NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 24, ISSUE 1: OCTOBER 2022

EDTECH IN HIGHER EDUCATION: PROTECTING STUDENT DATA PRIVACY IN THE CLASSROOM

Patricia M. Sheridan, J.D.*

The COVID-19 pandemic forced students to abruptly shift from the classroom environment to an online mode of learning, and teachers scrambled to find creative solutions to deliver their course content in a virtual format. Months of school lockdowns sparked an explosion in the use of educational technologies, and many of the cloud-based tools, mobile applications, and online platforms that were initially viewed as temporary solutions are now firmly embedded in the student learning experience. The privacy implications of the widespread use of educational technology for students in grades K–12 has been discussed extensively by researchers, but the impact on students in higher education has not received much attention. Protocols for adopting educational technology in the K–12 environment are generally robust, but professors teaching in higher education are free to independently select course materials and electronic resources for their courses. Faculty members often require students to use free and easily downloadable educational technologies to complete class activities, effectively compelling students to accept the vendor's policies concerning the usage of their personal information. The cumulative effect of ad hoc class-level decisions by faculty members in higher education increases the potential for violations of the Family Educational Rights and Privacy Act of 1974 and can ultimately lead to the serious erosion of data privacy for college students. Faculty members, as front-line decision makers regarding data collection practices that affect students, can play a key role in improving privacy awareness among college students and strengthening privacy protections across higher education institutions.

* Associate Professor of Law, O'Malley School of Business, Manhattan College, Riverdale, New York.

TABLE OF CONTENTS

I. INTRODUCTION

The abrupt shift to remote learning prompted by the COVID-19 pandemic forced educators at all levels to quickly adapt to teaching their classes in a different format. In an effort to more actively engage students in the new virtual learning environment, teachers were eager to integrate educational technologies and online resources into their courses. Some of the learning tools accessed by teachers and their students were immediately downloadable for free, and the ease of using these products often overshadowed any potential concerns regarding the data collection and privacy practices of the service providers.

When an academic institution adopts an educational technology or learning platform for school-wide use, the contractual agreement between the institution and the vendor typically undergoes review by appropriate school administrators to ensure that the vendor's

policies comply with applicable laws. Educational technology adopted specifically for use in the classroom, however, is not subject to similar scrutiny. Faculty members in higher education have greater autonomy than K–12 teachers regarding the selection of individual course materials and resources. A college faculty member may decide unilaterally to use specific software or a mobile learning application in their class, with little oversight by school administrators. The ease of accessing these online educational technology products often leads faculty members to overlook the vendor's stated policies regarding the collection, storage, and management of students' data. By requiring students to access third-party electronic resources to complete class activities, the faculty member imposes the vendor's privacy policies on students regardless of whether or not the vendor has appropriate protections in place for consumers' data. In light of the increasing use of educational technology in the higher education classroom, the cumulative effect of ad hoc decisions by individual faculty members can lead to a serious erosion of students' rights to data privacy. Frequent independent adoptions of educational technologies by faculty may contribute to a sense of complacency about privacy among college students by normalizing the routine granting of consent to numerous service providers' data collection practices.

In the higher education setting, classroom-level decisions regarding the use of educational technology place individual professors in a key position to make decisions regarding data collection practices that affect their students. Faculty members play a crucial role in managing third-party risk and protecting student privacy, but many do not appreciate the significant privacy implications associated with their decisions.

Part I of this Article provides an overview of student data privacy within the framework of the Family Educational Rights and Privacy Act of 1974 ("FERPA")[1] and explains the three main loopholes that permit the sharing of students' personal information with outside vendors. Part II explores popular types of educational technologies and compares the privacy policies contained in institution-level vendor agreements with those typically included in

[1] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

clickwrap agreements, which are often utilized for class-level adoptions. Part III highlights the inherent differences between the K–12 and higher education settings in terms of teacher autonomy and explains how these variations foster an environment that leads to numerous ad hoc decisions by individual faculty members to use course-specific educational technology at the higher education level. Part IV examines faculty class-level adoptions of educational technology within the framework of FERPA and argues that the statutory exceptions that typically permit academic institutions to share student information with third party vendors do not squarely apply to course-specific educational technologies accessed via clickwrap agreements. Part V emphasizes the important role that faculty members play in protecting student privacy and recommends strategies that can be implemented within the classroom to draw students' attention to the complex issues surrounding data privacy. Part V also offers suggestions for strengthening privacy protections across campuses to raise privacy awareness and to curb downstream uses of student data.

II. STUDENT DATA PRIVACY

Beyond student academic records and transcripts, higher education institutions collect and store vast amounts of private information about students from various sectors of campus life.[2] For example, students receiving tutoring or other forms of academic support at a campus resource center may divulge personal information regarding learning disabilities and accommodation plans. Students visiting the on-campus health or counseling center may reveal medical and psychological conditions, as well as substance abuse problems. Financial transactions through the Bursar's office and purchases at the college bookstore or in the cafeteria often involve personal credit card and financial information. A student who swipes to enter the library, residence hall, or a campus office building reveals information about their

[2] Merritt Neale & Matthew Tryniecki, *The Post-Pandemic Evolution of Student Data Privacy*, EDUCAUSE (Aug. 10, 2020), https://er.educause.edu/articles/2020/8/the-post-pandemic-evolution-of-student-data-privacy [https://perma.cc/HHG5-UHLP] (listing various data collection points for a typical college or university student in a single day).

whereabouts at certain times of the day. Within the classroom, individual faculty members generate student data by posting students' grades and assignments online, by tracking attendance, and by electronically reporting academic warnings for struggling students.

