Youth and Media

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

Privacy & Student Data: Companion Learning Tools

March 2017

Leah A. Plunkett
Dalia Topelson Ritvo
Paulina Haduong

For use as a companion tool to
Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies
by Dalia Topelson Ritvo

table of contents

Introduction and Discussion Questions

Scenario One

Scenario Two

Scenario Three

Scenario Four

Scenario Five

35

Conclusion

introduction

Overview

Educators are at the vanguard of the massive transformation of primary and secondary (K-12) learning environments unfolding today.[1] As the educational technology ("ed tech") industry booms, educators have unprecedented opportunities to engage with their students using dynamic learning experiences, personalize learning for individual students, and gain insight into the strengths and weaknesses that both students and entire cohorts exhibit.[2] Ed tech also offers educators new and streamlined ways to store and analyze information about students and cohorts related to educators' own classroom management responsibilities, such as attendance records, disciplinary incidents, and grades.[3]

Ed tech today looks almost nothing like the classroom technologies of yesteryear. Handwritten flashcards, individual teacher gradebooks, and other tech products that belong only to one brick and mortar classroom at a time are out. Lectures that thousands of students around the world can watch and respond to at the same time, robots that help students on the autism spectrum learn to read social cues, and other Internet-based technologies have taken their place.[4] Computer programs, apps, and networked technologies that we use all the time in our personal lives that aren't necessarily geared toward education—

[1] *See, e.g., ConnectEd Initiative*, White House, https://www.whitehouse.gov/issues/education/k-12/connected (last visited on July 17, 2015) (describing Presidential plan "designed to enrich K-12 education . . . empower[ing] teachers with the best technology and the training to make the most of it.").

[2] *See generally* Leah Plunkett, Alicia Solow-Niederman, and Urs Gasser, *Framing the Law & Policy Picture: A Snapshot of K-12 Cloud-Based Ed Tech & Student Privacy in Early 2014*, BERKMAN CENTER FOR INTERNET & SOCIETY 5 (June 2014), https://cyber.law.harvard.edu/publications/2014/law_and_policy_snapshot [hereinafter SPI, *Framing the Picture*].

[3] *See generally id.* at 5-6.

[4] *See, e.g.,* Alexandra Pannoni, *MOOCs A New Tool for High School Teachers*, U.S. NEWS & WORLD REPORT (Oct. 27, 2014), http://www.usnews.com/education/blogs/high-school-notes/2014/10/27/moocs-a-new-tool-for-high-school-teachers; Bridget Carey, *Meet Milo, A Robot Helping Kids with Autism*, CNET (May 13, 2015), http://www.cnet.com/news/meet-milo-a-robot-helping-kids-with-autism/; Joel Reidenberg *et al.*, *Privacy and Cloud Computing in Public Schools*, CENTER ON LAW AND INFORMATION POLICY, Fordham Law School 1 (Dec. 13, 2013), http://ir.lawnet.fordham.edu/clip/2/ [hereinafter *CLIP Report*].

This document does not constitute legal advice and does not represent the formation of an attorney-client relationship between the authors of this guide and any users of the guide. Users should consult an attorney as necessary to receive legal advice on protecting student privacy as needed for their specific uses of educational technologies in their jurisdictions. Student privacy laws are evolving rapidly; the information on this checklist reflects the current federal laws COPPA, FERPA, and PPRA and accompanying regulations as of June 7, 2016. The document does not include any state laws or regulations that may apply based on where users are located.

like Facebook and FitBits—are also finding their way into connected learning environments.[5]

This new generation of connected ed tech harnesses the Internet's ability to facilitate the collection, sharing, and processing of data on an unprecedented scale, with the result that more types of student data are being collected, shared, and analyzed than in the past.[6] While the use of these technologies creates opportunities for individualized learning and easier access to information by parents and students, their use also raises concerns around protecting student privacy, such as ensuring data security; preventing unauthorized access, as well as undesirable or unauthorized uses of data by authorized users (such as marketing to students and families by ed tech companies); and ensuring that students are not profiled in ways that could be deleterious or even discriminatory.[7]

As school and district-level decision-makers, you are likely on the receiving end of many questions from faculty and staff in your schools about what federal student privacy laws permit them to do with respect to ed tech. You might also have had experiences where some faculty and staff members have gone ahead and used ed tech products—with the best of intentions but without asking such questions—only to have it come to light later that those uses were not in line with best practices or were not compliant with federal or state student privacy laws.

We have compiled these materials to explain and clarify three key federal student privacy laws and their impact on ed tech adoption and use, so that you can create meaningful learning experiences with core faculty and staff constituencies. The laws are the Family Educational Rights & Privacy Act or "FERPA" (20 U.S.C. § 1232g), the Children's Online Privacy Protection Act or "COPPA" (15 U.S.C. § 6501), and the Protection of Pupil Rights Amendment or "PPRA" (20 U.S.C. § 1232h) . The materials proceed in two parts: (1) Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Connected Through Networked Technologies (the "Guide")[8], which summarizes FERPA, COPPA, and PPRA in a user-friendly question & answer format, and (2) hypothetical scenarios in this "Companion Guide"—involving classroom teachers, curriculum directors, and tech directors—that aim to bring key takeaways to life from the Guide.

These scenarios are meant to create illustrative learning experiences, not an exhaustive list of every potential scenario that could arise. They are meant

[5] *See, e.g.*, Gail Leicht & Don Goble, *Should Teachers Be Using Social Media in the Classroom?*, PBS NEWSHOUR (Oct. 1, 2014), http://www.pbs.org/newshour/updates/social-media-valuable-tool-teachers/; Neil Johnson, *Edgerton Schools Using Technology to Track Student Fitness*, GAZETTEXTRA (Dec. 27, 2013), http://www.gazettextra.com/article/20131227/ARTICLES/131229855.

[6] *See generally CLIP Report* at 1; SPI, *Framing the Law & Policy Picture* at 5-7.

[7] *See generally* SPI, *Framing the Picture* at 15, 17-18, 21-24.

[8] See Dalia Topelson Ritvo, *Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies*, Cyberlaw Clinic at Harvard Law School (June 2016), https://dash.harvard.edu/handle/1/27410234 http://cyber.law.harvard.edu/publications/2013/privacy_and_childrens_data [hereinafter *Guide*].

to help you and your colleagues understand when to ask questions about whether FERPA, COPPA, or PPRA apply and what they require, as well as how to go about answering those questions. You should also note that other laws or policies may apply to your particular school or district, so you should be mindful that this toolkit does not address state or municipal privacy laws that may apply to a particular school system. As you navigate this complex, evolving legal landscape, please remember to consult your school's legal team to obtain answers to your specific ed tech and student privacy questions.

At this stage of ed tech development, with so many new products coming to market and laws evolving so rapidly, it is best in most situations to make ed tech choices centrally at the school and district levels.[9] Tipping the balance now toward centralization facilitates a collaborative, team-based approach to ed tech adoption. In this set-up, classroom teachers can share their insights and desired ed tech pedagogical innovations with school and district leaders who can bring necessary backgrounds in technology, privacy, and other related fields to bear in assessing whether a given product contains appropriate privacy supports.[10] In some instances, it may be necessary for such a team to seek legal counsel to determine whether all applicable federal and state privacy laws and regulations would be followed in a given course of action. Clear lines of communication, a high degree of trust between stakeholders, and a shared commitment to both technological innovation and student privacy will support an enjoyable and productive iterative process in the dynamic twenty-first educational landscape.

[9] *See* SPI, *Framing the Picture* at 9-11.
[10] *See id.*

These questions are designed to guide discussion of each scenario. You might also find them helpful as a guide for discussing real world situations. A "cheat sheet" of notes on key takeaways based on these questions follows each scenario but is not an exhaustive list of every topic that could arise.

