification has been done based on qualitative—not quantitative—information, including outputs from the multi-stakeholder working group meetings that Berkman has convened on student privacy issues (the second of which was co-organized with CoSN). *See* Alicia Solow-Niederman, Leah Plunkett, & Urs Gasser, *Student Privacy*

The preliminary recommendations (based on the state of play in early 2014) that this paper offers in response to each of these three questions are designed to safeguard both privacy and the potential for technological innovation. There is often no bright line rule to be applied to balance these and other imperatives; however, there are pragmatic positions that can be taken, consistent with legal and regulatory requirements, as well as emerging best practice standards. As the authors continue to learn about the complex and dynamic cloud ed tech terrain, the positions reflected in this paper will no doubt evolve. The authors recognize that the proposed practices are in flux and have to be read as supplements to rather than substitutes for formal policy guidance and possible long-term privacy reform. They also leave unaddressed important deeper-layered normative questions in this sphere, such as the desirability of data driven education.[11]

I. CLOUD-BASED ED TECH: BACKGROUND & STATE OF PLAY

Schools and districts use educational technologies in a number of complex and rapidly evolving ways, giving rise to an "estimated $8 billion market" for "educational technology software" from pre-K to grade 12.[12] Within this booming market—which includes an array of technology types—cloud technologies offer unique benefits: "elastic, scalable computer resources; consumption-based pricing; and, minimization of operational expenses and elimination of upfront investments."[13] Educational institutions are required to store large amounts of student data (everything from grades to health records to bus schedules and beyond); to manage that data effectively (for instance, allowing teachers to access attendance records for their classes easily); and to protect that data so only faculty and administrators authorized by law, regulation, and policy can access it (e.g., not allowing teachers to see attendance records for students in other classes).[14]

Especially given the resource constraints under which school systems tend to operate and considering the generative potential of the Internet, many policy and decision-makers have started to embrace cloud products that promise a cost-effective "technological fix" for massive student data challenges.[15] In particular, cloud-based ed tech allows multiple users to work with

---

and Cloud-Computing at the District Level: Next Steps and Key Issues, BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (Jan. 15, 2014), http://cyber.law.harvard.edu/publications/2014/district_level [hereinafter SPI, *Student Privacy and Cloud Computing*]; Urs Gasser, Alicia Solow-Niederman, & Caroline Nolan, *Student Privacy in the Cloud Computing Ecosystem: State of Play and Potential Paths Forward,* BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (Nov. 2013), http://cyber.law.harvard.edu/node/8650 [hereinafter SPI, *State of Play*].

[11] *See, e.g.*, SPI, *State of Play* at 2.

[12] Natasha Singer, *Group Presses for Safeguards on Personal Data of Schoolchildren*, N.Y. TIMES (Oct. 13, 2013), http://www.nytimes.com/2013/10/14/technology/concerns-arise-over-privacy-of-schoolchildrens-data.html?_r=0. *See also CLIP Report* at Exec. Summary ("[D]istricts rely on cloud services for a diverse range of functions including data mining related to student performance, support for classroom activities, student guidance, data hosting, as well as special services such as cafeteria payments and transportation planning.")

[13] Gasser, *Cloud Innovation* at 5.

[14] *Cf. generally CLIP Report* at 17-21 (mapping the "functions that schools outsource to third parties and that involved the transfer of student data").

[15] Singer, *supra* note 6 (describing how superintendent of Jefferson County, CO school system "thought [cloud provider inBloom] sounded like a technological fix for one of her bigger data headaches," namely the non-inter-operability of existing ed tech systems in the district).

sub-sets of the same body of data simultaneously but for different ends (for example, all advisors want to send real time email alerts to parents of kids who are tardy for class at the same time that the teachers of those classes want to grade homework assignments).[16] These technological solutions encompass a wide spectrum of products, including offerings from tech giants like Google, Microsoft, and Amazon, as well as smaller companies like Socrative and ClassDojo.[17] Such technologies may also offer capacities beyond those possessed by faculty and administrators themselves; for instance, some cloud technologies offer "[d]ata analytics services . . . that aggregate and analyze student data . . . [to] provide a 'big picture view'" of students' and schools' performances along various metrics.[18]

Educators' use of cloud-based ed tech should be understood not only as a response to challenges, but also as an affirmative embrace of the generative potential of these technological innovations.[19] Cloud-based ed tech affords significant—if not unprecedented—opportunities to explore and strengthen connected learning frameworks. Broadly speaking, these new and emerging approaches to education recognize that much learning no longer occurs in classrooms but outside of formal school settings and, when learning does take place in school, it is often less hierarchical or standardized (for instance, through peer-to-peer instruction).[20] Cloud-based ed tech offers infrastructures that connect previously siloed spheres, bridging formal (classroom) and informal (home and social) spaces, as well as different interest groups or departments within schools (such as by offering highly interoperable platforms that facilitate opportunities for interdisciplinary studies).[21] These infrastructures also have implications for interactions that transcend any type of learning space; for example, students may develop new connections with tech providers as industry players (from Microsoft to Apple and iTunes University to Google and beyond) enter the cloud-based ed tech space and from there begin to forge relationships with students and their families across other spheres of life.[22]

The potential for such transcendent tech relationships—informed by tech providers' possession and use of student data—raises privacy concerns for various stakeholders. Indeed, a number of

---

[16] *See generally* Isaac Meister & Alicia Solow-Niederman, *K-12 Edtech Cloud Service Inventory,* BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (Jan. 15, 2014), http://cyber.law.harvard.edu/publications/2014/edtech_cloud_service_inventory [hereinafter SPI, *Cloud Service Inventory*].

[17] Unless otherwise indicated, all references in this whitepaper to actual ed tech products are meant for descriptive purposes only and should not be taken either as an endorsement or a criticism of the products by SPI. For a detailed taxonomy of the different types of cloud technologies in the educational space, please see SPI's *Cloud Service Inventory*. *See also CLIP Report* at 17-18 (offering another taxonomy).

[18] *CLIP Report* at 17.

[19] *See*, *e.g.*, Andrea Cascia, *Don't Lose Your Head in the Cloud: Cloud Computing and Directed Marketing Raise Student Privacy Issues in K-12 Schools*, 261 ED. LAW. REP. 883, 884 (2011) (explaining that "potential [cloud-based ed tech offers] for online educational applications is tremendous").

[20] *See* Mizuko Ito *et al.*, *Connected Learning Research Network, Connected Learning: An Agenda for Research and Design*, DIGITAL MEDIA AND LEARNING RESEARCH HUB 6-8 (Jan. 2013), http://dmlhub.net/sites/default/files/ConnectedLearning_report.pdf.

[21] *See*, *e.g.*, Cascia, *supra* note 19 at 884 ("Cloud-based ed tech means "that teachers can communicate with students twenty-four hours a day using any device with a connection to the Internet. Students may also be instructed to use online communication tools to collaborate with other students on projects.")

[22] *See*, *e.g.*, *id.* at 884-85.

constituencies—from parents to members of the United States Congress[23]—have voiced concerns about the extent to which data analytics and similar functions could yield a wealth of data about students that marketers might wish to mine for commercial use.[24] Concerns have also been raised around other privacy issues, including whether adequate "security measures" are required to protect student data and whether parents continue to have a meaningful "right to access" their children's records once they are in the cloud.[25] Researchers have confirmed that there is, in fact, a solid basis for many of these privacy concerns, which generally share the same animating objection: that going to school (which kids are legally required to do) should not be used essentially to force young people to turn over information about their private lives to non-educational institutions that might use it for their own ends, handle it carelessly, or aggregate and analyze it beyond the comprehension or control of students and their parents. According to one recent study, educational "[c]loud services are poorly understood, non-transparent, and weakly governed . . . [d]istricts frequently surrender control of student information when using cloud services . . . [and these] cloud service agreements generally do not provide for data security."[26] Despite these and similar weaknesses in the current generation of educational cloud computing arrangements, the efficiencies and innovative potential of cloud-based ed tech, not to mention the rapidly expanding ed tech market more broadly, suggest that they will remain a key part of the picture in schools and districts across the country.[27]

II. PAPER METHODOLOGY

This law and policy analysis will pursue its goal of exploring and elevating key privacy discussions for policy and decision-makers by focusing on a hypothetical product in the

---

[23] *See*, *e.g.*, Corinne Lestch & Ben Chapman, *New York Parents Furious at Program, inBloom, that Compiles Private Student Information for Companies that Contract with It to Create Teaching Tools,* N.Y. DAILY NEWS (Mar. 13, 2013), http://www.nydailynews.com/new-york/student-data-compiling-system-outrages-article-1.1287990; Natasha Singer, *Senator Raises Questions About Protecting Student Data*, N.Y. TIMES (Oct. 13, 2013), http://bits.blogs.nytimes.com/2013/10/22/senator-raises-questions-about-protecting-student-data/; Benjamin Herold, *Draft Overhaul of Federal Privacy Law Released by U.S. Senators Markey, Hatch*, Education Week (May 14, 2014), http://blogs.edweek.org/edweek/DigitalEducation/2014/05/draft_overhaul_of_federal_stud.html (highlighting key proposed reforms, such as "prohibit[ing] the use of personally identifiable student information for advertising").