Colleges and universities routinely release students' personal information to external service providers that are hired to perform specific functions on behalf of the school.[3] A school may outsource the payment processing for their bookstore and dining services or contract with a vendor to deliver a learning management system that can track students' grades, attendance, and performance. Some of these data sharing transactions between academic institutions and external service providers implicate major federal privacy-oriented regulations, such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[4] and the Gramm-Leach Bliley Act of 1999 ("GLBA"),[5] but the primary federal regulation addressing student privacy is FERPA.[6]

A. FERPA Overview

In 1973, the U.S. Department of Health, Education, & Welfare recommended "the enactment of a federal 'Code of Fair Information Practice' for all automated data systems containing information about individuals."[7] The Code of Fair Information Practice ("FIP")

---

[3] Jon Marcus, *More Colleges and Universities Outsource Services to For-Profit Companies*, HECHINGER REP. (Jan. 8, 2021), https://hechingerreport.org/more-colleges-and-universities-outsource-services-to-for-profit-companies/ [https://perma.cc/58GN-GFAX] (noting public and non-profit colleges and universities are "paying tens of billions of dollars a year to for-profit corporations to create and operate online courses, recruit and enroll students, advise and tutor those students once they start school, oversee research, manage information technology and utilities[,] and build or manage dorms, classrooms, labs, parking[,] and student unions").

[4] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[5] Gramm-Leach Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in relevant part primarily as 15 U.S.C. §§ 6801–09, §§ 6821–27).

[6] 20 U.S.C. § 1232g.

[7] *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, U.S. DEP'T OF

created five basic principles or safeguards for automated personal data systems, namely:

> 1. There must be no personal data record-keeping systems whose very existence is secret;
>
> 2. There must be a way for an individual to find out what information about him is in a record and how it is used;
>
> 3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent;
>
> 4. There must be a way for an individual to correct or amend a record of identifiable information about him; and
>
> 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[8]

These core principles provide an ethical framework for various sets of FIPs that have been adopted around the world by various entities and organizations.[9]

The privacy framework under FERPA is based on the five FIP principles with an emphasis on access, notice, and consent to the disclosure of personally identifiable student information.[10] FERPA applies to "educational institutions"[11] that maintain students' "educational records."[12] FERPA protects a student's "Personally Identifiable Information" ("PII") which includes:

HEALTH, EDUC., & WELFARE (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/L2PB-AUXD].

[8] *Id.* at xx–xxi.

[9] In its 1998 report to Congress, the Federal Trade Commission named five core principles of privacy protection, namely: (1) notice/awareness; (2) choice/consent; (3) access/participation; (4) integrity/security; and (5) enforcement/redress. *Privacy Online: A Report to Congress*, FED. TRADE COMM'N 10 (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/T3K2-R2YC].

[10] 20 U.S.C. § 1232g.

[11] § 1232g(a)(3). This provision defines an educational agency or institution as "any public or private agency or institution which is the recipient of funds under any applicable program." *Id.*

[12] § 1232g(a)(4)(A). This provision states that the term "education records" means, except as may be provided otherwise in subparagraph (B), those records,

> (a) The student's name;
>
> (b) The name of the student's parent or other family members;
>
> (c) The address of the student or student's family;
>
> (d) A personal identifier, such as the student's social security number, student number, or biometric record;
>
> (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
>
> (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
>
> (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.[13]

Parents can exercise FERPA rights on behalf of any child under the age of eighteen, but students gain access to their own educational records on their eighteenth birthday or upon entry to a post-secondary academic institution.[14] Under FERPA, educational institutions must grant parents or eligible students access to the educational records upon request and provide an opportunity to contest any erroneous information contained in the record.[15] Educational institutions may not disclose a student's educational records or the student's PII absent the parent's or eligible student's consent, unless a statutory exception exists.[16] Educational institutions must also provide parents or eligible students with an annual notification detailing the various rights under FERPA.[17]

---

files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution. *Id.*

[13] 34 C.F.R. § 99.3.

[14] 20 U.S.C. § 1232g(d). This section provides: "For the purposes of [FERPA], whenever a student has attained eighteen years of age, or is attending an institution of postsecondary education, the permission or consent required of and the rights accorded to the parents of the student shall thereafter only be required of and accorded to the student." *Id.*

[15] § 1232g(a)(1)(A).

[16] § 1232g(b).

[17] 34 C.F.R. § 99.7(a)(1).

B. Key Exceptions Under FERPA

While FERPA generally prohibits the disclosure of a student's PII to a third party,[18] consent to disclosure is not required where the student's records are shared with other "school officials"[19] or when the disclosure involves solely "directory information."[20] In addition, FERPA does not restrict the release of "de-identified" student records where all PII has been removed.[21] When taken together, these three FERPA loopholes allow the release of a significant amount of student information to third parties.