- What types of ed tech are involved in this plan?
- Will any information about students leave the school?
- Will this information be hosted on systems not controlled by the school (*e.g.* "on the cloud"[11] or servers operator by an external company)?
- Will this information be shared with companies or individuals that are not school employees?
  - If the answer is yes to the preceding question, who will have access to the information? (Make a list of everyone who will or should have access to this information.)
- What types of information are being shared? (Create a list of all the student information that will be collected, shared, or accessed by third parties.)
- Is there any information being shared that could be considered sensitive? Is there any that could be considered "personally identifiable information" ("PII") under FERPA, "personal information" ("PI") under COPPA, or "personal information" ("PI") or other types of information protected under PPRA?[12]
- Do you know what the parties who get the information will do with it? If one of these parties is a company, do you know what its privacy practices are?

[11] While there are many different definitions of the "cloud," we understand "cloud ed tech" or "cloud-based ed tech" to mean those 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 administrative work." SPI, *Framing the Picture* at 4 (internal reference omitted).

[12] Please note that the definitions of "personal information" in COPPA and PPRA are different, so in doing your analysis, it is important to specify whether you are referring to "personal information" as defined in COPPA or "personal information" as defined in PPRA. *See Guide* at 20. Please also note that PPRA has extra protections in place—in certain- circumstances—for eight categories of highly sensitive information. *See Guide* at 16-18.

- Does your school or district have a contract with any of the parties who will have access to the information?

- Do you plan to ask students' parents for consent to share this information? What about consent from students themselves?

- What benefits do you think sharing this information about students might bring to the students? To you as an educator? To the school?

- What risks do you think sharing this information might pose to students? To you as an educator? To the school?

- Are there key areas where you need more information to be able to answer these or related questions? Where might you get that information?

- Who else might you want to consult with to make sure these or related ed tech and student privacy questions are answered fully and satisfactorily?

how to use this guide

Student privacy questions were easier back in the days when an apple on a teacher's desk meant a fruit, not an iPad. There's no potential student privacy problem when educators ask students to use their basic calculators to solve an equation, for instance, because the calculators aren't transmitting any information from the students to a third-party outside the learning environment. But if students use an online-based quiz tool to respond to the same question, potential issues arise. Are students being asked to share any personal information with the company that runs the tool? Do you know what the company might be doing with this information? If you're relying on an online-based program to help you track discipline problems and recommend learning modules to students to address infractions, is that company building profiles of individual students that could negatively impact students down the road?

These and similar questions come up all the time with ed tech today. They can feel frustrating, even overwhelming, and may cause educators to shy away from using ed tech—even if such use might actually enhance both professional and educational experiences.

The five hypothetical scenarios below are geared for use by school and district level decision-makers. They are designed to surface tough questions around ed tech and student privacy, as well as offer guidance on how you and core groups of your colleagues—classroom teachers, curriculum directors, and tech directors—might go about coming up with answers to these questions in ways that both address your educational needs, while also complying with best practices, COPPA, FERPA, and PPRA. A set of discussion questions is provided up-front, followed by key takeaways (that reference the Guide) provided below each scenario. These scenarios are designed to be used to create relevant and dynamic learning experiences within your school or district. In addition, the following discussion questions can serve to guide your school or district's decision-making process surrounding your actual adoption and use of real ed tech products.

scenario one

Feed Yourself, Be Yourself

The physical education teachers at Anywhere Middle School (AMS) in Anywhereville, USA—a public school—are excited to have received a state government grant to run a new series of lesson modules for their PE classes in the upcoming academic year: “Feed Yourself, Be Yourself.” Designed to promote youth health and wellness, the goal of this series is to help kids understand their bodies’ unique nutritional needs (including how to cope with any food allergies or sensitivities), learn how to cook healthy snacks and meals, and how to shop for healthy food within a budget. The modules will be team-taught by the PE teachers from Anywhere Middle School and a nutritionist from Anywhere Hospital. Because of the state government grant, all materials will be provided to all students in the PE classes free of charge.

The PE teaching team plans to include the following in its curricular proposal: Students will wear Kidbits that are manufactured by TrakBit, a company dedicated to developing technological tools to help people get fit. TrakBit is donating bracelets and watches that monitor the wearer’s activity levels throughout the day and sync back to TrakBit’s servers to determine what the kids’ caloric needs are. In addition to the real-time data collected through the Kidbits, TrakBit also receives every student’s name, birthday (month and year), gender, height, and weight. Students must also identify any health issues they may have from a pre-populated list created by TrakBit, based on their research on what health issues may be relevant to an individual’s health needs. This information will be reviewed and accessible by the PE teachers, students, the students’ parents, and, if students are taking in an unhealthy number of calories, the nutritionist from the Hospital.

Students will participate in a Massive Open Online Course (“MOOC”) run by Anywhere State University’s Extension School called “Cooking 101,” which will teach them the basics of food shopping, storage, and safe preparation. As part of the MOOC, students will be assigned to teams with other course participants of all ages from around the world to staff a virtual restaurant, for which they will need to create menus and business plans. Students will have the option of publishing their menus and plans on social media to receive feedback from the general public, in addition to the feedback that teammates will give each other and receive from the MOOC instruction team.

At the conclusion of the course, Anywhere Middle School will have a special lunch menu one day featuring recipes from the virtual restaurant. Students will take their favorite recipes from the virtual restaurant and prepare them--with oversight and support from the cafeteria staff--for their classmates and teachers. (The cafeteria supervisor can track the type and quantity of food each student buys each day because the purchases are linked to each student’s ID card, so if one or more items on the special menu is a hit, the supervisor is willing to consider making it a permanent part of the menu rotation.)

Students’ grades in PE will reflect their performance in this series of modules. Points will be assigned for wearing the Kidbits, MOOC participation, food preparation, and other related activities in addition to standard PE requirements (exercise, etc.).

You are part of the PE teaching team. You and your teammates are preparing to present this proposal to your curricular director. Do you think the proposal is likely to raise any privacy concerns? Why or why not?

Scenario One Cheat Sheet

Types of Ed Tech

Multiple types of ed tech are involved here: the Kidbits are a form of ed tech because they are networked devices being used for educational purposes; the MOOC—and any related social media uses—is a type of ed tech; and even students' cafeteria IDs are a form of ed tech (although decisions about cafeteria IDs are arguably outside the scope of the PE teaching team's authority).

Understanding who will have access to the information, and how the information will be used.

Student information is going to be shared outside the school with TrakBit (weight, height, activity level, etc.), potentially with the nutritionist from the Hospital and, depending on what students share about themselves in the MOOC, with the MOOC provider, other MOOC participants, social media tools and even the general public. It is also possible that TrakBit plans to reshare the information further in ways that were not explicitly stated in the scenario; the teaching team will need to work with colleagues—such as the tech director—to determine what the company's privacy policies, terms of uses, and other practices are in this area.

Analyzing the level of sensitivity of the information collected or shared with other parties.

Much of this information is very sensitive, as it relates to students' health, daily routines, and other intimate details of their daily lives. There are many potential pedagogical benefits to this information sharing. For instance, students, teachers, and parents could gain unique insights into students' health habits through the Kidbits, and students' participation in the MOOC could expand their horizons in important ways. There are risks as well, including that one of the third parties that obtains student information will use it to market to students and their households; create profiles of students that could have a deleterious impact on students at some point down the road if the profiles were re-shared for commercial or other purposes (for instance, this student was gluttonous and out of shape as a twelve year-old, so his life insurance premiums as a twenty-two year-old should be higher than his peers). Additionally, the health issues identified by students could be highly sensitive information that, while its inclusion may improve the analysis of TrakBit, may be information that the student or their parents prefer not to have shared.