[24] *See Response of Secretary Duncan to Letter of Sen. Markey* 4 (Jan. 13, 2014), http://www2.ed.gov/about/offices/list/om/docs/pirms/edrespmarkey.pdf [hereinafter *Duncan Response to Markey*] (responding to Markey's concern about whether there are limits on the ability of "private companies" to re-sell "student records" that schools have transferred to them). *See also* Natasha Singer, *Federal Regulators Seek to Stop Sale of Students' Data,* N.Y. TIMES (May 23, 2014), http://mobile.nytimes.com/blogs/bits/2014/05/23/federal-regulators-seek-to-stop-sale-of-students-data (reporting on bankruptcy of ConnectEDU, "a popular college and career planning portal in Boston," and the company's attempts to sell student data that it had collected).

[25] *Duncan Response to Markey* at 6-7.

[26] *CLIP Report* at Exec. Summary (finding "only 25% of districts inform parents of their use of cloud services, 20% of districts fail to have policies in place governing the use of online services, and a sizeable plurality of districts have rampant gaps in their contract documentation, including missing privacy policies.")

[27] *See, e.g.*, Dan Adiletta, *7 Innovators of Ed Tech to Watch: SXSWedu 2014* (Mar. 9, 2014), http://exitticket.org/7-innovators-of-edtech-watch-sxswedu-2014/ (describing some innovators in the cloud ed tech space); Jonathan Shieber, *Education Technology Start-Ups Raised Over Half a Billion Dollars in Q1*, TECHCRUNCH (Mar. 26, 2014), http://techcrunch.com/2014/03/26/education-technology-startups-raised-nearly-half-a-billion-dollars-in-q1/ ("judging by the increased pace of early-stage investment, venture capitalists are catching on" to the booming ed tech space). Of course, the strong likelihood that cloud ed tech will continue to take root across the country does not mean that every such offering will meet with success. *See, e.g.*, *supra* note 4 (describing collapse of inBloom).

educational cloud technology firmament: "Scholair." Scholair is meant to provide one point of entry into this vast universe of products. Scholair is not meant to cover all scenarios and is not offered as an exemplary model for schools' use of cloud computing; in fact, some of its value lies in capturing facets of a cloud-based ed tech product and implementation that might not be the most prudent but are happening—or could well happen—in schools and districts across the country. There are a range of potential approaches to cloud technologies that schools can take—as detailed further in SPI's K-12 Ed Tech Cloud Service Inventory—that come with their own advantages and challenges.[28]

First, this paper will describe Scholair and its implementation by a hypothetical school—Anywhereville Middle School ("AMS")—by summarizing a letter sent from the principal—Principal Smith—to parents of AMS students.[29] It will then turn to the significant questions of law, policy, and implementation implicated by Scholair's design and its proposed use by AMS, offering an analysis of these issues from various perspectives—including law, technology, and the social sciences. Depending on the specific matter at play, this analysis will include an explanation of why a given decision in the Scholair hypothetical strikes a desirable balance between student privacy and other interests or not, as well as potential options for improving upon undesirable product attributes or school decisions. In conclusion, this paper will distill a set of general suggestions that reflect the current policy environment as well as the current state of technology and current practices at the school and district level. These takeaways are offered at the level of pragmatic guidance for creating and implementing law, regulation, and policy, not at the level of overarching values or principles regarding the normatively desirable balances between student privacy, teacher and administrative autonomy, and technological innovation in schools. Such questions are the subject of consideration by the authors in other and future work.

III. SCHOLAIR HYPOTHETICAL

Everything in this section is hypothetical, but inspired by a number of real world scenarios.[30] Scholair is not a real product; AMS is not a real place; and Principal Smith is not a real person. The product and implementation plan described in the letter to parents (set forth in its entirety in Appendix A and summarized in the section below) that follows are designed to track real life, while also taking some license in order to provide a use case that captures key flashpoints in the K-12 cloud-based ed tech policy discussions and debates playing out across the country today.

> *We here at Anywhereville Middle School, USA (AMS), are excited to announce a partnership with Scholair, an educational technology company that provides three main services: it (1) stores student data in the "cloud"; (2) offers a dashboard that gives authorized users easy ways to input, access, and analyze this data; and (3) provides access to end-user software applications. Scholair is totally FREE for you and your child to use and comes at a very reasonable cost to the school. In addition, Scholair provides its customers with access to some applications ("apps") developed by third party app developers, who may charge a small fee.*

[28] SPI, *Cloud Service Inventory*.
[29] *See* Appx. A, *infra.* (containing full letter).
[30] *See generally* Part I, *supra.*

AMS will transfer to Scholair all data about current students that it either has on file, whether in hard copy or on existing databases, or adds in the future. Scholair will safely store all of your child's records on servers managed on behalf of Scholair by its third party service providers. Scholair will not combine data on AMS students with data it holds for other schools, except as described below.

Each student will have a virtual "cubby" that authorized users can access through the dashboard provided by Scholair. Scholair's software also gives us a unique learning opportunity: we can compare trends in our clusters and student body as a whole to those in other schools that store their data in Scholair. And Scholair offers a virtual library of educational software applications ("apps") to help your child learn.

We will be sending home permission slips for you to sign that authorize your child's teachers to select the apps that will go in your child's cubby. We ask you to review the details of Scholair's Terms of Use, Privacy, and other policies on Scholair's website.

IV. ANALYSIS OF SCHOLAIR

The analysis that follows focuses on three pressing questions—out of the larger universe of questions in this space—related to the adoption of cloud services in educational settings:[31]

- Who should decide whether to adopt ed tech;
- Whether parental consent is needed; and
- How best to secure student data in the service of protecting student privacy?

Discussion of the Scholair hypothetical will serve as the point of entry for exploring all these issues before broadening out to also consider real world data and examples.

1) Who Should Make Cloud Ed Tech Choices? Achieving Balance in Decision-Making

AMS's adoption of Scholair does not appear to be part of any coordinated plan or subject to any oversight at the district level. Instead, Principal Smith seems to be moving independently to use Scholair in his school and to give teachers considerable freedom to make their own cloud-based ed tech decisions by choosing apps from the Scholair library. While principals and teachers have a unique understanding of the needs of their individual schools and classrooms and should be afforded considerable decision-making autonomy so that they can experiment and tailor choices to local factors, the complexities of the legal, regulatory, and policy regime surrounding cloud technologies suggest that centralizing ed tech decision-making at the district level would likely be the more prudent course of action at this time.[32] As the cloud-based ed tech space continues

[31] *Cf. generally* Daniel Solove, *Interview with Kathleen Styles, Chief Privacy Officer, U.S. Department of Education,* LINKEDIN (Apr. 18, 2013), http://www.linkedin.com/today/post/article/20130417111651-2259773-interview-with-kathleen-styles-chief-privacy-officer-u-s-department-of-education (emphasizing that annual disclosures to parents required by FERPA should "'clearly explain who constitutes a school official and what constitutes a legitimate educational interest,'" as well as more broadly that "schools and districts should be clear about what student information they are collecting, how they are protecting it, and what they are doing with it.")

[32] This was a point of rough consensus among participants in the November 2013 Berkman working meeting—co-organized with CoSN—on student privacy. SPI, *Student Privacy and Cloud Computing* at 3. *See also CLIP Report* at 70-71 ("Districts should also have employee computer use policies that bar employees from using cloud services

to evolve—in terms of factors such as available technologies, clarity of applicable legal, regulatory, and policy regimes, and various constituencies' comfort with the cloud—the optimal point along the sliding scale between centralization and decentralization is likely to move. Early indicators suggest, however, that absent centralization during this initial phase of cloud-based ed tech, school administrators and classroom teachers might inadvertently run afoul of requirements such as those imposed by the Children's Online Privacy Protection Act ("COPPA") or other legal schemes and regulatory regimes.[33] (As will be discussed further below, Principal Smith's planned use of Scholair does indeed run up against several important legal and regulatory requirements.)

At this moment in the evolution of cloud-based ed tech, districts are typically better positioned than their member schools to devote the time and resources to such vital tasks as understanding the legal and regulatory requirements around the adoption of these technologies; developing and overseeing policies that comport with these requirements as well as fulfill the needs of the district and the various constituencies within it; negotiating contracts with cloud providers that comply with all relevant laws, regulations, and policies; and monitoring and ensuring data security.[34] For example, some of these functions are likely to require consultation with legal counsel, who is typically retained at the district level rather than the school level.[35] Some will also require the technological expertise and sophistication that a district-wide Chief Information Officer ("CIO"), Chief Technical Officer ("CTO"), Chief Privacy Officer ("CPO"), or a similar official could bring to the table.[36]

If the cost of such a position is prohibitive, districts could consider having a part-time administrator, group of administrators (who each take on some components of the CIO / CTO role), or outside consultant in such a position.[37] Local and state law and policymakers might want to consider requiring—through statute, ordinance, regulation, or similar method—that districts adopt ed tech policies that effectuate such centralization. Any such requirement,

---

not approved by the districts. Without such policies, teachers are likely to inadvertently compromise student privacy.")

[33] *See CLIP Report* at 24 (finding that "approximately 20% of the responding districts had no policies addressing teacher use of information resources . . . For example, if a school principal or teacher decided to use a service such as Dropbox for students to share family photos, the central administration would not have the opportunity to vet the terms and conditions of the service and would not have the ability to ensure COPPA compliance.") Note that policies don't in and of themselves ensure compliance. *CLIP Report* at 66 (cautioning that "even in districts with policies, the degree of compliance is not known").