FERPA's "school official" exception permits an educational institution to disclose a student's PII without first obtaining consent from a parent or eligible student if:

> (A) The disclosure is to other school officials, including teachers, within the agency or institution whom the agency or institution has determined to have legitimate educational interests.
>
> (B) A contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions may be considered a school official under this paragraph provided that the outside party--
>
> (1) Performs an institutional service or function for which the agency or institution would otherwise use employees;
>
> (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and
>
> (3) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.[22]

The term "school official" is broadly construed to encompass outside vendors, contractors, and suppliers hired by the institution to perform functions normally performed by the institution's own employees, provided that the outside vendor is under the direct control of the institution and is subject to general prohibitions

[18] 20 U.S.C. § 1232g(b).
[19] 34 C.F.R. § 99.31(a)(1)(i)(A).
[20] 20 U.S.C. § 1232g(a)(5)(A).
[21] 34 C.F.R. § 99.31(b)(1).
[22] § 99.31.

regarding the use and redisclosure of a student's PII.[23] The "direct control" requirement is deemed to be satisfied where "the disclosing entity requires the recipient, pursuant to a written agreement, to use reasonable methods to protect student information, only use information for the authorized purpose, and destroy the information when it is no longer needed."[24] However, in practice, the school official exception under FERPA permits educational institutions to delegate the obligation to protect students' PII to the various vendors and suppliers hired by the educational institution, so long as these vendors in turn use reasonable methods to protect students' PII.[25] A school official receiving PII may not redisclose the PII from a student record without prior consent, and FERPA requires that "the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student."[26]

FERPA's second major exception pertains to the sharing of a portion of the student's educational record considered to be "directory information." Directory information is normally not considered harmful if disclosed, and includes the following:

> The student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended.[27]

A student's directory information can be shared without consent, but an educational institution must provide a notice that explains the type of PII designated as directory information and must provide students with the right to opt-out of or restrict the release of directory information, as well as a description of the timeframe to exercise the

---

[23] § 99.31(a)(i)(1)(B)(2) (noting that recipients must be "under the direct control of the agency or institution with respect to the use and maintenance of education records").

[24] Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPS,* 8 DREXEL L. REV. 339, 371 (2016) (online corrected).

[25] *See id.*

[26] 34 C.F.R. § 99.33(a)(1).

[27] § 99.3(a).

right.[28] Although students have a right to opt-out of sharing directory information, the required consent is usually implied by merely including a notice to that effect within the institution's annual FERPA notice to students.[29] Educational institutions do not have to record the specific disclosures of directory information or the disclosures made pursuant to the school official exception,[30] provided their general practices are described in their annual FERPA notice.[31]

The third major loophole under FERPA permits an educational institution or third party receiving students' information to release de-identified records and information.[32] De-identification occurs "after the removal of all personally identifiable information provided that the educational agency or institution or other party has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information."[33] Since de-identified data does not involve a student's PII, FERPA does not restrict its release.

There is no single method that must be followed in order for data to be considered sufficiently de-identified, but "properly performed de-identification involves removing or obscuring all identifiable information until all data that can lead to individual identification have been expunged or masked."[34] To determine whether data have

---

[28] 20 U.S.C. § 1232g(a)(5).

[29] 34 C.F.R. § 99.31(a)(1)(ii); § 99.34(a)(1)(ii).

[30] § 99.32(d)(2).

[31] § 99.7(a)(3)(iii) (stating that, if the educational agency or institution has a policy of disclosing education records under § 99.31(a)(1), the annual notice must include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest).

[32] § 99.31(b)(1).

[33] *Id.*

[34] *Data De-Identification: An Overview of Basic Terms,* PRIV. TECH. ASSISTANCE CTR. (Oct. 2012), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf [https://perma.cc/VAY6-SVTW]. *See also Guidelines for Data De-Identification or Anonymization,* EDUCAUSE (July 2015), https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/guidelines-for-data-deidentification-or-anonymization [https://perma.cc/LBK5-TZC8] (last visited July 20, 2022)

been sufficiently de-identified, the cumulative re-identification risk from all previous data releases must be considered, as well as other available information, including directory information and other de-identified data releases.[35] FERPA does not prevent a party receiving student PII, including a vendor under the school official exception, from further sharing de-identified student data.[36]

III. EDUCATIONAL TECHNOLOGY AND METHODS OF ADOPTION

Educational technology ("edtech") broadly refers to a wide array of computer software, mobile applications ("apps"), and web- or cloud-based tools that are used to enhance teaching and learning and to improve student education.[37] According to a funding database compiled by EdSurge, edtech startups in the United States raised over $2.2 billion in venture capital and private equity financing across 130 deals in 2020, which marks the highest investment for the U.S. edtech industry in a single year.[38] Some types of edtech, such as record keeping or learning management systems, are intended for school-wide application and are meant to be deployed across an entire academic institution. Other types of edtech products are designed as student engagement tools with targeted functions, making them more suitable for use by individual teachers for a

(describing subtle differences between de-identification, anonymization, and sanitization of data).

[35] EDUCAUSE, *supra* note 34.

[36] *See* 34 C.F.R. § 99.31(b)(1) (stating "a party that has received [de-identified] records and information . . . may release the records or information without the consent" of an eligible student or guardian).

[37] *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices,* PRIV. TECH. ASSISTANCE CTR. (Feb. 2014), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf [https://perma.cc/36CD-NKZR] [hereinafter *PTAC Requirements and Best Practices*] (explaining that online educational services, or "edtech," refers to the broad category of tools and applications provided by a third party that students access via the internet and use as part of a school activity).

[38] Tony Wan, *A Record Year Amid a Pandemic: US Edtech Raises $2.2 Billion in 2020,* EDSURGE (Jan. 13, 2021), https://www.edsurge.com/news/2021-01-13-a-record-year-amid-a-pandemic-us-edtech-raises-2-2-billion-in-2020 [https://perma.cc/5CUK-NBEH].

particular class. Regardless of whether the edtech adoption occurs on a school-wide or class-specific basis, FERPA applies if students' personal information is shared with an outside service provider.