The PE teaching team should be prepared to consult with the curricular director (and other administrators, as necessary) to determine whether any of this sensitive student information is considered to be “personally identifiable information” (PII) from “education records” under FERPA.[1] The information collected by TrakBit (which may be shared with the nutritionist) is at the heart of the “Feed Yourself, Be Yourself” curricular plan, so it makes sense to focus the PII analysis here. The information collected by TrakBit does qualify as PII because the combination of information being provided to TrakBit could easily identify a child (e.g., age, weight, height, and gender of the child). In addition, biometric information, which is generally considered highly sensitive information, can also qualify as PII. Although the amount of activity a student engages in probably wouldn’t identify a child itself, the combination of this information, along with the age, weight, height, and gender, could identify the child. In addition, it appears as if the school will be requiring or strongly encouraging participating students to share this type of information themselves in their engagement with the MOOC or social media. If students rather than the school itself are sharing PII, such activity may not technically be PII-sharing under FERPA; however, as a best practice, the school should proceed as if it were. The school should take responsibility for reading, understanding, and (if necessary) negotiating terms of use and related policies with the MOOC provider and any required or recommended social media sites since their use is part of a comprehensive curricular plan.

It’s not clear from this plan what uses TrakBit, the MOOC, the nutritionist, or general social media might have for information about students in this class. The teaching team should review privacy policies and terms of use for Kidbit, the MOOC, and any social media that students might use through the MOOC to see if these third-parties might be engaged in re-sharing this information or using it for marketing purposes. TrakBit is a fitness company, thus it may well have an interest in using such information for marketing or similar purposes. The team should also ask the nutritionist what uses he/she plans for this information. If any re-sharing or marketing is planned, the team would want to put the re-sharing plans in the requested consent under FERPA—or, better yet, try to negotiate for no-resharing—and, depending on what school and district policies are, try to negotiate to stop the marketing. This type of analysis of privacy policies and terms of use might well require consultation with a tech director, other administrator, or even an attorney. In addition, any follow-up negotiation around re-sharing or marketing proposals might be best done by a school or district-level

[1] *Guide* at 2-4.

leader rather than the teaching team directly. Finally, the school should be aware that the nutritionist may be subject to additional privacy obligations under HIPAA.[2]

Necessary Consents and other Privacy Protecting Measures

Because PII (under FERPA) is being shared with third parties, it is possible that parental consent would be required under FERPA.[3] Whether or not consent is required under FERPA depends on whether (i) PII from an education record is being shared with a third party (in this case yes), and (ii) whether the sharing of the information is covered by one of the exceptions to the consent requirement in the statute. In this case, while it is possible that TrakBit, the nutritionist, and the MOOC might be covered under the "school official" exception, it is a good idea to obtain consent from the parents, as parents might well be upset if they find out after the fact that sensitive PII (height, weight, caloric intake, health issues, etc.) was being shared with a private company or others without their knowledge. In addition, obtaining consent from parents ensures that the program is compliant with FERPA requirements. (Note: the "school official" exception wouldn't apply to social media use here.)

That said, if a school would prefer to move ahead without consent, the school would need to ensure that TrakBit's and the others' collection and receipt of information about the students fell under one of the exceptions. In this case, the appropriate exception would be the "school official" exception, where schools may share education records with contractors that: (i) fulfill a role the school would otherwise perform itself, (ii) are subject to the direct control of the school, and (iii) will not redisclose this information to anyone else.[4] In this case, the school would need to have a contract with TrakBit and the others that ensured that they would only use the information collected about and from the students as necessary to provide services to the school, and restricting them from sharing the information with any third party. Likewise, the school should conduct due diligence on TrakBit and the others to ensure that TrakBit's information practices will allow it to comply with the necessary restrictions for the school to comply with FERPA. Admittedly, obtaining consent from parents is the easier route, although it does raise the risk that one parent can either unravel the program, or that students have differing experiences based on the comfort level of each student's parents.

In the course of this due diligence, if the school finds that TrakBit, the nutritionist, the MOOC, or social media might be planning to use PII to market or sell to students (or to share the PII with a third party so that third party could market or sell to students), the school will need to follow PPRA requirements. While

[2] *See generally* U.S. Dep't Ed. & U.S. Dep't Health & Human Servs., *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPPA) to Student Health Records* (Nov. 2008), http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf.

[3] *Guide* at 3-5.

[4] *Id.* at 7.

PII under FERPA and PI under PPRA are not identical categories, a good "rule of thumb" is that any PII-sharing likely means PI is being shared too. PI is broadly defined as "individually identifiable information"—which includes names, addresses, home phone numbers, and Social Security numbers—but isn't limited to those categories.[5] Because the school has already determined that PII is being shared under this plan, it should assume that PI is being shared as well.

Under PPRA, when there are plans for students' PI to be used "'for the purpose of marketing or selling that information (or otherwise providing that information to others for that purpose),'" the school is required to notify parents of those plans, give them an opportunity to "inspect any instrument used in obtaining [personal] information," and give them an opportunity to opt-out their children from participation.[6] (It is unlikely that TrakBit's potential activities would fall into one of the exceptions for which parental notice and opt-out for marketing and selling students' personal information isn't required.)[7] However, if the school finds that TrakBit and the others will just be using any data collected for the benefit of student participants and sharing data only with the school—and the school puts a strong contract in place to ensure this arrangement—then parents probably don't need to be given PPRA's notification, inspection, or opt-out rights.

Turning now to COPPA, it appears as if students under 13 may be inputting "personal information" (PI) about themselves (as defined by COPPA) directly into commercial websites (social media). Under COPPA, the websites need to obtain parental consent if they collect PI from children under the age of 13.[8] If the websites are going to be collecting, using, or sharing the PI for any reason other than providing services to the school (which it likely will be), teacher consent cannot be substituted for parental consent.[9]

Schools aren't legally required to gain consent from students under 18, but as a matter of modeling good digital citizenship for students—that is, asking them to be aware of whom they share private information with and why—explaining the information-sharing to them and asking them to endorse it in some way (such as an "assent form," rather than the legally-binding consent form that would be given to their parents) would make sense to incorporate into the curricular plan. An "assent form" or similar device would also serve to empower students in their educational experiences.

[5] 20 U.S.C. § 1232h(c)(6)(E).

[6] *Guide* at 18.

[7] *See id.* at 17-18.

[8] *Id.* at 11-12.

[9] *Id.* at 13.

scenario two

TEABOT

“Die Susie you f*(*@)! c*&$” scream the bright red letters spray painted across the front door of Anywhere High School (AHS) in the sleepy suburb of Anywhereville, USA. This graffiti isn’t the first to deface the building during the current academic year. Every week or so, a nasty message about a student has appeared somewhere, making the whole school community anxious, tense, and hostile. The principal is worried about his students’ safety—and a little bit about the effect of the unanticipated clean-up costs on her already strapped budget. The students are worried that they will be the next target of a nasty message—or worse. The teachers are upset that the tone of the school has gotten so disrespectful and dangerous, and the parents are angry that the perpetrators have yet to be caught.

One day, the tech director receives a solicitation packet in the mail from Scholair, a company that specializes in “customized, cutting-edge, and cost-cutting technological interventions for school systems.” One of their new offerings is the TEABOT, a “robot that combines an educator’s intuition with law enforcement instincts to keep your halls safe, your students on the straight and narrow, and your budget in the black.” According to the brochure, the TEABOT can move through hallways, locker-rooms, and other non-classroom spaces more efficiently and inexpensively than human foot patrols, its video and audio sensors live-streaming back to a cloud-based program that analyzes the data in real time.