[34] *Cf. CLIP Report* at 67-71 (setting forth recommendations on contract terms for "school districts, policymakers, and vendors to consider," noting that often "districts are passive parties to cloud service contracts," and urging both "service providers and districts to play closer attention to privacy issues and obligations [in contracting].")

[35] *See* PTAC, *Best Practices* at 13 (advising schools and districts that it is "always a best practice to consult legal counsel to determine the applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers.")

[36] *See also CLIP Report* at 71 (recommending that states and "larger districts and those with extensive cloud networks and intensive data transfers" have Chief Privacy Officers); Greg Mortimer *et al.*, Remarks at South by Southwest EDU: Data Privacy: What Parents DON'T Know Can Hurt You (Mar. 4, 2014). *Cf.*, *e.g.*, *Gov. Cuomo and Legislative Leaders Announce Passage of 2014-2015 Budget*, SAUGERTIES POST STAR (Apr. 1, 2014), http://www.poststarnews.com/article/20140401/NEWS/140409981/?Start=4 (budgeting for Chief Privacy Officer for New York State Department of Education).

[37] Such an approach was discussed by participants at a December 2013 workshop convened by Fordham CLIP in advance of its report release.

however, should encompass ongoing dialogue and close collaboration with school-level administrators and faculty so that centralized decisions reflect the valuable, informed perspective of those members of the educational community who regularly interact with students.[38] Of course, even with this multi-lateral approach, there are potential costs of centralization that also need to be taken into account. Tradeoffs in the near term may include a decrease in school level control and freedom to innovate, as well as an increase in the time it takes for promising new technologies to roll out in the classroom.[39]

Over time, as the collective knowledge base regarding cloud-based ed tech grows more robust, it may become both adequate and desirable to shift more decision-making safely to the level of the school and / or classroom. Such decentralization—or at least the possibility of a less centralized model—might ultimately better realize educational and efficiency gains from having front-line administrators and faculty members make ed tech decisions. Anticipating shifts of this sort, current legal, regulatory, or policy requirements established for centralization might be equipped with a "sunset provision" to ensure periodic reviews of any arrangement as a formal requirement of centralization may become less necessary. For example, a district, group of districts, state, geographic region, or other collaborative unit could band together to create "app stores" or "app catalogues" (to the extent that proprietary concerns might make an actual store difficult) for administrators and / or teachers.[40]

Under such a model, the appropriate CTO / CIO (or group of CTOs / CIOs)—in consultation as needed with legal counsel or other relevant experts—could vet all the apps based on an agreed-upon methodology prior to their inclusion in the store and continue to monitor them for compliance with best practices, such as model contract terms, data security protocols, and other

[38] Even at moments such as these when the sliding scale of centralization / decentralization appears to be optimized toward the centralization end, it seems imperative to preserve space for local experimentation and innovation. For instance, a school or district might wish to offer a weekly forum or message board where teachers can share ideas with the CIO, CTO, or similarly positioned individual(s). *See generally* edSurge, *#Edtechchat Turns 'One'* (May 20, 2014), https://www.edsurge.com/n/2014-05-20-edtechchat-turns-one ("Perhaps most important, the #edtechchat community wants administrators to foster risk-taking cultures" in schools.)

[39] Centralization of decision-making could also affect smaller ed tech firms' ability to enter the market. On the one hand, these companies may be in a position to be more nimble in their contracting terms and therefore able to respond to districts' needs and requests, which could facilitate their entry. On the other, they are likely to have less name recognition, which risks their being overlooked by administrators in favor of more well established counterparts. *Cf.* Keith Wagstaff, *Classroom 2.0: Can Teachers Take Advantage of the Ed Tech Boom?*, NBC NEWS (May 5, 2014), http://www.nbcnews.com/tech/tech-news/classroom-2-0-can-teachers-take-advantage-ed-tech-boom-n97171 (noting that "'schools have a special social responsibility, and that effects how much experimentation they are willing to tolerate.'")

[40] This idea was floated at the November 2013 Berkman working group meeting (co-organized with CoSN) but did not achieve rough consensus. Meeting participants discussed both pros and cons of this type of approach. *See generally* SPI, *Student Privacy and Cloud Computing* at 8. CLIP suggested a similar concept, though not at the level of the app store: "districts need to have an easy means such as a web portal for teachers to identify approved services or to request approval to use new tools." *CLIP Report* at 71. Industry providers of apps to kids (both inside and outside of schools) have also been innovating around the use of specific portals or sections of stores for the youth market. *See*, *e.g.*, Sarah Perez, *Introducing Apple's New "Kids" App Store*, TECH CRUNCH (Sept. 22, 2013), http://techcrunch.com/2013/09/22/introducing-apples-new-kids-app-store/ (announcing launch of Apple's Kids App Store).

vital components of privacy-respecting ed tech.[41] Individual administrators and / or teachers could then use any apps that the store permitted them to access. For instance, high school teachers would likely have access to more app choices than their colleagues at the middle and elementary schools because COPPA requirements do not apply to children over age 13.[42]

Putting together this type of fully vetted ed tech app store would be labor intensive, as well as require thorough understanding of the relevant legal and regulatory requirements along with thoughtful creation of appropriate standards to assess apps. If done well, this sort of investment might realize a number of possible benefits. Among others, such an app store could reduce on-going transaction costs (since teachers would not have to ask the CIO / CTO each time they wanted to use something new, although they would of course need to continue to be vigilant about appropriately implementing any vetted apps they chose to use); promote school and teacher control over their educational spaces (since individuals at the school and classroom level could experiment with apps best-suited for their particular contexts); and incentivize ed tech innovation that comports with legal, regulatory, and policy requirements (since vendors would ostensibly want to develop apps that would be included in such vetted stores, thereby fostering competition to create both innovative and privacy-conscious products).

2) When Is Parental Consent Needed? Unpacking Law, Policy, & Best Practices

A. Clarifying Statutory Consent Requirements

Principal Smith's plans for Scholair are poised to run afoul of several provisions of key federal laws—FERPA, COPPA, and PPRA—and accompanying regulations that control when schools and districts need parental consent to use ed tech as opposed to when educators and administrators may make such decisions on their own. Note that none of these legal schemes were developed for ed tech generally or cloud-based ed tech in particular; rather, they all apply more broadly to educational settings and / or website operators that make services available for use by children. Translating them to the ed tech realm has not typically been a smooth, straightforward process for the various ed tech stakeholders.[43] The consent issues raised by AMS's proposed use of Scholair are described below according to the legal regime with which they come into tension, followed by a discussion of how the overarching legal principle of having parents consent to disclosure of their children's private information—unless a specific exception applies such that lawmakers and regulators have effectively substituted their judgment for parental consent and deemed such disclosure safe for children—might be more meaningfully effectuated.

---

[41] *Cf. also* CoSN, *Toolkit* at 18 (suggesting that a school could "have legal counsel create a rider containing the School System's minimum requirements and obligations that teachers or other employees can give to providers to sign before utilizing their services [through clickwrap agreements].")

[42] *See* Dalia Topelson *et al.*, *Privacy and Children's Data: An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act,* BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY 7 (Nov. 13, 2013), http://cyber.law.harvard.edu/publications/2013/privacy_and_childrens_data [hereinafter Cyberlaw Clinic, *FERPA/COPPA Guide*].

[43] *See*, *e.g.*, Cascia, *supra* note 19 at 891-99.

→ Family Educational Rights and Privacy Act ("FERPA")

Much of the data AMS proposes to store in Scholair —including, but not limited to, students' names and disciplinary histories—qualifies as "education records" under FERPA (although in other contexts the status of student data as "education records" may be less clear cut).[44] AMS teachers and school officials need to access "personally identifiable information" ("PII") about students from these records in order to do their jobs. Common types of PII include students' names, addresses, birthdays, and Social Security Numbers, as well as any other facts that would make it possible for an average person in a given community to figure out a student's identity.[45] As a general rule, whenever AMS faculty or administrators want to share PII about students outside of AMS, they need to obtain parental consent ahead of time.[46] Parental consent must be written and specify which PII is being disclosed, to whom, and why.[47] Certain types of PII—such as students' names and email addresses—constitute "directory information."[48] AMS does not need parental consent to share this limited category of PII, although they do need to give parents the ability to "opt-out"—within a reasonable time frame—of having their kids' information included in any directory.[49] In this case, Principal Smith has not requested consent from parents to share students' PII with Scholair, nor has he given information about how to opt-out of sharing the "directory information" subset of PII.

Now, this "directory information" exception might not come into play here because Principal Smith is presumably relying on the "school official" exception to FERPA's consent requirement to transfer students' non-directory PII to Scholair.[50] Under this exception, if AMS is outsourcing

---

[44] *See* Family Educational Rights & Privacy Act (FERPA), 20 U.S.C. § 1232g(a)(4)(A) (2012). For a comprehensive overview of FERPA's provisions, please see Cyberlaw Clinic, *FERPA/COPPA Guide. See also* Cascia, *supra* note 19 at 891-99. At this point in time, FERPA is forty years old. 20 U.S.C. § 1232g (2012). In light of its age, coupled with the rapidly changing ed tech landscape, policy and decision-makers at all levels have been giving serious consideration to whether and how FERPA might need to evolve going forward. *See*, *e.g.*, Senator Ed Markey's Office, *Press Release: Markey, Hatch Release Discussion Draft of Legislation Addressing Student Privacy* (May 14, 2014), http://www.markey.senate.gov/news/press-releases/markey-hatch-release-discussion-draft-of-legislation-addressing-student-privacy (focusing FERPA reform on "need to protect students, provide tools to parents when information shared with third parties").