A. Institution-Level Edtech Adoptions Pursuant to Written Vendor Agreements

Some edtech companies partner with higher education institutions to deliver products that can be integrated with a school's student information system.[39] Prior to utilizing edtech on a school-wide basis, institutions usually enter into detailed, written service agreements with vendors.[40] These written agreements typically undergo some type of internal review by school administrators and are adopted only after strictly-followed approval protocols.[41] The institution-level contract review often initially verifies that the vendor meets the definition of a school official, as set forth in the school's annual FERPA notice.[42] The evaluation also confirms that provisions restricting the vendor's subsequent release of student data are included and that the vendor's further uses of

---

[39] Student information systems "manage student data, including but not limited to registering students in courses, managing grades, transcripts, and student test data." *Student Information Systems*, EDUCAUSE, https://library.educause.edu/topics/administrative-and-business-services/student-information-systems [https://perma.cc/YW7C-Z4U9] (last visited Sept. 28, 2022). Some of the largest learning management systems used in higher education systems include Canvas by Instructure, Blackboard Learn by Anthology (Blackboard), and Moodle. *See Higher Education Learning Management Systems Reviews and Ratings*, GARTNER, https://www.gartner.com/reviews/market/higher-education-learning-management-systems [https://perma.cc/PGR5-UTUR] (last visited July 20, 2022).

[40] Nadine Sterne, *Privacy and Confidentiality: Holding IT Service Providers Accountable, 2009* EDUCAUSE CTR. FOR APPLIED RSCH. (Nov. 3, 2009), https://library.educause.edu/-/media/files/library/2009/11/erb0922-pdf [https://perma.cc/C7AF-5J98] (providing sample service provider contract provisions to protect the confidentiality of college data).

[41] *See PTAC Requirements and Best Practices, supra* note 37, at 8 (noting most schools or districts have procedures and processes in place for evaluating vendor contracts for privacy and security considerations).

[42] 34 C.F.R. § 99.7(a)(3)(iii).

student data are limited to educational purposes.[43] When appropriately crafted, written contractual obligations between the institution and an external vendor have been found to demonstrate the requisite "direct control" needed to satisfy the school official exception for purposes of FERPA.[44]

While FERPA does not specifically mandate written agreements between service providers and academic institutions, contract obligations limiting the potential uses of student data are the most common way that schools can assure vendors' handling of student data are FERPA-compliant.[45] Absent a separately negotiated written agreement, the edtech provider's standard privacy policies apply, and these tend to impose only minimal restrictions on how student information can be used. For example, Ellucian is a global technology company that provides services to higher education institutions around the world.[46] Ellucian's products include various technology platforms for managing student records and transcripts, such as the Banner, Degree Works, and Workflow systems, that are used on an institution-wide basis.[47] Regarding the redisclosure of acquired data, Ellucian states the following in their online privacy notice:

> Ellucian processes Personal Data that its customers have chosen to share with Ellucian. Ellucian has no direct or contractual relationship with the subjects of this Personal Data (the "Customer Data Subjects"). As a result, when customer data includes Personal Data, the customer is solely

---

[43] *See PTAC Requirements and Best Practices, supra* note 37, at 9–10 (recommending that schools and districts include certain provisions in written vendor agreements as a way to maintain direct control over students' data).

[44] *See id.* at 4 (pointing out the possibility that the standard terms of service agreement for an online educational service might also "contain all of the necessary legal provisions governing access, use, and protection of the data, and thus may be sufficient to legally bind the provider to terms that are consistent with these direct control requirements").

[45] *See id.* ("While FERPA regulations do not require a written agreement for use in disclosures under the school official exception, in practice, schools and districts wishing to outsource services will usually be able to establish direct control through a contract signed by both the school or district and the provider.").

[46] *About Us*, ELLUCIAN, https://www.ellucian.com/about-us [https://perma.cc/GLA8-NRJX] (last visited July 20, 2022).

[47] *All Products*, ELLUCIAN, https://www.ellucian.com/solutions/all-products [https://perma.cc/HUD8-U8GQ] (last visited July 20, 2022).

> responsible for satisfying all legal obligations owed directly to Customer Data Subjects under applicable data protection laws.[48]

The policy further states Ellucian shares personal data with "subcontractors, business partners and third-party agents and contractors only to the extent required in order to deliver products or services requested by customers."[49] Ellucian's standard privacy provisions state that the liability for protecting students' PII rests with Ellucian's customers, but make it clear that individual contracts between Ellucian and academic institutions containing different terms regarding protection of personal data supersede any conflicting terms in their privacy notice.[50] Although FERPA's school official exception to the consent requirement permits academic institutions to share students' PII with third parties who qualify as school officials with legitimate educational interests, written agreements must be carefully crafted to counteract the default privacy policies of edtech providers, which may not sufficiently limit subsequent disclosures and uses of student data.

B. Edtech Adoptions Pursuant to Clickwrap Agreements

In addition to institution-wide learning management systems, students often use edtech in a localized form when teachers integrate these products directly into particular course curricula. Many specialized learning tools are available for free and can be downloaded immediately from the cloud or the vendor's web page simply by clicking "Yes" to accept the vendor's terms of service agreement. A so-called "clickwrap" agreement "presents the user with a message on his or her computer screen, requiring that the user manifest his or her assent to the terms of the license agreement by clicking on an icon. The product cannot be obtained or used unless

---

[48] *Privacy Notice*, ELLUCIAN, https://www.ellucian.com/privacy#customers [https://perma.cc/XEH7-M385] (last visited July 20, 2022).