TEABOT will alert IT, the principal, and local police immediately if it sees a threat, as well as run longer-term analysis of trends in student behaviors and practices that can be used to inform staffing and programming decisions. TEABOT can also be programmed to email or text warnings to parents if their children are seen to be engaged in suspicious behavior, like cutting class or making out with another student, and to offer suggestions to teachers and school counselors about corrective actions to take for such students, like requiring a student seen smoking a cigarette to complete an online module about the risks of smoking. TEABOT’s trend analysis depends, in part, on comparing what it sees in one school with profiles of other schools where it is in use across the country. Scholair is offering a free trial run of one TEABOT for a month to AHS.

You are the tech director at AHS. Should you recommend to the principal of AHS that she give TEABOT a try? Why or why not?

Types of Ed Tech

Multiple types of ed tech are at play here: video and audio recorders, email and text alerts, and web-based teaching modules. Also, Scholair will be running data analytics on the information that TEABOT collects through video and audio recording of the school; it is likely that Scholair would also be running analytics on parental interactions with the TEABOT program—how many sign up for alerts, how many respond, etc.

Understanding who will have access to the information, and how the information will be used.

This information will be shared with Scholair. Scholair will be using the information to loop back safety monitoring updates to the school, as well as to run analytics on potential disciplinary issues and try to head them off at the pass. It will also be suggesting corrective learning modules to teachers to use with students when they do misbehave. There may be other uses as well—and this lack of knowledge should cause concern.

It's not clear if this information will be shared with any other parties through Scholair—but don't assume that this lack of clarity means that no re-sharing will occur. In fact, the opposite is more likely to be true: the lack of an affirmative commitment not to re-share on Scholair's part should suggest to you that the company is at least keeping the door open to doing so. It is important for the tech director to get additional clarity on whether any other parties will have access to the information, as well as exactly what these parties—as well as Scholair—propose to do with it.

Analyzing the level of sensitivity of the information collected or shared with other parties.

Because TEABOT is engaging in potentially unrestricted video and audio recording of the school premises, a significant amount of sensitive information will be leaving the school, including but not limited to students' private conversations, their images, and their daily routines (when they arrive on campus, which class they go to first, etc). The tech director should be prepared to discuss with the principal (and other administrators, as necessary) whether any of this sensitive student information is considered to be "personally identifiable information" (PII) from "education records" under FERPA.[1] The answer is yes: TEABOT's recordings are "materials that are 'maintained by an educational agency or institution or by a person acting for such agency or institution' and

[1] *Guide* at 2-4.

contain information directly related to a student."[2] (Note that records of a "law enforcement unit" within a school are not considered "education records" within the meaning of FERPA; however, the scenario here contemplates the principal, not a police officer, running and managing TEABOT so that exception doesn't apply.[3])

Having established that TEABOT will be keeping education records, the question now becomes whether the information is protected PII under FERPA. Much—if not all—of it will be; for instance, of particular significance here, "personal identifiers . . . such as fingerprints [and] facial characteristics" are considered PII, and TEABOT will be capturing such information in its video and audio recordings.[4]

Necessary Consents and other Privacy Protecting Measures

Both parents and students are likely to react to TEABOT with questions and mixed emotions related to privacy and safety concerns. Parents may be more likely than students to appreciate the program's safety benefits, while students might more quickly see the potential privacy intrusions. Each group, however, is likely to appreciate the potential upside (safety) and potential downside (privacy concerns) to some extent.

Because TEABOT will be capturing PII, the principal is required to get parental consent before using TEABOT or to make sure Scholair fits into the "school official" exception under FERPA.[5] Even if the principal makes such a determination, it would better cultivate parental investment and school-home trust if the principal obtained parental consent up-front.

In order to lay the groundwork for parental consent, as well as to foster a culture where students will be supportive, the tech director should advise the principal to familiarize herself with TEABOT and engage in an intra-school public awareness campaign about the TEABOT proposal to bring both parents and students on board before asking for parental consent. To be prepared to launch such a

[2] *Id.* at 2.
[3] *Id.* at 3.
[4] *Id.* at 4.
[5] *Id.* at 6-7.

campaign, the tech director should help the principal understand the positives: greater safety surveillance, real-time safety alerts, potential identification of problems before they arise, and thoughtful responses to incidents after they occur. These benefits will likely save money—TEABOT is less expensive than additional security personnel or reacting to problems after they occur—and, more significantly, create a safer school climate.

The tech director should also help the principal understand the privacy risks—both so she can attempt to prevent privacy problems from occurring (such as by entering into a negotiated, written contract with Scholair so that AHS student information is not re-shared or used for marketing or similar purposes) and so she can have thoughtful, reassuring responses as students or parents raise concerns. Privacy risks include: unknown third parties seeing PII and using it for their own purposes; creation of student and family profiles that could be used in a variety of ways—for instance, re-sold to a company that helps colleges vet potential candidates; and strengthening of the "school-to-prison" pipeline, through which many students (especially students of color) get referred to the justice system for disciplinary infractions that take place in school.

Much more information is needed to identify what data Scholair will collect, what it will do with the data, whether and with whom it will share the data, and what those potential third parties might do with the data. Other data security questions exist as well, including how long Scholair will store this data, how it will dispose of data that's no longer necessary, and how it will provide AHS access to the data to respond to parental requests for student records under FERPA or similar information needs.[6] The tech director would want to read Scholair's available Terms of Use and Privacy or other policies closely, then follow-up by asking Scholair directly for this information. Checking on education listservs to see if any tech directors or similar administrators counterparts at other schools are familiar with TEABOT could also be helpful.

In addition to the principal, the tech director should consult with an attorney or advise the principal to consult with an attorney to determine whether TEABOT is a good fit for the school. Certainly, to enter into a negotiated, written contract with Scholair for the use of TEABOT, involving an attorney is necessary. The school might also consider involving local law enforcement in the discussion; most schools have some level of police presence these days, so making sure TEABOT supports rather than intrudes upon their efforts—as well as making sure local law enforcement aren't using TEABOT to monitor students in inappropriate or invasive ways—would be valuable.

It would also be valuable to ask this attorney specifically about any applicability that COPPA and PPRA might have to the TEABOT plan. It appears unlikely that either law would apply to this scenario. High school students are typically above

[6] *Id.* at 3.

the age of COPPA applicability.[7] TEABOT's proposed activities are unlikely to count as a survey or evaluation of students not for the use of the school.[8] If it appears that Scholair might be intending to use PI (under PPRA) collected by TEABOT for marketing or advertising purposes, then PPRA requirements would apply; however, if the school does go ahead and enter into a negotiated contract with Scholair that prohibits such activities (as suggested above), then there should be no need to give parents notice, inspection, or opt-out rights.[9]

[7] *Id*. at 9.

[8] *See id.* at 17.

[9] *See id.* at 18.

scenario three

The Power of Digital Learning

Ms. Q has recently graduated from Awesome U with a Master's in Education and is eager to start teaching 7th and 8th grade math at Anywhere Middle School. During graduate school, Ms. Q took a seminar called "The Power of Digital Learning," which inspired her to embrace the use of online tools to enhance her students' learning experience in the classroom. Rather than lecturing to her students, Ms. Q has decided to have her students engage in real-time exercises in the classroom.

To do this, Ms. Q has decided to use an online tool called RockIt! that allows teachers to create interactive quizzes and problem solving games that provide students with real time feedback on their performance. The system also has preloaded problems and games that students can access both in and out of the classroom. RockIt! also tracks students' performance over time, identifying areas they have mastered, as well as areas where they could improve.