[45] Cyberlaw Clinic, *FERPA/COPPA Guide* at 9. Non-PII is not protected by FERPA, thus schools that wish to restrict ed tech providers' use of non-PII must do so through contractual terms that reflect recommended good practices. *See generally* CLIP Report at 68.

[46] Cyberlaw Clinic, *FERPA/COPPA Guide* at 3.

[47] *Id.*

[48] *Id.* at 6.

[49] *Id.* at 5. *See also* PTAC, *Best Practices* at 3-4 ("While the directory information exception can seem to be an easy way to share PII from education records with providers, this approach may be insufficient for several reasons . . . schools and districts may not find this exception feasible for disclosing PII from education records to providers to create student accounts or profiles.")

[50] *See generally* Daniel Solove, *Interview with Kathleen Styles, Chief Privacy Officer, U.S. Department of Education,* LINKEDIN (Apr. 18, 2013), http://www.linkedin.com/today/post/article/20130417111651-2259773-interview-with-kathleen-styles-chief-privacy-officer-u-s-department-of-education; *Frequently Asked Questions—Cloud Computing,* PRIVACY TECHNICAL ASSISTANCE CENTER, U.S. DEPARTMENT OF EDUCATION 4 (June 2012), http://ptac.ed.gov/sites/default/files/cloud-computing.pdf [hereinafter PTAC, *FAQ Cloud Computing*] ("While FERPA does not directly address the viability of specific cloud solutions, the [U.S.] Department [of Education] recognizes that their use is a growing trend and is beginning to pilot its own cloud computing solutions."); *The Family Educational Rights and Privacy Act: Guidance for Parents,* U.S. DEPARTMENT OF EDUCATION 3 (Feb. 2011), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/for-parents.pdf ("Although the term 'school official' is not defined in the statute or regulations, this Office generally interprets the term to include parties such as . . . a contractor,

services to a third-party service provider (in this case, Scholair) who is under the school's "direct control" and performing services for which school officials would otherwise be responsible,[51] AMS does not need parental consent—as long as Scholair isn't turning around and sharing the PII with anyone else or using it for purposes beyond the scope of those for which AMS gave Scholair the PII in the first place.[52] If any one of these three factors—direct control, otherwise done in-house, no re-sharing—is not met, then the outsourcing exception does not apply, and parental consent is required to share PII.[53]

On the surface, Principal Smith's plans for Scholair seem to fall nicely under the school official exception: AMS is having a third-party (Scholair) do work that teachers and administrators would otherwise do themselves, and the school has put (some) restrictions in place on what Scholair can do with the student data it gets from the school. However, closer inspection reveals that this exception does not apply seamlessly.

First, from the notice, it is unclear whether Scholair is under the "direct control" of AMS. Smith's letter talks about "partnering" with Scholair, but does not elaborate on what that phrase means. There is nothing in the letter to indicate that AMS has any control over what Scholair can do with the information it will be storing on behalf of AMS; most significantly, the letter does not state whether there is a negotiated contract in place between AMS and Scholair. Indeed, Smith's request that parents read Scholair's Terms of Use, privacy policy, and other policies strongly suggests that no negotiated contract is in place. If AMS in fact had control over Scholair in the form of a negotiated contract, then the contract between AMS and Scholair—rather than Scholair's policies—would control Scholair's actions with respect to AMS students' information. Such a negotiated contract should specify what Scholair can or can not do with the students' data (with FERPA compliance as a baseline contractual requirement), as well as give AMS the ability to enforce certain behaviors by Scholair, such as refraining from any data mining that is not under AMS's control.[54]

---

consultant, volunteer or other party to whom the school has outsourced institutional services or functions."). It is also possible that AMS is relying in part on the FERPA exception for "organizations conducting studies on behalf of the educational agency or institution" to the extent that Scholair is engaged in data analytics of "trends in our [AMS] clusters and student body as a whole." However, such reliance would appear to be misplaced; "[t]o be in compliance, these studies must be conducted in order to develop, validate, or administer predictive tests, administer student aid programs, or improve instruction." *CLIP Report* at 7. Note also that valid use of this exception requires that "information disclosed to such vendors remains confidential and there is a schedule for deletion of such records following the completion of the stated purpose." *CLIP Report* at 7. *See also* PTAC, *Best Practices* at 3-4.

[51] *See*, *e.g.*, Cascia, *supra* note 19 at 896 ("For example, a school district may not use this [outsourcing] exception to disclose education records, without consent, to a company that provides a student discount on services that the school would not otherwise provide. The department [of education] created this section to 'prevent uncontrolled designation of outside parties as "school officials" for marketing and [certain] other purposes . . .'") (internal references omitted).

[52] Cyberlaw Clinic, *FERPA/COPPA Guide* at 5-6.

[53] The U.S. Department of Education "commonly refers to this exception to the requirement of consent in FERPA as the 'school official' exception [34 C.F.R. § 99.31(a)(1)]" because the exception allows a third party to do work that school officials would normally do. PTAC, *FAQ Cloud Computing* at 2.

[54] *See CLIP Report* at 68. Other terms should include the "specification of the types of data transferred [to] or collected [by]" Scholair, as well as the guarantee that Scholair would not try to get parents to agree to any privacy terms other than those agreed upon in the contract between AMS and Scholair. *Id.* at 69. For detailed recommendations on contractual terms, see *CLIP Report* at 67-70 and CoSN, *Toolkit* at 15-17.

Second, Scholair has reserved the ability to re-share student data, in encrypted form, with third-party providers of its choosing—the identities of which might change anytime—as necessary to provide the services described in the letter. To the extent that the re-shared data is actually de-identified (as in the case of Scholair's proposed use of third-party servers to store encrypted, de-identified data), then no violation of the prohibition on re-sharing occurs.[55] But "[d]e-identification of data is a tricky process . . . there is no statutorily approved method for de-identifying FERPA protected information."[56] Thus to the extent that the data is not de-identified (as in the case of Scholair's proposed use of as yet unspecified third parties to "identify opportunities for further educational growth and development for all members of the AMS community"), then this re-sharing by Scholair would render the school official exception inapplicable. Moreover, the very real possibility of re-identification raises reasonable doubt about whether any data is ever truly de-identified without eliminating its utility.[57] The fact that the identities of the receiving third parties are subject to change anytime amplifies these concerns.[58]

→ Children's Online Privacy Protection Act ("COPPA")

Although Principal Smith's letter is not explicit on this point, Scholair appears to be a commercial enterprise (AMS will have to pay a fee for Scholair's services). Because Scholair is a for-profit company that will collect some "personal information" ("PI") directly from kids under 13,[59] Scholair is required under COPPA to obtain parental consent before getting this information—unless an exception applies.[60] COPPA's definition of PI is quite broad (and not

[55] *See* CoSN, *Toolkit* at 12.
[56] CoSN, *Toolkit* at 12.
[57] *See also* CoSN, *Toolkit* at 12 (flagging that U.S. Department of Education "Chief Privacy Officer Kathleen Styles cautions 're-identification risk is a very real risk. You can't just take off somebody's name and say that the record is anonymized.") *See generally* Arvind Narayanan and Vitaly Shmatikov, *Robust De-Anonymization of Large Datasets (How to Break Anonymity of Netflix Prize Dataset)*, THE UNIVERSITY OF TEXAS AT AUSTIN (Feb. 5, 2008), http://arxiv.org/pdf/cs/0610105.pdf ("demonstrat[ing] that an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber's record in the dataset."); L. Sweeney, *Matching Known Patients to Health Records in Washington State Data*, DATA PRIVACY LAB, IQSS, HARVARD UNIVERSITY (June 1, 2013), http://privacytools.seas.harvard.edu/publications/matching-known-patients-health-records-washington-state-data (demonstrating potential for re-identification in large data sets with sensitive information); Adam Tanner, *Harvard Professor Re-identifies Anonymous Volunteers in DNA Study*, FORBES (Apr. 25, 2013), http://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/ (describing how researchers at Harvard's Data Privacy Lab re-identified 40% of supposedly anonymous volunteers in a high-profile study).
[58] In addition to the parental consent issue, there's a parental access issue: if students' data goes from Scholair to unknown other third parties, then parents aren't able to exercise the right FERPA gives them to access, review and, if appropriate, request amendment of students' records. *See* Cyberlaw Clinic, *FERPA/COPPA Guide* at 3.
[59] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6 (1998). Providers subject to COPPA are those whose services are "directed to children under thirteen years of age that collect [] personal information from children" or whose services are for a "general audience" but have "actual knowledge" of getting "information from children under thirteen years of age." Cyberlaw Clinic, *FERPA/COPPA Guide* at 7-8. *See also* David R. Hostetler & Seiko F. Okada, *Children's Privacy in Virtual K-12 Education: Virtual Solutions of the Amended Children's Online Privacy Protection Act (COPPA) Rule*, 14 N.C. J.L. & TECH. ON. 167, 188 (2013) (explaining that for-profit "app developers and website operators targeting K-12 education are now subject to COPPA, just like other commercial app developers and website operators.")
[60] Exceptions to prior parental consent include contacting kids "as reasonably necessary to protect the safety of a child participant on the website." Types of approved "verifiable" parental consent include written, electronic, and other methods. Cyberlaw Clinic, *FERPA/COPPA Guide* at 11, 16.