[49] *Id.*

[50] *Ellucian Customers*, ELLUCIAN, https://www.ellucian.com/privacy#customers [https://perma.cc/JZ25-SCJS] (last visited Aug. 24, 2022) ("The contracts between Ellucian and its customers may contain terms regarding the protection of Personal Data. When that is the case, the applicable contract provision shall supersede any conflicting provision in this Privacy Notice.").

and until the icon is clicked."[51] Clickwrap agreements, including any provisions governing the collection, use, and sharing of personal data generated by the use of the software application system, are generally enforceable. This is because the agreement essentially requires "users to perform an affirmative action unambiguously expressing assent *before* they may use the software, [and] that affirmative action is equivalent to an express declaration stating, 'I assent to the terms and conditions of the license agreement' or something similar."[52]

The Privacy Technical Assistance Center ("PTAC") of the U.S. Department of Education[53] issued a Model Terms of Service document as a guide for evaluating the privacy protections contained in clickwrap agreements with online educational service providers.[54] The PTAC document provides a list of twelve key provisions included in standard clickwrap agreements, with illustrations as to what constitutes appropriate language and which terms may be problematic.[55] According to the PTAC guidance, some of the main clickwrap provisions to evaluate include terms pertaining to data collection and use, data de-identification, data sharing, data mining, marketing and advertising, and modification of terms.[56] The PTAC guidance warns that accepting a clickwrap agreement containing inadequate privacy protections may lead to

---

[51] Specht v. Netscape Commc'n. Corp., 150 F. Supp. 2d 585, 593–94 (S.D.N.Y. 2001).

[52] *Id*. at 595 (emphasis added). A clickwrap agreement differs from a "browse-wrap" agreement "where website terms and conditions of use are posted on the website typically as a hyperlink at the bottom of the screen." Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 366 (E.D.N.Y. 2009).

[53] The U.S. Department of Education runs the Privacy Technical Assistance Center as a "one-stop" resource for answering questions related to privacy. *Privacy*, U.S. DEP'T OF EDUC. OFF. OF EDUC. TECH., https://tech.ed.gov/privacy/ [https://perma.cc/2UP6-6DC9] (last visited July 20, 2022).

[54] *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service,* PRIV. TECH. ASSISTANCE CTR. (Jan. 2015, revised Mar. 2016), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf [https://perma.cc/DBH7-AUF2] [hereinafter *PTAC Model Terms of Service*].

[55] *Id.*

[56] *Id.* at 3–6.

violations of FERPA or other laws.[57] In many cases, however, a vendor's clickwrap agreement pertains only to the terms governing use of the service, and the agreement includes a broad statement whereby the user acknowledges having read the company's general privacy policies viewable on a different screen.[58] A company's privacy policies are usually not the subject of a separate, standalone clickwrap agreement, and breach of contract claims relating to a company's privacy policies have been largely unsuccessful since the privacy practices are not viewed as separate contracts with the user, but instead as mere notices and broad statements about a company's policies.[59]

A user often automatically acquiesces to the vendor's stated privacy practices by accepting the terms of service via a clickwrap agreement, and there is no real opportunity to negotiate any changes to a privacy policy that includes sweeping data collection, data use, and data sharing provisions. For example, Socrative is a popular educational software and assessment tool used by faculty to deliver various interactive activities, such as quizzes and surveys, that can be accessed by students via their mobile devices.[60] The free basic plan allows teachers to create a single account for all class members, while the upgraded account allows teachers to directly import a class

---

[57] *Id.* at 1 ("Depending on the content, [c]lick-[w]rap agreements may lead to violations of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), or other laws, as well as privacy best practices.").

[58] The new definition of "consent" under the California Privacy Rights Act, which takes effect in 2023, may require businesses to implement different consent mechanisms on their websites and mobile applications. *See* Stevie DeGroff, *CPRA Countdown: New Rules for Consent in California, But Only in Limited Use Cases*, JD SUPRA (Apr. 23, 2021), https://www.jdsupra.com/legalnews/cpra-countdown-new-rules-for-consent-in-4224714/ [https://perma.cc/WSK9-GGN3] (noting that the definition mirrors consent under Article 4 of the European Union's General Data Protection Regulation which must be "freely given, specific, informed").

[59] Dyer v. Nw. Airline Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (stating that "broad statements of company policy generally do not give rise to contract claims").

[60] *Higher Ed*, SOCRATIVE, https://www.socrative.com/higher-ed/ [https://perma.cc/Z7GL-ZLJJ] (last visited July 20, 2022).

roster into the Socrative system.[61] Access to the class account is restricted to enrolled students by means of unique log-in credentials and shareable links sent to students' email accounts.[62]

By downloading the application, users agree to the terms and conditions of service,[63] which contains an acknowledgement of having read and understood Socrative's privacy policy[64] posted on a separate webpage and available by clicking through a hyperlink. Socrative's privacy policy states that if the teacher is using the free version of the service, Socrative will collect information about each student's activity within the service and IP address by using session-based and persistent cookies to track and analyze the student's use of the services.[65] The privacy policy states that Socrative may utilize other third-party analytics tools and technologies, such as Google Analytics, for this purpose.[66]

Socrative's privacy policy provides that the company can disclose students' personal information to third-party service providers for purposes of internal business operations, account administration, billing, and improvement of services. Socrative may also share student information with sub-processors located outside the United States.[67] The privacy policy contains language that any changes to its terms will be posted on the website and will be effective when posted.[68] While Socrative's privacy policy states that student information transferred to third parties is not used for

---

[61] *Id.*

[62] *Id.*

[63] *Terms and Conditions of Service*, SOCRATIVE, https://www.socrative.com/terms-of-use/ [https://perma.cc/7QSY-5SWD] (last visited July 20, 2022) [hereinafter *Socrative TOS*].