To sign up, a teacher first has to set up an administrative account with RockIt!. The administrative account allows the teacher to create quizzes, problem sets and games, as well as track her students' performance. The teacher may also create unique awards and grades that her students can accrue based on reaching certain milestones. In addition, the teacher can download and export all records regarding her students' performance on any or all tasks performed by her students, including metrics that can help the teacher track her students' individual and collective performance. These metrics can be broken out by subject matter, kind of task, type of problem, and difficulty. In addition, the teacher can cross-reference those metrics with demographic information about her students, such as gender, age, race, neighborhood, among others. A teacher can also add additional data points that may not already exist in the system. If a teacher adds any data points to her dashboard, RockIt! reserves the right in its Terms of Use and Privacy Policy to learn from what teachers are looking at and subsequently enable and offer those data points for all users in future versions of the system.

In order for students to access the system, a teacher must create accounts for each student in her class. A teacher can always access her students' dashboards. The teacher is responsible for providing usernames to each student and creating an initial password for the student. RockIt! never has access to the passwords but does have mechanisms for password retrieval if someone forgets a password. The teacher can also input the student's age, gender, home address, race, religious affiliation, and any other information the teacher would like to record in the student's account. None of this information can be seen by anyone other than the teacher and RockIt!, and RockIt! promises in its privacy policy that it will not share personally identifiable information about the students with anyone except with its third party vendors that help RockIt! deliver the services. That said, RockIt! does reserve the right to share aggregated de-indentified demographic information with third parties—including researchers, investors, schools, superintendents, and any other third party they believe would find this information useful—though RockIt! claims it would never sell this information to anyone.

The student dashboard allows a student access to all quizzes and games created by the students' teacher, as well as those offered by RockIt!. The student can also track her individual performance, see all awards and grades she has accrued, as well as see how she's doing in comparison to her peers. The comparison tool does not show individual performance, but rather provides the student with a ranking in comparison to all other members of a class. The students can also interact with each other and play games with each other to help sharpen their skills. The student dashboard also has a couple of widgets so students can automatically post reports on their successes on social media sites like Facebook and Twitter. The goal, according to RockIt!, is to inspire accountability, healthy competition, and a sense of pride in students based on improved performance. Parents do not have any access to the system as configured, unless a student chooses to share her login/password information with her parent. Parents also do not receive reports from the system on their child's performance.

Ms. Q plans to use RockIt! for all in class exercises, homework, quizzes, and tests, as she believes it will help her better track her students' performance and help her keep each student's records organized. While Ms. Q plans to keep records of any graded tests or quizzes, Ms. Q plans to delete all other records regarding her students at the end of the academic year, after final grades are delivered to students. In addition, Ms. Q hopes that her students will engage with the tool outside of the class, though students' extracurricular use of RockIt! will not count toward students' grades or assessment in any way. Finally, Ms. Q is also continuing to work with one of her former professors at Awesome U to study whether online tools can help students increase performance over time. Her goal is not only to collect information about her students' progress throughout the academic year, but also to track her students' future performance after they leave the classroom throughout high school. Ms. Q plans to share the data she collects with her former professor, as well as her professor's research assistants. Otherwise, Ms. Q does not plan to share the information with anyone else.

You are Ms. Q, and you are preparing to share your plan with your curricular director. What is the director likely to think of your plan?

Scenario Three Cheat Sheet

Types of Ed Tech

The primary ed tech involved in this plan is the RockIt! system. That said, Ms. Q should be mindful that the system provides users with access to other social media tools such as Facebook and Twitter, so these tools should also be included in the list of ed tech involved in this plan. (For thoughts on how to analyze and approach students' use of social media sites in the context of a class, please see Scenario One above.)

Understanding who will have access to the information, and how the information will be used.

In this case, Ms. Q, the students, and RockIt! will have access to the information; parents also will if their children have provided them with log-in information. With respect to RockIt!, it should be assumed that all of its personnel and subcontractors that help deliver the services may have access to the information. Before launching RockIt! in the classroom, Ms. Q should review RockIt!'s Terms of Use and Privacy Policy to understand how RockIt! will use and share the information it collects, stores, and processes through its systems.

Generally, reading the terms of use and privacy policy should be the first step for any teacher seeking to use a product similar to RockIt! with her students, as it can be the first place to identify any issues that the teacher may face based on the company's published privacy practices. (If you are a teacher and do not feel comfortable reading these documents, reach out to the appropriate administrator to be connected to your school's or district's lawyers for help understanding these documents.) Also, many school systems and districts have started pre-vetting tools and programs in order to help teachers identify "safe" and "approved" tools, which reduces the need for the teacher to navigate the contracts and privacy practices of the companies that deliver these types of tools. Using these pre-approved tools reduces the need for teachers to have to read contracts and corporate policies. Likewise, using these tools increases the likelihood that the tools will comply with FERPA, COPPA, and PPRA.

Analyzing the level of sensitivity of the information collected or shared with other parties.

Ensuring that an ed tech company has appropriate privacy practices is extremely important considering the types of sensitive information being collected, stored, and processed by these companies. For instance, in this case, RockIt! will have access to the students' performance metrics drawn from the students' engagement with any of the activities available through the system, including any quizzes, games, problem sets, etc. In addition, depending on what information Ms. Q chooses to input about her students, RockIt! could also have access to the students' ages, genders, home addresses, races, religious affiliations, and any other information Ms. Q thinks may be worth tracking. Depending on what usernames Ms. Q chooses to assign for her students, it's possible that RockIt! could have access to the students' names.

Both the performance metrics collected automatically by the RockIt! system, as well as the demographic information that can be inputted into the system, could be considered sensitive information. For instance, the performance metrics could impact a student's academic future and opportunities. Also, the demographic information can provide information about a student's background and socioeconomic status. In addition, much of this information would also qualify as personally identifiable information (PII) under FERPA.[1] For instance, a student's home address and full name would qualify as PII on their own. Further, while the other demographic information input into the system may not individually qualify as PII, in combination this information is likely to be considered PII, as it would be easy to re-identify a student with only race and gender, let alone age and religious affiliations. In a class of 20 students, even just race or religious affiliation on their own could be PII, depending on the demographic compilation of the class. In essence, the the more information added you add to this list, the more personally identifiable the information becomes.

Necessary Consents and other Privacy Protecting Measures

Because it is likely that RockIt! will have access to PII, it is likely that Ms. Q will need to obtain parental consent under FERPA, unless RockIt! falls under one of the exceptions to the consent rules. In this case, the appropriate exception would be the "school official" exception, where schools may share education records with contractors that: (i) fulfill a role the school would otherwise perform itself, (ii) are subject to the direct control of the school, and (iii) will not redisclose this information to anyone else.[2] In this case, the school would need to have a contract with RockIt! that both restricts RockIt! from using or sharing the information collected about the students for any purpose other than to provide services to the school and Ms. Q and obligates RockIt! to use commercially reasonable efforts to protect the security and confidentiality of the student information. RockIt!'s standard terms of use can qualify as this contract, assuming: (a) the contract places the necessary restrictions and obligations on RockIt! to give the school control over how RockIt! treats the student information and (b) Ms. Q is authorized to execute contracts on behalf of the school. Ms. Q should understand what the school's policies are with respect to whether she can enter into contracts on behalf of the school. If there is no policy, Ms. Q should consult with the appropriate administrator or the school's lawyer, if she has access to that lawyer. If RockIt! doesn't qualify under the school official exception,

[1] *Guide* at 3-4.
[2] *Id.* at 7.

then Ms. Q will need to obtain consent directly from the parents to use RockIt! with her students.