equivalent to the definition of PII under FERPA), and includes names, addresses, Social Security numbers, IP addresses, photos and "any other information that permits the physical or online contacting of a specific individual."[61]

The Federal Trade Commission has stated that teachers "may act in place of a parent in deciding whether to give consent" to commercial cloud providers who will obtain PI from students under 13.[62] Upon first glance, then, it appears that Scholair may well be able to rely on AMS teachers to give consent for their students' use of Scholair and the apps available in its library instead of having to get consent directly from parents.[63] To the extent that Scholair and its associated app developers plan to "collect data for limited purposes of internal school [AMS] use,"[64] they are on solid ground if they rely on AMS teachers' consent instead of parental consent.[65] (Note that this terrain would be firmer still if instead of AMS asking parents to sign permission slips for teachers to choose apps, the permission slips asked for thoroughly informed parental consent to have the app developers collect information directly from students.)[66] But Principal Smith's letter suggests that Scholair and the developers will go beyond data collection for internal AMS use. There is no stated limit on what developers will do with the data; indeed, Scholair plans to analyze student data provided by its member schools across the country. Thus upon final review, it does not appear that Scholair can in fact rely on teachers' consent as a substitute for parental consent for the purposes of COPPA.[67]

---

[61] Cyberlaw Clinic, *FERPA/COPPA Guide* at 9. Note that the current definition of PI became effective only recently—July 1, 2013—and "greatly expand[ed]" the previous definition. *See* Hostetler & Okada, *supra* note 59 at 185.

[62] *FTC—How to Protect Kids' Privacy Online: A Guide for Teachers,* BETTER BUSINESS BUREAU NEWS CENTER (Dec. 1, 2002), http://www.bbb.org/us/article/ftc--how-to-protect-kids-privacy-online-a-guide-for-teachers-4550. *See also Complying with COPPA: Frequently Asked Questions*, BUREAU OF CONSUMER PROTECTION BUSINESS CENTER (April 2014), http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions [hereinafter *Complying with COPPA FAQ*].

[63] Teachers are supposed to serve this role pursuant to the policies of the district in which they teach. *See FTC—How to Protect Kids' Privacy Online*, *supra* note 62; *Complying with COPPA FAQ* M(3). *Cf. also* Hostetler & Okada, *supra* note 59 at 170, 191-92 (expressing frustration that "[t]he COPPA framework, including the amended Rule [effective July 1, 2013] . . . fails to give any special attention to children's online privacy threats in virtual education . . . the amended Rule continues, after more than a dozen years, in failing to define the role of school officials acting as parental surrogates in providing consent for children's information being collected by website operators and mobile application ("app") developers.") To some extent, the FTC addressed such concerns via updated FAQs in April 2014. *See Complying with COPPA FAQ.* Note that COPPA is concerned with websites' obtaining information directly from children, so COPPA would not apply to school administrators' use of commercial web services—even if the information these administrators share concerns children under 13. Cyberlaw Clinic, *FERPA/COPPA Guide* at 7.

[64] Hostetler & Okada, *supra* note 59 at 170.

[65] *See Complying with COPPA FAQ* M(1)-(2).

[66] The kind of transparency necessary to achieve fully informed parental consent is discussed in more detail below in the sub-section on Challenges & Opportunities of the Current Consent Standard.

[67] Scholair and other ed tech providers also should be mindful of parents' right to opt their children's PI out of further use by the provider, even if parents give initial consent for the PI to be used. *See* COPPA, 15 U.S.C. § 6502(b)(1)(B)(ii).

→ Protection of Pupil Rights Amendment ("PPRA")

AMS might also be on shaky ground with provisions of PPRA. If students at AMS are asked questions about "protected information" ("PrI")[68] on a survey that is funded—to any extent—by the U.S. Department of Education, prior written parental consent is required.[69] PrI includes, but is not limited to, information from students about "sex behavior or attitudes," "mental or psychological problems" that they or their families have, or "demeaning behavior" that they exhibit.[70] Principal Smith's letter leaves open the potential that some of the library apps—notably the ones "available to help your child learn 'soft skills,' such as forming healthy friendships and dating relationships"—might constitute a survey of PrI. His letter is silent on whether AMS will put any federal Department of Education funds toward Scholair and associated apps, but if it does, then parental consent for any survey of PrI would be necessary.

Even if no federal funds are involved, it appears that parents still have the right under PPRA to obtain notice of and "opt out" their children from "activities involving the collection, disclosure, or use of personal information obtained from students for marketing, sale, or for other distribution of the information to third parties."[71] Principal Smith's letter is conspicuously silent on whether Scholair, the associated app developers, or Scholair's third-party sub-contractors will use the information for marketing or other prohibited purposes.[72] At the very least, it is likely that AMS has not contractually bound Scholair to refrain from such activities.[73] AMS parents thus may have the right to opt out their children from supplying PrI for inclusion in marketing or similar activities—a right that was not mentioned in Principal Smith's letter.

Commercial use of student data by cloud providers or third parties to whom providers re-disclose data—for example, to create personalized online advertisements aimed at children—is one of the core concerns shared by parents, advocacy groups, and some lawmakers and regulators.[74] The

---

[68] This paper uses the abbreviation PrI to avoid confusion with PI ("personal information"). In other contexts, "protected information" might be abbreviated as "PI."

[69] *See* Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. § 1232h(b) (2002). *See Model Notification of Rights Under the Protection of Pupil Rights Amendment (PPRA)*, U.S. DEPARTMENT OF EDUCATION 1 (May 26, 2006), http://www2.ed.gov/policy/gen/guid/fpco/pdf/modelnotification.pdf. Consent must be written. PPRA, 20 U.S.C. § 1232h(b). *See also* PTAC, *Best Practices* at 3.

[70] *See Model Notification of Rights Under the Protection of Pupil Rights Amendment (PPRA)*, U.S. DEPARTMENT OF EDUCATION 1 (May 26, 2006), http://www2.ed.gov/policy/gen/guid/fpco/pdf/modelnotification.pdf.

[71] *CLIP Report* at 8. *See* PPRA, 20 U.S.C. §§ 1232h(c)(2)(A)(ii) & (C)(i). *See also Duncan Response to Markey* at 5 ("[PPRA] also provides parents with rights with regard to some marketing activities . . . PPRA also requires, with limited exceptions, school districts to develop and adopt policies, in consultation with parents, governing the collection, disclosure, or use of personal information collected from students for marketing purposes.")

[72] To the extent that they are just using it for the "exclusive purpose of developing, evaluating, or providing education products or services for, or to, students or educational institutions," PPRA does not seem to provide parents with any notice or opt-out rights because the relevant local educational agency of which AMS is part would not be required to have policies in place around marketing or selling PrI. *See* PPRA, 20 U.S.C. §§ 1232h(c)(4)(A).

[73] *See CLIP Report* at Exec. Summary (stating that "fewer than 7% of the contracts restrict the sale or marketing of student information by vendors, and many agreements allow vendors to change the terms without notice. FERPA, however, generally requires districts to have direct control of student information when disclosed to third-party service providers.")

[74] *See*, *e.g.*, *Duncan Response to Markey* at 4-5 (stating that the U.S. "Department [of Education] shares your concern about commercialization of student data, and intends to provide guidance . . . [that] will clarify the following key points. When a school or district discloses or re-discloses FERPA protected data to contract out for

reasons for these concerns vary; some are rooted in principled normative commitments to keep educational spaces free from commercial influence, whereas others are more pragmatic, arising from concern about children's unique impressionability and vulnerability to commercial speech directed at them.[75] Despite these varying perspectives, many—although not all—stakeholders in the cloud ed tech space likely would agree that children's data should not be treated the same as adults' in regulation of commercial activities, such as advertising; however, there is by no means a consensus regarding the proper boundaries of the permissible approach to commercial content aimed at children.[76] At minimum, it seems that greater PPRA adherence and enforcement could help to protect parents' right to know about and opt their kids out of marketing or similar activities.[77] It also might be worthwhile to explore the feasibility and utility of an affirmative "opt-in" regime under which a student's data could be used for marketing or other commercial purposes only after her parents had given affirmative consent.[78]

B. Challenges & Opportunities of Current Consent Standard

Principal Smith's letter reflects some confusion on the part of the school—and likely Scholair too—about when parental consent is needed to share data with a third-party cloud ed tech provider. Such confusion is also rampant in the real world, in part due to some lack of clarity in federal laws and regulations—notably FERPA and COPPA—over when exceptions to the parental consent standard apply. This ambiguity is not productive; such murkiness may not only hinder industry innovation, but also impede school and district efforts to adopt innovative cloud-based ed tech in a way that conforms to consent requirements.[79] It also risks exposing students' private information to disclosures that their parents do not want and about which they might be unaware. However, imposing consent requirements that are too monolithic or cumbersome—for instance, saying that schools cannot use third-party vendors in any circumstance unless parents give consent—risks producing significant inefficiencies for schools, districts, and ed tech

---

certain services, its contractors never 'owns' the data . . . [contractor can use FERPA protected data to develop products for school use but not for outside school or for marketing].")