[64] *Privacy Policy*, SOCRATIVE, https://www.socrative.com/privacy/ [https://perma.cc/85W2-AF4T] (last visited July 20, 2022) [hereinafter *Socrative Privacy Policy*].

[65] *Socrative TOS*, *supra* note 63.

[66] *Socrative Privacy Policy*, *supra* note 64.

[67] *Id. See also Who Socrative Shares Your Data With*, SOCRATIVE, https://help.socrative.com/en/articles/2242715-who-socrative-shares-your-data-with [https://perma.cc/R7ZP-YUMB] (last visited July 20, 2022) (providing a list of Socrative's current sub-processors including Amazon Web Services, CloudFront, and Convert API).

[68] *Socrative Privacy Policy*, *supra* note 64.

marketing or advertising, Socrative's subcontractors are not explicitly bound by the same policies and may engage in onward transfers of student personal data for various purposes.[69] Although Socrative's standard privacy policies contain some basic restrictions regarding the use and sharing of student data, provisions regarding modification of terms and data sharing that do not adhere to the PTAC guidance[70] cannot be modified since they are included in a clickwrap agreement.

Kahoot! is another popular online game-based learning platform used in college classrooms "around the world, including 87% of the global top 500 universities."[71] The company claims that Kahoot! "wants to empower everyone, including children, students, and employees, to unlock their full learning potential."[72] Kahoot!'s terms and conditions page provides a link to a separate privacy policy posted on its website. The privacy policy states the service automatically collects device information, usage data, log data, and information to, among other things, offer "the opportunity to participate in sweepstakes, contests and similar promotions."[73]

Kahoot! advertises it will use personal information to improve, optimize, and personalize the service, and may share personal information with third parties considered to be "affiliates," "service providers," and "advertising partners."[74] While Kahoot! also notes third parties designated as "service providers" are contractually restricted in how they can use personal information, similar limitations are not specifically placed upon "affiliates" or

---

[69] *See Who Socrative Shares Your Data With*, *supra* note 67 (which merely states that, prior to engaging any third party, Socrative will perform due diligence to assess their privacy, security, and confidentiality practices).

[70] *PTAC Model Terms of Service*, *supra* note 54, at 4–6.

[71] *Key Numbers*, KAHOOT!, https://kahoot.com/company/#key-numbers [https://perma.cc/NN2V-87C3] (last visited July 20, 2022).

[72] *About Us*, KAHOOT!, https://kahoot.com/company/ [https://perma.cc/SC6R-6YN8] (last visited July 20, 2022).

[73] *Kahoot! Privacy Policy: Use of Personal Information*, KAHOOT!, https://trust.kahoot.com/privacy-policy/ [https://perma.cc/B6JF-DQME] (last visited July 20, 2022).

[74] *Kahoot! Privacy Policy: Sharing Your Personal Information*, KAHOOT!, https://trust.kahoot.com/privacy-policy/ [https://perma.cc/B6JF-DQME] (last visited July 20, 2022).

"advertising partners."[75] Additionally, the privacy policy does not prohibit parties receiving personal information from attempting to re-identify any de-identified data.[76] The standard privacy policies for Kahoot!, available by clicking on a separate hyperlink within its terms of service clickwrap agreement, do not strictly adhere to the PTAC guidance in the areas of data use, data sharing, and de-identification.[77]

IV. THE TEACHING ENVIRONMENT IN HIGHER EDUCATION IS CONDUCIVE TO CLASS-LEVEL EDTECH ADOPTIONS

In the higher education setting, administrators exercise limited supervision and control over the day-to-day activities that take place in the classroom. For the most part, faculty members are free to integrate edtech products into their courses without first seeking institutional approval of a vendor's terms of service agreement. The autonomy of college faculty regarding edtech selections stands in stark contrast to edtech decisions made within the K–12 school environment, which are subject to great administrative oversight. Additional federal privacy protections which apply only to younger students, along with an increased level of control exerted over K–12 teachers, make independent, classroom-specific edtech adoptions easier and thus more common in higher education.

Besides FERPA, any edtech vendor that collects personal information online from children under the age of 13 is subject to the Children's Online Privacy Protection Act of 1998 ("COPPA"),[78] which prohibits unfair or deceptive acts in connection with the collection, use, and/or disclosure of personal information from and about children on the internet.[79] COPPA requires companies to provide notice of their data collection and use practices and obtain parental consent before collecting certain types of student

---

[75] *Id.*

[76] *See Privacy Evaluation for Kahoot*!, COMMON SENSE PRIV. PROGRAM, https://privacy.commonsense.org/evaluation/kahoot [https://perma.cc/KS4H-PWLD] (last visited July 20, 2022).

[77] *PTAC Model Terms of Service*, *supra* note 54, at 3–6.

[78] 15 U.S.C. §§ 6501–06.

[79] *Id.*

information.[80] Schools may consent on behalf of parents to edtech vendors' collection of students' personal information only when such information is used for a noncommercial, school-authorized educational purpose—provided that the edtech vendor furnishes the school with the necessary COPPA notice of its data collection and use practices.[81] The parental consent requirement imposed by COPPA has forced K–12 school districts to develop internal organizational systems for communicating the privacy practices of potential edtech vendors to parents if a student will be using any external apps or tools in the classroom.[82] Implementing these notice and disclosure processes has led to the creation of robust in-house approval protocols regarding the use of edtech in the K–12 classroom, designed to discourage individual teachers from adopting edtech without first seeking approval from the school administration.[83]

Resultant disclosures regarding the data collection practices of edtech vendors hired by school districts has, in turn, motivated parents of younger students to become well-informed, highly engaged advocates for the protection of student data.[84] The additional parental scrutiny may also dissuade K–12 teachers from adopting edtech without the school's knowledge. Intense efforts to protect K–12 student data have been well-publicized, and student privacy concerns have prompted the creation of guides with privacy evaluations of popular edtech apps.[85] In addition, the Future of

---

[80] 16 C.F.R. §§ 312.3(a), (b).