Generally, obtaining consent is the easiest way to ensure that use of the ed tech in the classroom will comply with FERPA. It also helps avoid any backlash from parents by making sure they understand how information about their children is being used and collected through technological tools managed and hosted by third parties. Nonetheless, relying on the consent requirement bears the risk that some students will be restricted from accessing the system while the rest of the class is able to use the tool, based solely on individual parent's perceptions and values of privacy. In these circumstances, Ms. Q will need to decide whether the tool is valuable enough to warrant the varied learning experiences amongst her students, or whether she should just abandon the program so that all students are treated equally.

In this case, where Ms. Q would like to use RockIt! as the primary learning tool within the classroom, it would seem worthwhile to take the time to enter into the appropriate contracts with RockIt!, and to conduct due diligence on RockIt!'s information practices to ensure they are aligned with the school's obligations under FERPA. In addition, as a best practice, Ms. Q could deliver notices to parents prior to launching the program in the classroom and engage parents in a Q&A to address any concerns they may have about the system. Finally, since Ms. Q has administrative power over the student accounts, Ms. Q could implement practices to help preserve as much privacy as possible while still achieving her learning goals in the classroom. These types of practices include:

- assigning anonymized or random usernames to ensure the students are not identifiable by name within the system. This way, neither RockIt! nor its third party vendors will have access to the information.
- limiting the information that Ms. Q inputs about each student to only the information she needs to achieve her research and teaching goals. Keep in mind that research goals may compel Ms. Q to input much more information than she otherwise would if she was only using the tool for teaching purposes, so Ms. Q should think about whether the privacy risk is worth it to achieve her research goals. Ms. Q should also be aware that collecting information on her students for research purposes may require her to go through IRB approval, or other approvals through the school. Likewise, Ms. Q may need to obtain additional consents from parents to collect information on the students for research purposes to comply with federal or state laws that govern the study or surveying of student subjects for research purposes. Ms. Q should connect with her principal before collecting any information for research purposes about her students. This conversation should happen before Ms. Q sets up accounts or inputs any information about the students into the RockIt!

system to ensure she shares the minimum amount of information necessary to achieve her goals.

- having students sign a privacy pledge that describes the privacy risks associated with the system; sets ground rules for how students should behave on the system, including how they interact with their peers through the system; and describes the risks of posting any information generated through the system on social media sites like Facebook and Twitter. If any of Ms. Q’s students are under the age of 13, Ms. Q may want to create a rule that does not allow students to utilize some of the tools allowing students to post information on social media sites. Likewise, Ms.Q may want to ask RockIt! if it has a version created specifically for individuals under the age of 13.

It should be noted that since Ms. Q’s students will be engaging with RockIt!’s system directly, and some of Ms. Q’s students may be under the age of 13, under COPPA, RockIt! will need to obtain parental consent if it collects PI from the students who are under the age of 13.[3] If the website is going to be collecting, using or sharing the PI for any reason other than providing services to the school outside of the school ecosystem (which it likely will be), teacher consent cannot be substituted for parental consent.[4]

In addition, Ms. Q should determine specifically whether or not RockIt! intends to use any “PI” (“personal information” under PPRA) collected from students for “‘the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose.)’”[5] Recall that, depending on what information Ms. Q chooses to input about her students, RockIt! could have access to the students’ ages, genders, home addresses, races, religious affiliations, names, and other information. While this information would not be collected from students themselves, RockIt! would be collecting other information from students’ themselves (performance metrics), which could potentially fall under the potentially broad “personal information” umbrella—especially if paired with the information Ms. Q has shared with the system. If RockIt! intends to use students’ personal information for marketing or similar purposes for “the exclusive purpose of developing, evaluating, or providing educational products or services’ for students or schools,”[6] then PPRA’s parental notice, inspection, and opt-out requirements do not apply.[7] It would still be prudent, however, for Ms. Q to inform parents and students of RockIt!’s plans so that all key stakeholders here understand the scope of any marketing or similar activities.

[3] *Id.* at 11-12.

[4] *Id.* at 13.

[5] *Id.* at 18.

[6] *Id.* at 17.

[7] *Id.*

More significantly, Ms. Q's envisioned research study could be considered a survey of the students under PPRA.[8] She is an employee of a Local Education Agency ("LEA") who plans to conduct research on student subjects using an instrument developed by a third-party (MasterIt). This could qualify as a "survey," especially if her research uses demographic information about her students and their families.[9] In such circumstances, parents need to be able to inspect and potentially opt out their children from participation.[10] Ms. Q should be prepared to explore her survey plans in detail with the curricular director and other administrators as needed for collective determination about PPRA applicability (and potentially other legal and regulatory requirements around human subjects research, such as IRB approval).[11] Once the line is crossed from a teacher's using ed tech for instructional or other curricular purposes within the school to using ed tech for research on the students that will circulate outside the school, heightened diligence must be exercised to make sure students are accorded all rights under PPRA and any other relevant legal and regulatory frameworks.

[8] *See id.* at 16.

[9] *See id.* at 16-17.

[10] *See id.* at 16-18.

[11] *See generally* U.S. Dep't Health & Human Servs., Office for Human Research PRotections, IRB Registration, http://www.hhs.gov/ohrp/register-irbs-and-obtain-fwas/irb-registration/index.html (last visited March 2, 2017).

scenario four

“What is a picture worth?”

The students at Anywhere Elementary School (AES) are very excited to be getting ready for the opening night of their school’s annual art exhibition. Every available inch of space showcases student work. Spaceship drawings are taped to the hallway ceilings; ceramic handprints line the top of the piano in the choir room; and self-portraits hang on every classroom wall.

This year, in addition to showing the work to proud parents and friends, Mr. Mather (the art teacher for third-fifth grades) has decided that his students will share their work through an online site: Littlest Masters, a for-profit, cloud-based company whose goal is to “discover and nurture tomorrow’s artistic leaders today.”

Mr. Mather has created an account for AES at Littlest Masters. To populate that account, he has already imported the name, date of birth, gender, home address, home phone number, and email address (or parental email address) of each of his students from AES’s LMS (Learning Management System). He has also included key demographic information about students’ disabilities, ethnic backgrounds, and household income. When members of the AES community and the general public look at the Littlest Masters site, only a child’s first name and school (AES) will be visible, along with the art. But Littlest Masters will have full access to the detailed information that Mr. Mather has shared, as will Mr. Mather himself.

On opening night of the art show, he plans to hand out instructions to all parents and guardians in attendance that tell them how to take pictures of their child’s work, upload them, and tag them with their child’s name. If parents and guardians choose, they can create their own personal user account at Littlest Masters through which they can order products (mug, keychain, etc.) emblazoned with their child’s artwork. These accounts are free, but the products cost money. All profits are retained by Littlest Masters.

Littlest Masters claims that it will conduct a “machine-based review” of all the uploaded art to “identify nascent talent and connect this talent with scholarships and other rewarding opportunities, including to do drawing and design work for some of our country’s leading businesses.” For every student identified as talented by Littlest Masters, AES will win points that it can cash in for art and other curricular supplies.

You are the head of the art department. You find out about Mr. Mather’s plan two hours before the opening night festivities start. What do you do?

Scenario Four Cheat Sheet

Types of Ed Tech

The primary type of ed tech at play here is a cloud-based program (Littlest Masters), which will aggregate and ultimately analyze large amounts of student data. There is also a parental BYOD (Bring Your Own Device) component because parents will be using their own devices to take pictures and upload them to Littlest Masters; thus, while parents' phones and tablets may not generally be thought of as ed tech, they essentially are in this scenario.

Understanding who will have access to the information, and how the information will be used.