[75] *See*, *e.g.*, Common Sense Media, *School Privacy Zone Campaign* (last visited on May 13, 2014), https://www.commonsensemedia.org/school-privacy-zone (articulating principle that "students' personal information or online activity shall not be used to target advertising to students or families"); *Senate Hearing on Children's Online Privacy*, TECH LAW JOURNAL (Sept. 24, 1998), http://www.techlawjournal.com/privacy/80923.htm (quoting Sen. Bryan, one of the main sponsors of COPPA, as explaining that "'children by their very nature are honest and trusting, and when approached on the Internet by their favorite cartoon, or offered the chance to win a prize or to participate in some kind of a contest, children will provide very personal and private information. Children under the age of twelve years old are not likely to have the judgment to know what is appropriate.'"). *See generally* Caroline Knorr, *Sneaky Ways Advertisers Target Kids*, COMMON SENSE MEDIA (Jan. 28, 2014), http://www.commonsensemedia.org/blog/sneaky-ways-advertisers-target-kids (listing stealth techniques advertisers use to reach youth audiences through social media and other outlets).

[76] *See generally* SPI, *Student Privacy and Cloud Computing* at 7-8 (identifying need for "shared culture and conversation of trust" around cloud ed tech issues).

[77] *See*, *e.g.*, *Duncan Response to Markey* at 5 ("[PPRA] also provides parents with rights with regard to some marketing activities . . . PPRA also requires, with limited exceptions, school districts to develop and adopt policies, in consultation with parents, governing the collection, disclosure, or use of personal information collected from students for marketing purposes.")

[78] *See generally* SPI, *Student Privacy and Cloud Computing* at 4.

[79] *See generally id.*

providers, as well as potentially precluding the important use of digital technologies for teaching and learning purposes.[80]

The challenge around parental consent, then, is preserving and protecting the innovative potential underlying cloud-based ed tech without either cutting parents out of the loop or having students' data follow a path where parents do not know exactly where it will end up or how it will ultimately be used. To address this challenge, one potential addition to the legal and regulatory toolbox that warrants serious consideration is for ed tech providers to provide standardized, user-friendly labeling of their products, along the lines of a nutrition label. Such a scheme could be the result of enacting new federal statutory and accompanying regulatory requirement to this effect or adoption of a voluntary system, either instead of or as a precursor to a mandated system.[81] Such labeling could be required to include an up-to-date list of all student data that an ed tech company collects, all uses to which the ed tech company puts this data (including, but not limited to, any form of advertising or marketing), and the identities of all third-parties (sub-contractors, app developers, etc.) with which the company has relationships.[82] This labeling might also facilitate school and district understanding of a given company's activities in order to make more informed and efficient determinations as to when parental consent would be required for student data to be shared with that company, as well as to better develop other essential terms of their agreement with that cloud provider.[83] It could also potentially both help parents monitor whether or not they should be asked for their consent for the use of ed tech products at their

---

[80] *See generally* Ito *et al. supra* note 20 at 12 (noting importance of "online platforms and digital tools" for innovative connected learning approaches).

[81] This suggestion was discussed at the Berkman Center (co-organized with CoSN) November 2012 working meeting; however, no consensus was reached around its desirability. SPI, *Student Privacy and Cloud Computing* at 5. Those who raised the suggestion were drawing on previous research on the concept of privacy labeling more broadly outside of the specific ed tech context. *See*, *e.g.*, Kashmir Hill, *Is It Time for Privacy Nutrition Labels?*, FORBES (Mar. 23, 2011), http://www.forbes.com/sites/kashmirhill/2011/03/23/is-it-time-for-privacy-nutrition-labels/; Patrick Gage Kelley *et al.*, *A "Nutrition Label" for Privacy*, CARNEGIE MELON UNIVERSITY (2009), http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf; Asa Raskin, *Privacy Icons*, MOZILLA FOUNDATION (2010), http://www.w3.org/2010/api-privacy-ws/slides/raskin.pdf. *Cf.*, *e.g.*, Common Sense Media, *Learning Ratings*, http://www.commonsensemedia.org/learning-ratings (setting forth ranking system for use by parents and schools for identifying "fun and educational apps and games"). The CLIP Report makes recommendations around transparency—such as having districts post identities of third-party service providers and the arrangements with those providers conspicuously on district websites—but it does not go as far as this labeling requirement. *CLIP Report* at 67. Some districts are experimenting with user-friendly labeling for parents around data security concerns. *See*, *e.g.*, Houston Independent School District, *Software Ratings for Parents*, http://www.houstonisd.org/Page/109830 (classifying websites used in the district according to "low, medium, and high" categories of data security).

[82] *Cf. generally* PTAC, *Data Sharing Under FERPA*, Slide 22 (Jan. 11, 2012 & May 2013), http://ptac.ed.gov/sites/default/files/webinar-data-sharing-011112_final_0.pdf (outlining the basic "who, what, why" questions necessary for data sharing agreements to comport with best practices under FERPA).

[83] *See CLIP Report* at 24-25 (finding that "districts were rarely in control of the terms and conditions of data transfers. Vendors typically presented the school districts with standard form contracts that would often contain misleading or inappropriate provisions . . . vendors sometimes include clauses allowing the vendor to share data with affiliates without committing those affiliates to any privacy protections . . . vendor agreements would often grant the vendor the right to modify the terms and conditions at the vendor's discretion—and often without direct notice to end users and district-based systems administrators. In other words, districts legally relinquished the ability to comply with FERPA.") *See generally* Gasser, *Cloud Innovation* at 17 ("In the cloud context, *contracts* have played a particularly important role in embracing (and absorbing) some of the challenges associated with the technological innovation.")

child's school or district and streamline governmental oversight of ed tech products. Of course, any labeling requirement must be thoughtfully vetted so as to include a reasonable amount of relevant information to render the label both meaningful and manageable; it is also likely to require a corresponding compliance and enforcement scheme to make the labeling regime effective.

The topic of labeling is far from purely academic. In fact, the U.S. Department of Education recently reiterated its concern about unauthorized re-disclosure of student data by third party service providers and highlighted government penalties for such violations: "if while investigating a complaint [about reasonable methods of data access controls] we find that a third party re-disclosed PII from education records it received from a school or district in violation of FERPA, the Department could require the school or district to not allow the third party responsible for the improper re-disclosure access to PII from education records for at least five years."[84] Such investigations might become more efficient if standardized, user-friendly labeling were required.[85] More generally, greater transparency around the (re-) use of data might result in fewer complaints and reduce the need for ex post investigation.[86]

Such a shift might occur for two primary reasons. Districts would have easier access to more comprehensive information about cloud-based ed tech products up-front, which might enable them to make more informed decisions that would in turn avoid unwelcome surprises after a technology or service had already been adopted. Also, if cloud providers were required to share their activities in this area in such a user-friendly, public manner, then they might be incentivized by the promise of greater market share and avoidance of negative publicity to take even more responsibility to self-monitor their sub-contracting and other activities for compliance with FERPA and other legal regimes.[87] New responsibilities for ed tech companies would be time-consuming, of course, especially given the rapid pace of ed tech evolution in which identities of sub-contractors and uses of data are quite dynamic.[88] However, tech companies are best

[84] *Duncan Response to Markey* at 8.

[85] *Cf. generally id.* at 8-9 (suggesting that the Department of Education has limited resources to investigate but does have the authority to conduct investigations in certain well-defined situations).

[86] Some scholars go further than considering how to streamline existing investigatory powers and emphasize what they see as fundamental procedural weaknesses involving the Department of Education's enforcement powers under FERPA. *See, e.g.,* Daniel Solove, *Big Data and Our Children's Future: On Reforming FERPA*, TAP BLOG (May 20, 2014), http://www.techpolicy.com/Blog/Featured-Blog-Post/Big-Data-and-Our-Children-s-Future-On-Reforming-FE.aspx (asserting that a major issue with FERPA is that it "lacks meaningful enforcement . . . FERPA needs to provide the Department of Education with a vibrant enforcement toolkit and the ability to issue meaningful sanctions in adequate proportion to the gravity of the violation. The Department of Education needs vastly more enforcement resources and personnel.")

[87] Indeed, the cloud ed tech provider community has already demonstrated its awareness of and responsiveness to stakeholder concerns around privacy in a variety of ways. *See*, *e.g.*, Nick Grandy, *So You're Building an Ed Tech App? An Intro to Data Privacy*, CLEVER (Apr. 21, 2014), http://blog.clever.com/2014/04/data-privacy-for-edtech-vendors/ (advising developers not to "be the bad guy" and to use '[h]uman readable privacy policies"); Bram Bout, *Protecting Students with Google Apps for Education*, GOOGLE (Apr. 30, 2014), http://googleenterprise.blogspot.com/2014/04/protecting-students-with-google-apps.html (describing changes in the company's Google Apps for Education services, namely the "remov[al] of a the 'enable/disable' toggle for ads" such that "ads in Apps for Education services are turned off and administrators no longer have the option or ability to turn ads in these services on" and the "remov[al] [of] all ads scanning in Gmail for Apps for Education, which means Google cannot collect or use student data in Apps for Education services for advertising purposes.").

[88] *See* SPI, *Student Privacy and Cloud Computing* at 2.

equipped to know and hence to share this information. And concerns about the labeling requirement being overly onerous could be addressed by setting a reasonable timeline for updates to the original label that could promote transparency while simultaneously allowing the company's business relationships and products to advance.