[81] *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 [https://perma.cc/Y22B-ZY64].

[82] *See id.*

[83] *See id.*

[84] Lisa Cline, *Parents Nationwide File Complaints with U.S. Dept. of Education; Seek to Address Massive Student Data Privacy Protection Failures*, SENTINEL (July 12, 2021), https://www.thesentinel.com/communities/parents-nationwide-file-complaints-with-u-s-dept-of-education-seek-to-address-massive-student/article_3133b6ce-e30e-11eb-9a6f-4b21a35875b0.html [https://perma.cc/4QX6-6PCD].

[85] *See All Common Sense Privacy Evaluations*, COMMON SENSE PRIV. PROGRAM, https://privacy.commonsense.org/evaluations/1 [https://perma.cc/8MPY-KSLS] (last visited July 20, 2022). According to a 2021 report analyzing the privacy policies of two hundred of the most popular kidtech

Privacy Forum's Student Privacy Pledge,[86] which is a signed code of conduct geared toward edtech providers in the K–12 context, has approximately 247 signatories,[87] and the Federal Trade Commission can bring enforcement actions against edtech providers who sign the pledge but fail to adhere to the stated commitments.[88]

Unlike the heavily controlled K–12 system, the higher education classroom boasts a less restrictive environment where faculty have great leeway to decide how best to teach and communicate their subject matter. A basic component of academic freedom is a faculty member's near-complete discretion to select appropriate textbooks, create assignments and exams, and choose outside resources for teaching their classes.[89] Individual professors exercise personal

---

and edtech applications and services, 26% received a "Pass" rating for meeting minimum safeguards, while 74% received a "Warning" rating for failing to meet minimum privacy recommendations. Girard Kelley et al., *2021 State of Kids' Privacy,* COMMON SENSE MEDIA 1 (Nov. 16, 2021), https://www.commonsensemedia.org/sites/default/files/research/report/common-sense-2021-state-of-kids-privacy_0.pdf#section*.58 [https://perma.cc/2QKJ-8G5E].

[86] *See Student Privacy Pledge 2020*, FUTURE OF PRIV. F. & SOFTWARE & INFO. INDUS. ASS'N, https://studentprivacypledge.org/privacy-pledge-2-0/ [https://perma.cc/QV26-9YD7] (last visited July 20, 2022). *But see* Alexi Pfeffer-Gillett, *Peeling Back the Student Privacy Pledge*, 16 DUKE L. & TECH. REV. 100 (2018) (arguing that the Pledge does not contain any meaningful oversight or enforcement provisions).

[87] *Pledge 2020 Signatories*, FUTURE OF PRIV. F. & SOFTWARE & INFO. INDUS. ASS'N, https://studentprivacypledge.org/signatories/ [https://perma.cc/829D-3QE9] (last visited July 20, 2022) (list of signatories includes Apple, Blackboard, Khan Academy, Moodle, Nearpod, Newsela, and Pear Deck).

[88] Sophia Cope et al., *FPF's 2020 Student Privacy Pledge: New Pledge, Similar Problems,* ELEC. FRONTIER FOUND. (Sept. 28, 2021), https://www.eff.org/deeplinks/2021/09/fpfs-2020-student-privacy-pledge-new-pledge-similar-problems [https://perma.cc/EF6E-988C] (stating that the Pledge provides schools, parents, and students with false assurance due to numerous loopholes). *See Pledge 2020 Guidelines and FAQs*, FUTURE OF PRIV. F. & SOFTWARE & INFO. INDUS. ASS'N, https://studentprivacypledge.org/faqs/ [https://perma.cc/TT49-N2T4] (last visited July 20, 2022). *But see* Pfeffer-Gillett, *supra* note 86, at 127 (stating that very little has been done to hold companies accountable for complying with the Pledge).

[89] *Statement on The Freedom to Teach*, AM. ASS'N OF UNIV. PROFESSORS (Nov. 7, 2013), https://www.aaup.org/news/statement-freedom-teach#.Yf2lfurMLIV [https://perma.cc/N52R-W6P5] ("The freedom to teach includes the right of the

judgment to determine when (and if) students use course-specific edtech to perform required tasks for class. Faculty members can also unilaterally decide that students will access web- or cloud-based tools, or download mobile learning applications to complete coursework, assignments, and quizzes. Faculty members are likewise free to introduce edtech tools into a course simply to liven up the classroom experience or to engage students in a fun, interactive activity, regardless of whether or not the technology is essential to teaching course content.

According to a comprehensive 2017 study, decisions regarding edtech in higher education are increasingly decentralized and made at the individual faculty level,[90] and the most common method for deciding to use an edtech product in higher education is by recommendation from colleagues or biased suggestions by a vendor.[91] Faculty members operate individually when choosing edtech for their courses—not necessarily to circumvent their institution's internal procedures, but often because the school lacks strict edtech approval protocols or because the school does not have an identified person or office within the institution with primary responsibility for vetting new edtech products.[92] The discretion to introduce edtech into a course allows faculty to be inventive and creative in their teaching methods, but it may inadvertently contribute to the dissemination of vast amounts of student data.