Student work (art) and information is going to be shared outside the school with Littlest Masters (name, address, contact information, demographic information, gender, etc.). Both Mr. Mather and Littlest Masters will have full access to the student information that Mr. Mather shares, as well as images of the art that the parents share. It appears likely that Littlest Masters will be sharing some of the student information and images with third parties in order to link students up with scholarship and employment opportunities, as well as potentially to fulfill any art orders that the parents place. Because the potential for re-sharing exists, it would be important for the art department head to have Mr. Mather— likely in conjunction with colleagues, such as a tech director or other relevant administrator—determine what privacy policies, terms of use, and other practices Littlest Masters has around re-sharing art images and student information.

Analyzing the level of sensitivity of the information collected or shared with other parties.

All of the information and images being shared with Littlest Masters should be understood as sensitive because of the details of students' personal and familial lives included, such as disability status and income level. Even seemingly less intimate information—such as students' names—should still be considered sensitive because it allows an audience outside of the school (Littlest Masters) to identify students.

By using Littlest Masters, AES is potentially creating positive opportunities for students and their families, including a free repository for student artwork, the opportunity to create and own products developed from this artwork (for a fee), and connections for students with scholarship options. That said, using Littlest Masters in this context bears some risk. Mr. Mather has populated the system with highly sensitive information about each student. This decision could be problematic depending on how secure Littlest Masters' systems are and with whom Littlest Masters shares the information. In addition, depending on Littlest Masters' privacy policy, students' information and artwork could be used to profile the students, not only with respect to talent and potential, but for targeted marketing or advertising. The analytics Littlest Masters conducts could also result in profiling that students and their families are not aware of, do not have easy access to, and could be deleterious or even discriminatory (since gender, ethnicity, disability, and other identity characteristics are being shared).

Even though the clock is ticking, the department head should not proceed with his plan without first analyzing AES's responsibilities to protect the privacy of the information and images. A key step will be consultation with administrative colleagues to determine whether any of this sensitive student information and images is considered to be "personally identifiable information" (PII) from "education records" under FERPA.[1] All of the information being shared here qualifies as PII from education records because it is either a direct identifier (such as students' names) or an indirect identifier (such as date of birth) that was obtained from the school's learning management system. The status of the images is more ambiguous because they may not qualify as an "education record." Further, it's possible that a particular image would not contain any information that would directly tie the work to a particular student. However, it would be prudent to treat all the images as if they did contain PII because some images could well contain such information (for instance, imagine a student's self-portrait with accompanying personal narrative), thus casting a broader net is efficient and prudent. That parents rather than the school are sharing the images with Littlest Masters doesn't alter the status of the images as education records with PII, although it affects the type of consent needed for the image sharing, as discussed below.

Necessary Consents and other Privacy Protecting Measures

Because PII is being shared with third parties (Littlest Masters and possibly others), it is possible that parental consent would be required under FERPA before student information or images were shared with Littlest Masters.[2] The next step is to determine whether this sharing is covered by one of the exceptions to the consent requirement in the statute (directory information and "school official" exceptions).

While some of the information Mr. Mather has shared with Littlest Masters prior to the art show would be covered by the directory information exception (chiefly name and address), not all of it would be. Mr. Mather may believe that involving parents in the Littlest Masters program (by having them take and upload pictures of their children's artwork to the site) implicitly fills the role of parental consent. While this is an understandable opinion, it is not legally sound for two reasons. First, it doesn't appear that Mr. Mather obtained parental consent for the PII

[1] *Guide* at 2-4.

[2] *Id.* at 4.

he uploaded to Littlest Masters prior to the art show night, thus he should have obtained parental consent prior to uploading the non-directory PII to the Littlest Masters system. Second, FERPA requires parental consent to be in writing—not implied—and must include the details about the education records that will be shared, why they will be shared, and with whom they will be shared.[3] Thus even if parents became aware at the time of the art show that Mr. Mather had previously shared students' PII and didn't express any concerns about it, such lack of concern would not qualify as consent for the purposes of FERPA.

Other than the directory information exception, the most likely exception that Mr. Mather may be able to rely on for sharing PII without parental consent would be the legitimate school official exception. Under this exception, schools may share education records with contractors that fulfill a role the school would otherwise perform itself, provided that the contractors are subject to the direct control of the school, and do not redisclose this information to anyone else.[4] For this exception to be valid, AES would need a contract in place with Littlest Masters requiring Littlest Masters to use only students' information and images as necessary to provide services to the school and restricting Littlest Masters from sharing the information with any other third party. Since it doesn't appear that Mr. Mather has entered into such a contract prior to the art show, this exception would be unlikely to be valid.

In terms of the images themselves, because parents rather than the school are sharing them, it is most likely up to parents to review Littlest Masters' terms of use, privacy policies, and other relevant policies themselves and make their own decisions about whether or not to share their children's work. FERPA does not control what parents choose to do—or not do—with their children's education records, thus AES does not have a legal obligation to get FERPA-compliant consent (or rely on an exception from the consent requirement) from parents before the parents themselves share education records. However, AES has created the accounts, so it is possible that the school could be understood as "owning" the account, even if the parents are choosing whether or not to upload the images. Regardless of the impact of potential account ownership, in order to maintain open communication with parents, as well as to model sound digital citizenship (including privacy practices), it would be prudent for AES to have reviewed Littlest Masters' relevant policies and terms themselves, provide a summary of them to parents at the time of the show, and flag for parents why and how AES is recommending that they use Littlest Masters. (Note that even though Littlest Masters is subject to COPPA's requirements, because parents rather than children are interacting with the site, AES does not need to be concerned about COPPA in this scenario—although it should make clear to parents at the show that they, not their children, are expected to engage the site.)

It seems likely that Littlest Masters may be planning to market or advertise to students at some point; for instance, Littlest Masters might promote certain

[3] *Id.* at 4.

[4] *Id.* at 7.

products for parents to order with their children's artwork on them or promote particular scholarships or related opportunities for which students could apply. To the extent that there may be such marketing or advertising connected to students' PI, PPRA kicks in and provides parents with certain rights—unless an exception applies. For commercial activities like promoting certain art items to purchase, no PPRA exception would apply, so AES would be required to notify parents of those plans, give them an opportunity to "inspect any instrument used in obtaining [personal] information," and give them an opportunity to opt-out their children from participation.[5] However, marketing or advertising of scholarships for post-secondary education would most likely come under the "college recruitment" exception, so parental notice, inspection, and opt-out would not be required for that specific category of marketing or advertising activities.[6] Here again, it is crucial to read Littlest Masters' privacy policies, terms of use, and any other relevant policies to determine Littlest Masters' proposed activities as much as possible.

The tight timeline—with the show just a few hours away—is tricky. On the one hand, it's important to support educators' thoughtful innovations with their students (which Mr. Mather has done here); on the other, it's crucial for AES to ensure that sensitive student information does not get shared with third parties absent full legal compliance, as well as compliance with best practices around parental communication and digital citizenship. The most prudent course of action would be to have Mr. Mather remove the PII and PI he has already shared from Littlest Masters (and have an informed tech administrator follow-up with Littlest Masters to ensure that it is indeed fully removed) and remove the Littlest Masters component of the art show until the vetting described above can happen and AES can proceed either with a negotiated contract in place (to use the legitimate school official exception to share PII and establish PPRA compliant limitations on marketing or advertising) or to get informed parental consent—perhaps a follow-up show with a Littlest Masters add-on could take place in a few days or weeks.

[5] *Id*. at 18.