A labeling requirement might also prove advantageous by facilitating older students' meaningful awareness of and potentially even input into the ed tech decisions made by their schools and districts.[89] Although federal law does not give children and teenagers consent or opt out rights regarding data about them until they reach age 18, schools and districts might want to think about ways to incorporate student input during cloud-based ed tech decisions, perhaps by inviting a student representative to school board or board committee meetings to provide a student perspective on different ed tech companies or arrangements. Longer term, revisions to federal and / or state laws and regulations that would give students under 18 a right to see their ed tech digital footprint might well merit serious consideration. This sort of regulatory change could empower students under 18 to thoughtfully and comprehensively manage their online identities (perhaps by amending FERPA and its regulations to give access and review rights to students younger than age 18)—a crucial skillset for navigating school, workplace, and society more broadly in the twenty-first century.[90]

3) How to Effectively Secure Student Data & Protect Student Privacy? Surfacing Key Considerations and Establishing Good Practices

Despite the openness of this twenty-first century frontier, the realm of cloud-based ed tech is far from completely ungoverned and unprotected. To the contrary, ed tech providers and educators make many efforts to protect and secure student data, thereby limiting the extent to which data about students may become part of a more broadly available digital footprint. Returning to our hypothetical, Principal Smith's letter pledges that Scholair will encrypt AMS students' data and not mingle it with other schools' data also held by Scholair. This set-up does offer some data security benefits, as hard copy records stored in physical filing cabinets might in fact be more vulnerable to privacy invasions over the course of routine school life than those records stored appropriately in the cloud.[91]

In the hypothetical, there is an exception to the encryption and non-co-mingling requirements that bind Scholair, however, which raises data security concerns. This exception allows Scholair to analyze aggregated but de-identified data in order to track trends and engage in other data

---

[89] *Cf. generally* Sandra Cortesi *et al., Youth Perspectives on Tech in Schools: From Mobile Devices to Restrictions and Monitoring,* BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY 16 (Jan. 15, 2014), http://cyber.law.harvard.edu/publications/2014/youth_perspectives ("On a general level, one might ask as to what extent the youth perspectives highlighted in this brief [on digital tech in schools] align or contrast with an adult-normative perspective on these topics as expressed by parents, teachers, and school administrators.")

[90] *See generally* Khaliah Barnes, *Why a Student Bill of Rights Is Desperately Needed*, WASHINGTON POST (Mar. 6, 2014), http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.

[91] *Cf.*, *e.g.*, Univ. Santa Cruz, Information Technology Services, *Security Breach Examples and Practices to Avoid Them*, http://its.ucsc.edu/security/breaches.html (last visited on May 3, 2014) (reminding employees of importance of securing files, papers, and other physical repositories of information to prevent unauthorized access to student information).

analytics. It is not clear from the letter what Scholair's encryption and de-identification methods actually entail, making it difficult for parents to know if their children's information is kept safe and confidential.[92] Such lack of clarity around data security and de-identification measures taken by cloud providers is fairly common in the real world as well, with providers of some types of ed tech functionalities providing more explicit commitments to specific protocols than others; for example, researchers have found that providers of services such as cafeteria food are especially likely not to have adequate protocols in place.[93] Given the apparent absence of a formal agreement between Scholair and AMS, it is probable that no such commitments have been made in this instance.

No matter what contractual terms are put in place, however, the adoption of cloud-based ed tech will create some potential for harms to student privacy.[94] At this point in the evolution of these technologies, the most pressing potential harms relate to data input; that is, what threats might there be to data security and integrity as student information flows into and out of the cloud? The potential for data breach and data leakage from one cloud user to another are among the most salient risks in the first stage of the development of cloud-based ed tech.[95] These harms contemplate unauthorized access by people or entities other than the school and the ed tech provider. In order to minimize the potential for unauthorized data access and the accompanying risk of harm to students and their families—such as identity theft—schools would be well-served by being particularly mindful of the already existing FERPA requirement for data destruction by third parties after the provider has fulfilled the agreed upon function.[96] Schools also would do well to get providers to agree to issue prompt notification in the event of a data breach. Some state laws impose this requirement on for-profit entities; however, it is not typically part of cloud ed tech contracts, which may also be with non-profit entities.[97] For their part, states might consider additional possible actions; for instance, one approach would be to follow the lead of the Utah Attorney General's office and establish a unit for the investigation and prosecution of

[92] *See supra* note 27.

[93] Currently, the level of data security varies somewhat depending on what type(s) of function(s) an agreement covers. For instance, CLIP found that data security practices are not good for "special school functions": "None of the agreements . . . specified the level of security such as the NIST [National Institute of Standards and Technology] level. These findings are not encouraging, as they suggest that vendors of special school functions services—unlike the vendors of data analytics, student reporting, and guidance functions services—do not recognize data security as a concern and do not tailor their products and services accordingly." *CLIP Report* at 48.

[94] The degree of harm possible with cloud ed tech as opposed to with traditional, non-digital methods of storage is a matter of debate on which we take no position at this time. For the purposes of this paper, we seek to observe that cloud ed tech does pose some risks to student privacy, as do other forms of student data storage. *Cf. also* CoSN, *Toolkit* at 13 (listing "Security Questions to Ask of An Online Service Provider").

[95] *See* Gasser, *Cloud Innovation* at 10.

[96] *See CLIP Report* at 31 ("As a data security measure, FERPA requires the destruction or deletion of data after it is no longer needed for the purposes for which it was transferred."); *Best Practices for Data Destruction*, PRIVACY TECHNICAL ASSISTANCE CENTER, U.S. DEPT. EDUCATION 2-3 (May 7, 2014), http://ptac.ed.gov/document/best-practices-data-destruction ("While FERPA is silent on specific technical requirements governing data destruction, methods discussed in this document should be viewed as best practice recommendations for educational agencies and institutions to consider adopting when establishing record retention and data governance policies to follow internally, and also for inclusion in any written agreements and contracts they make with third parties to whom they are disclosing PII.").

[97] *See CLIP Report* at 36 (reviewing agreements and finding that "none of the agreements required vendors to notify districts of any data security breach.")

theft of juveniles' identities in case there is a rise in this type of crime in association with more student data going into the cloud.[98]

As cloud-based ed tech continues to develop, the types of harms that merit consideration will likely expand to encompass risks posed by the possible uses of student data by those with access to it—from educators to tech companies to (potentially) governmental entities. With this next generation of data analytics, students might become exposed to unforeseen, long-term, and deleterious consequences, such as using data in a discriminatory fashion.[99] Future SPI work will consider such 2.0 problems.

Turning back to the 1.0 challenges facing cloud-based ed tech now, it is worth considering the unique role that cloud providers themselves might play when it comes to ensuring that students' information is secure, de-identified (as appropriate), and not put to uses that transgress the spirit if not the letter of a given ed tech agreement. Because of the "wild west" terrain of ed tech—a booming industry with lots of aspiring entrants and a somewhat complex and fluid statutory and regulatory landscape—there is the opportunity for the industry itself to move toward adopting voluntary best practice standards to which participants could adhere.[100]

Such standards would not supplant the need for legislative and regulatory reform. Yet, at this point in time, they could potentially both serve as a valuable initial supplement to the law-making process as it moves forward and inform the ultimate outcome of such a process. For instance, the U.S. Department of Education has acknowledged that federal law might not go far enough in the realm of data security and "regularly urge[s] schools and districts to look beyond legal compliance with FERPA and other laws, to focus on FIPPs [Fair Information Practice Principles, such as data minimization] in making decisions about the use and protection of student data."[101] Of course, state laws could also address some of the weaknesses or gaps in the federal legal landscape; indeed, the volume of actual and proposed legislation in the states related to cloud-based ed tech reflects considerable effort toward this end.[102] As new state legislation continues to develop, however, industry best practices could be a responsible part of the collective learning process in which all cloud-based ed tech constituencies are currently engaged.

Within such a voluntary framework, room remains for individually tailored product design and unique agreements between schools / districts and providers, as the Department itself

---

[98] *See* IRIS: Child Identity Protection Program, OFFICE OF THE UTAH ATTORNEY GENERAL (last visited on Apr. 23, 2014), https://cip.utah.gov/cip/SessionInit.action.

[99] For example, given the available data on school-to-prison pipeline issues as particularly acute for minority populations, there is a concern that data analytics—if not properly handled—could contribute to tracking of minority students into the criminal justice system. *See*, *e.g.*, *School to Prison Pipeline*, NAACP LEGAL DEFENSE FUND, http://www.naacpldf.org/case/school-prison-pipeline (last visited on Apr. 23, 2014).

[100] *See*, *e.g.*, Mark Schneiderman, *SIIA Announces Industry Best Practice Standards*, DIGITAL DISCOURSE BLOG (Feb. 24, 2014), http://www.siia.net/blog/index.php/2014/02/siia-announces-industry-best-practices-to-safeguard-student-information-privacy-and-data-security-and-advance-the-effective-use-of-technology-in-education/.

[101] *See Duncan Response to Markey* at 5-6 ("FIPPs are widely accepted principles that serve as a framework for safeguarding individual privacy in information systems and programs . . . [also] a school or district making a disclosure to a third party under the school officials exception is responsible for controlling the length of time that a third party maintains PII from education records.")

[102] *See supra* note 9 (flagging state legislative activity in ed tech space).

recognizes.[103] But for cloud-based ed tech providers that want to be repeat customers with schools and districts, it would be prudent to make products whose default set up is not just for legal compliance (by schools and providers) but also for FIPPs or other best practice compliance.