[6] *Id.*

scenario five

Schoolhouse Rocked

Ms. Spano, the coach of the Anywhere High School (“AHS”) field hockey team, has a big problem. She’s been hearing rumors that her student athletes are “body-shaming” each other on social media. She hasn’t seen it, but parents have reported that certain team members are taking indecent pictures of other team members in the locker room and posting them on various social media sites with derogatory hashtags, like #fatslut or #movefatass.

This kind of behavior is bad for morale, as well as a flagrant violation of the AHS code of student conduct that bans hazing and harassment in all its forms. Ms. Spano believes that disciplinary action needs to be taken, but she has no proof of wrongdoing and no knowledge of the wrongdoers’ identities.

Eager for more information—but wanting to avoid actually seeing any of the pictures themselves, even if they’re publicly available—Ms. Spano does some online research of her own. She learns about a company called “Eyesback” (motto: “we have eyes in the back of our head—and everywhere—so you don’t have to.”). Eyesback is designed for use by schools. It promises to monitor publicly available social media accounts related to a given school for evidence of undesirable activity. It also says it can monitor the content of all Internet traffic over all AHS issued devices (laptops, iPads, etc.) from any location so that it can mine even privately available posts from those sources for inappropriate content. Eyesback is free for schools to use for the first six months, then carries a small fee. Eyesback will notify school administrators via email or text if inappropriate content is detected.

You are the head of the AHS IT Department. Ms. Spano approaches you to propose that AHS start using the free trial of Eyesback. What’s your response?

Scenario Five Cheat Sheet

Types of Ed Tech

Eyesback is a cloud-based monitoring program that analyzes students' social media use. AHS devices issued to students are also involved. Because it looks at publicly available posts from any source, it effectively turns students' personal devices (laptop, tablet, phone) used to make publicly available posts from any location into a type of ed tech because AHS is, to an extent, interacting with them.

Understanding who will have access to the information, and how the information will be used.

Eyesback (a third party) will have access to two categories of information: (1) all publicly available social media posts relating to AHS, and (2) all social media posts through AHS issued-devices. Eyesback represents that it will be monitoring the posts for inappropriate content but, based on the information Ms. Spano has obtained to date, a few key aspects of Eyesback's services are unclear, including: whether Eyesback will use any additional parties or services to assist with the monitoring, as well as whether Eyesback (or any additional parties) will use the social media content it obtains for any uses other than informing the school of inappropriate content. It is also unclear what data or metadata, other than social media posts, from AHS-issued devices Eyesback may be able to access. As head of AHS IT, you would want to obtain answers to these questions in order to inform your decision about whether or not to take the Eyesback free trial.

Analyzing the level of sensitivity of the information collected or shared with other parties.

It is unclear what the level of sensitivity will be in the social media posts, as students generate that content themselves and may choose to converse about anything and everything from cute cat pictures to serious mental health issues. It seems likely that the publicly available posts will be less sensitive than ones that may be set to private but sent on AHS-issued devices; however, students do sometimes post sensitive things publicly.

Necessary Consents and other Privacy Protecting Measures

FERPA does not clearly control AHS's choices here; however, it is still important for AHS to conduct a thorough and thoughtful privacy analysis before taking the Eyesback trial. (COPPA does not apply because students are over 13.)

As you recall, FERPA only applies to education records, so the first question is whether Eyesback is getting access to AHS students' education records. Publicly available social media posts sent from a student's own device are not education records: they are student generated content that relate to school only in that they mention school in the course of students' own speech. The status of privately available social media posts sent from AHS-issued devices is a trickier question. On the one hand, it's a stretch to say that students' private social media posts are somehow "maintained by an educational agency or institution"[1] (as required to be an education record) because they are student generated content that the students themselves are choosing to share; on the other, if the posts are being done on AHS-issued devices, and AHS maintains control over those devices, then arguably anything students do via those devices may become an education record (as presumably all activity over those devices contains information directly related to them).

To be prudent, AHS should make sure it either has parental consent for any Eyesback monitoring or enters into a contractual agreement sufficient to satisfy the legitimate school official exception (see above analysis in scenario 4).

AHS should also be mindful about the PPRA "rule of thumb" as it relates to FERPA (introduced in scenario 1 above). As you may recall, while PII under FERPA and PI under PPRA are not identical categories, a good "rule of thumb" is that any PII-sharing likely means PI is being shared too. PI is broadly defined as "individually identifiable information"—which includes names, addresses, home phone numbers, and Social Security numbers—but isn't limited to those categories.[2] Because the school has already determined that PII may well be shared under Eyesback's proposed services, it should assume that PI is being shared as well. Also, because the school has already determined that it is not sure what uses—if any—Eyesback might have for PII beyond monitoring, the school should assume that Eyesback might also use PI for purposes other than monitoring. For PPRA, the key question is whether Eyesback might be planning to use PI to market or sell to students (or to share the PI with a third party so that third party could market or sell to students). If the answer is yes (or isn't clearly no), the school will need to follow PPRA requirements.

Under PPRA, when there are plans for students' PI to be used "'for the purpose of marketing or selling that information (or otherwise providing that information to others for that purpose),'" the school is required to notify parents of those plans, give them an opportunity to "inspect any instrument used in obtaining [personal] information," and give them an opportunity to opt-out their children from participation.[3] (It is unlikely that Eyesback's potential activities would fall into one of the exceptions for which parental notice and opt-out for marketing and selling students' personal information isn't required.)[4] However, if the school finds

[1] *Guide* at 2.

[2] 20 U.S.C. § 1232h(c)(6)(E).

[3] *Guide* at 18.

[4] *See id.* at 17-18.

that Eyesback would just be using any data collected for the benefit of student participants and sharing data only with the school—and the school puts a strong contract in place to ensure this arrangement—then parents probably don't need to be given PPRA's notification, inspection, or opt-out rights.

Perhaps more significantly, AHS should engage in a multi-stakeholder decision-making process around its shared values around privacy, autonomy, free speech, and other normative commitments to (1) identify shared values and (2) determine whether or not using Eyesback furthers or erodes those values. In addition, AHS should strongly consider engaging in a more robust digital citizenship curriculum with its students than it perhaps has to date. Students can often find ways around any school monitoring or filtering programs, thus monitoring—even if FERPA compliant—is at most a bandaid fix. If AHS students are determined to engage in inappropriate speech, they will find a technology that enables them to do so; the key is to deepen their respect for themselves, others, and the school itself such that they choose their words more carefully.

conclusion

As the twenty-first century digital learning revolution continues, the role for ed tech in classrooms and school systems will only continue to grow and evolve. Engaging in collaborative, thoughtful deliberations around the adoption and use of ed tech will help support outcomes that respect student privacy while embracing both the efficiencies and innovations that ed tech has to offer. Multi-stakeholder conversations—such as the ones reflected in the above learning experiences—are essential to this process. The discussion questions you reflected on with these five fictional scenarios will translate smoothly into facilitating conversations about the many exciting real-world ed tech options that will come before you and your colleagues. While such conversations might feel initially confusing or unsettling, they will quickly become a regular and welcome part of building your learning community now and in the future.

acknowledgements

The authors wish to thank their colleagues on the Youth & Media team at the Berkman Klein Center for Internet & Society at Harvard University for their support of and contributions to this work, with special thanks to Urs Gasser, Sandra Cortesi, Andres Lombana-Bermudez, Crystal Nwaneri, David Cruz, Alissa Wang, and Amanda Kraley. We are also grateful for the input of external colleagues, especially those at iKeepSafe and the educators who participated in their professional development workshops and provided feedback on drafts of this work. This work was developed with valued support from the Digital Media and Learning Trust Challenge, which is supported by the MacArthur Foundation and administered by HASTAC.

BERKMAN
KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

Youth and Media