V. CONCLUSION: KEY TAKEAWAYS

The analysis of the Scholair-AMS hypothetical surfaces several key discussions currently swirling around the growing adoption of cloud-based ed tech: who in the educational system should make cloud-based ed tech decisions; when is parental consent needed for the adoption of these technologies; and how can data transferred, stored, and analyzed through these products be kept secure and, as necessary, de-identified? These complex questions implicate a variety of interests, values, and goals, with no uniform answer applying across all contexts. In general, though, certain pragmatic approaches emerge that could help guide decision-makers and policymakers in establishing and implementing legal, statutory, and policy frameworks around cloud ed tech:

- Consider (temporary) centralization of decision-making at the district level to foster the legal, technical, and other expert oversight necessary around cloud ed tech decision-making, taking care to preserve appropriate space for local experimentation and innovation.
- Examine adoption of user-friendly labeling of cloud ed tech products to increase transparency, thereby fostering compliance with parental consent and other legal requirements.
- Potentially adopt FIPPs and other best practice standards by industry providers to increase data security and protection, while recognizing that such best practices supplement rather than substitute for formal policy guidance and possible reform.

All of these suggestions are intended to respond to a contemporary snapshot of cloud ed tech and will likely—indeed, almost certainly—evolve as this picture develops further. SPI looks forward to continued engagement with stakeholders in this space to advance the opportunities that cloud ed tech offers to transform education, while being mindful of and responsive to the challenges it simultaneously presents.

[103] *Duncan Response to Markey* at 7-8 ("Our regulations do not require a 'one-size-fits-all' approach regarding reasonable methods for access controls, because we recognize that each school or school district needs to develop its own policies and procedures to meet its individual needs.") *See FERPA Guidance for Reasonable Methods and Written Agreements*, U.S. DEPARTMENT OF EDUCATION (Dec. 2011), http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf.

APPENDIX A: FULL SCHOLAIR HYPOTHETICAL

Greetings Parents,

We here at Anywhereville Middle School, USA (AMS), are excited to announce a change that will greatly enhance your and your child's school experience! Starting next month, we will partner with Scholair to maximize educational potential, minimize hassle for everyone, and explore new ways of responding to the challenges of twenty-first century school life.

Scholair is an educational technology company that provides three main services: it (1) stores student data in the "cloud"; (2) offers a dashboard that gives authorized users easy ways to input, access, and analyze this data; and (3) provides access to end-user software applications. Scholair is totally FREE for you and your child to use and comes at a very reasonable cost to the school. In addition, Scholair provides its customers with access to some applications ("apps") developed by third party app developers, who may charge a small fee.

Here is what will happen next:

AMS will transfer to Scholair all data about current students that it has on file, whether in hard copy or on existing databases. We will also store any new data about your child directly in Scholair by inputting the data through the dashboard. This data includes— but isn't necessarily limited to—names, contact information (address, phone, email), history, disabilities, homework assignments, dates of birth, attendance, discipline, health, report cards, fingerprints, and family status.

Scholair will safely store all of your child's records on servers managed on behalf of Scholair by its third party service providers. Scholair will only look at or share student data to the extent necessary to provide the services described below. Scholair will encrypt the data so that its third-party service providers will not be able to decipher the information contained your child's records.

Scholair will not combine data on AMS students with data it holds for other schools, except as described below. In most ways, it's as if AMS were a tenant and Scholair a landlord. AMS essentially will be renting storage space from Scholair and paying for certain services to be performed by Scholair. (Think the landlord coming in to install new window panes to help the tenant see better, just like Scholair will help us see trends within our school more clearly!) Other schools may also rent spaces in the same "building" by renting space on servers hosted by Scholair, but being our neighbor doesn't give them access to our belongings. Scholair will keep AMS' data in its own space, separate from any neighborly or outside access.

Once the data is stored with Scholair, here is what Scholair offers:

- **Cubbies:** Each student will have a virtual "cubby" that authorized users can access through the dashboard provided by Scholair. This cubby will store all the key information that teachers, administrators, parents, and students themselves need to fulfill their respective roles. Information kept in the cubby will include— but will not be limited to—attendance, discipline, health history, homework assignments, and report cards.

- **Access to Cubbies:**[104] Only you, your child, and any school employees who are working with your child can access your child's cubby. But not all types of access will be the same. Each person who accesses the cubby will see only the information permitted by law, regulation, and district and school policies. For example, my secretary will be able to look in the cubby for attendance, health, and discipline information, but not for homework assignments. You will be able to see all of your child's information, such as grades, homework assignments, and disciplinary incidents. But if you would like to access additional administrative records that may relate to your child—such as which teacher was with a given class at a particular time— you may request those records according to existing policies. No parent will be able to see information about any child other than her own, and no student will be able to see information about any student other than herself, unless a parent or student willingly shares that information.

- **Clusters of Cubbies:** Faculty and staff will be able to set up "cubby clusters" for groups of students who are in the same class, same activity, and so on, like all the students in Mrs. Jones's homeroom. These clusters will be accessed through the dashboard and allow employees to manage information and communication effectively; for instance, Mrs. Jones will be able to send the same message about the upcoming class trip to Chicago to all her students by pushing a single button. They will also allow employees to review both individual student records and groups of student records using analytical software developed by Scholair for the purpose of understanding trends, risks, and opportunities for growth within the student body at AMS. Tracking patterns across clusters might help us preemptively identify risks of bullying, threatening, or otherwise violent behavior, as well as highlight talents to develop, such as musicality or math aptitude. We can then make programming decisions based on this information, such as moving recess an hour earlier if we have many students in a class who have difficulty sitting still for long periods of time.

- **Studying Cubbies:** Scholair's software also gives us a unique learning opportunity: we can compare trends in our clusters and student body as a whole to those in other schools that store their data in Scholair. Scholair aggregates student data from all the schools that use its services so that it can provide individual schools with a broad basis of comparison to other schools nationwide. Don't worry—any data that is assessed in the aggregate will be safely and securely de-identified so that your child and any private information about her is not at risk. But we will be able to get a much better sense of what's happening in middle schools nationwide and how we might be able to bring model programming ideas from other schools into our community.

- **Messages in Cubbies:** Scholair offers a messaging function so that you, your child, and school employees can exchange private messages with each other through your child's cubby. These messages can be sent to one or more people with cubby access.

- **Art on Cubbies:** You and your child can "decorate" your child's cubby by choosing to

[104] This type of arrangement is sometimes referred to as "role-based" or "managed" access. *See Frequently Asked Questions on the Statewide Longitudinal Data Systems (SLDS) Grant Program*, NATIONAL CENTER FOR EDUCATION STATISTICS (last visited on Apr. 23, 2014), http://nces.ed.gov/programs/slds/faq_grant_program.asp.

display certain information for others in a "cubby cluster" of which your child is a member. For example, a student in the band cluster could post a digital picture of herself with her new French Horn for others with access to cubbies in the same cluster to see. You or your child could also share information about your child's growth (like when she finally hits five feet tall!) or expressions of personal preference (for instance, allowing your child to share that she loves our hometown baseball team!).

- **Library:** Scholair offers a virtual library of educational software applications ("apps") to help your child learn everything from reading, 'riting, and 'rithmetic to composing jazz music and combing through archaeological ruins. Apps are also available to help your child learn "soft skills," such as forming healthy friendships and dating relationships. Based on their knowledge of your child and the use of Scholair to analyze your child's needs, teachers will select apps that your child can then download and use. These applications have been developed by a variety of third-party providers for use by schools participating in Scholair.

- **Stocking the Library Shelves:** Scholair offers an Application Programming Interface, or API, (populated by sample student data) for app developers. Before apps can be put in Scholair's virtual library for students to purchase, Scholair must approve the apps. But Scholair won't put any real student data into the apps. Your child would be responsible for providing the information necessary to use any apps selected. You will be able to see any apps that your child has downloaded by accessing her or his cubby.

Here's what we'll need from you:

- We hope you will all be enthusiastic users of Scholair. We will be sending home permission slips for you to sign that authorize your child's teachers to select the apps that will go in your child's cubby. Please return those to your child's teachers ASAP.
- We ask you to review the details of Scholair's Terms of Use, Privacy, and other policies on Scholair's website. In particular, we wish to draw your attention to Scholair's storage of your child's personal information. Again, all of the data about students at AMS will be maintained on servers belonging to third-party cloud storage providers with which Scholair sub-contracts. These third parties will provide server space, but they will not be able to see the encrypted data about AMS students. Scholair may also sub-contract with other companies to perform additional support functions, such as providing infrastructure or other operations necessary to maintain Scholair. Scholair and its subcontractors will only have access to the information necessary to perform the services for which we have retained them, which include but are not limited to: storing individual and aggregated student records, analyzing these records, aggregating and analyzing anonymized student data from Scholair schools nationwide, and identifying opportunities for further educational growth and development for all members of the AMS community. (App developers have a license to sell their products through Scholair but are not subcontracted to provide services to Scholair.) The identities of Scholair's sub-contractors are subject to change at any time, as are the services they provide.

We encourage you to ask us any and all questions as we work together to put our school in the cloud—while keeping our feet firmly on the ground! All best, Principal Smith

ACKNOWLEDGEMENTS

The authors wish to thank the participants at the November 2013 Berkman Center workshop co-organized with the Consortium for School Networking. Participants' contributions at this event began many of the key discussions that informed this paper. Thanks also to Dalia Topelson, Alex Wood, and David O'Brien for their valuable feedback and to Abby Colella for providing research assistance.