---

faculty to select the materials, determine the approach to the subject, make the assignments, and assess student academic performance in teaching activities for which faculty members are individually responsible . . . .").

[90] Fiona M. Hollands & Maya Escueta, *EdTech Decision-making in Higher Education*, CTR. FOR BENEFIT-COST STUD. OF EDUC., TCHRS. COLL., COLUM. UNIV. (May 2017), https://symposium.curry.virginia.edu/wp-content/uploads/2017/06/WG-B-Edtech-Decision-Making-in-Higher-Education_FINAL.pdf [https://perma.cc/3HNS-YQH5].

[91] *Id.* at 28–32.

[92] Sydney Johnson, *Chief Privacy Officers: A Small but Growing Fleet in Higher Education*, EDSURGE (Mar. 25, 2019), https://www.edsurge.com/news/2019-03-25-chief-privacy-officers-a-small-but-growing-fleet-in-higher-education [https://perma.cc/RNW5-7ZWD] (stating that an EDUCAUSE committee for chief privacy officers in colleges and universities is relatively small, with approximately 30 members).

V. FERPA EXCEPTIONS DO NOT SQUARELY APPLY TO CLASS-LEVEL EDTECH ADOPTIONS

While school administrators oversee institution-level edtech adoptions to assure that vendors' privacy policies satisfy FERPA requirements, edtech adoptions at the classroom level do not undergo similar scrutiny, and statutory exceptions allowing institutions to share student data with third parties may not apply.[93] Class-specific edtech accessed by means of an online clickwrap agreement poses an increased likelihood of FERPA violations because such adoptions do not fit squarely within the school official or directory information exceptions. Even when a student consents on their own to use an edtech product or interacts with the product anonymously, class-level edtech adoptions raise serious student privacy concerns.

A. School Official Exception

An academic institution seeking to disclose student information to outside vendors usually relies on the school official exception under FERPA, which permits the sharing of student PII without consent as long as the vendor is under the direct control of the institution.[94] By extension, the school official exception to FERPA appears to provide a valid basis for a faculty member to share a class list and students' email addresses with an outside edtech provider for the creation of a class account, and "in essence, the act of an educational actor providing access to student information to a recipient performing some function for an educational actor is sufficient to satisfy the statute on its face."[95] But in order for the edtech provider to properly qualify as a school official for purposes of FERPA, the vendor must satisfy three elements: (1) meet the

---

[93] *See* Elana Zeide, *The Limits of Education Purpose Limitations,* 71 U. MIAMI L. REV. 494, 510 (2017) (stating that at the classroom level, teachers "may share information with companies without understanding what the information is they are sharing, with whom, and the terms of use that apply. Many of these platforms and applications are free, or only require payment for certain upgrades, which means they can be adopted by teachers independently without school or district approval.").

[94] 34 C.F.R. § 99.31(a)(1)(B)(2).

[95] Zeide, *supra* note 24, at 365.

definition of school official with a legitimate educational interest as set forth in the institution's annual FERPA notice, (2) be under the school's direct control regarding the restrictions on the use of students' PII, and (3) perform a service typically performed by employees of the institution.[96] It is highly unlikely that these three conditions are satisfied when a faculty member adopts edtech at the classroom level for a particular course.[97]

Under the first element, a faculty member would need to conduct an initial review of the institution's annual FERPA notice to verify that the edtech provider qualifies as a school official with a legitimate educational interest in accordance with the institutions' stated guidelines.[98] Unless a faculty member has undergone adequate and consistent privacy training, verifying that an edtech provider meets the definition of a school official as set forth in the institution's annual FERPA notice is not an instinctive step.

To satisfy the second school official exception element, the edtech provider must be under the direct control of the school regarding the use of student data.[99] While FERPA does not mandate separately signed and negotiated written vendor agreements, a faculty member would need to evaluate the default provisions of the vendor's online clickwrap agreement to ascertain whether or not the vendor has appropriate restrictions in place that limit the use of student data.[100] According to the PTAC Model Terms of Service document, this analysis should focus on whether the vendor can share data with others, whether amendments to the terms of service agreement can be made unilaterally by the vendor, and whether the

---

[96] 34 C.F.R. § 99.31.

[97] Leah Plunkett, *To Stop Sharenting & Other Children's Privacy Harms, Start Playing: A Blueprint for a New Protecting the Private Lives of Adolescents and Youth (PPLAY) Act*, 44 SETON HALL LEGIS. J. 457, 478 (2020) ("Effectuating proper use of the legitimate school official exception requires a directly negotiated contract (rather than a clickwrap), the use of template contractual terms that incorporate relevant FERPA and state student privacy law, or a similar approach that ensures the requirements for reliance on this exception are met.").

[98] 34 C.F.R. § 99.7(a)(3)(iii).

[99] § 99.31(a)(1)(B)(2).

[100] *See PTAC Requirements and Best Practices, supra* note 37, at 4.

vendor retains control of student data so that it can adequately respond to student requests for access to records.[101]

A determination that an edtech vendor is eligible for the FERPA school official designation requires a faculty member to conduct an accurate legal-style assessment of the contract terms set forth in the vendor's clickwrap agreement, which most faculty are simply not equipped to do. Even if the default provisions of the edtech vendor's clickwrap agreement arguably contain sufficient student privacy protections, there is still an overriding question of whether an individual faculty member possesses the requisite authority to designate a school official on behalf of the academic institution. Certainly, an increased risk for FERPA violations and the unauthorized disclosure of students' PII exists when individual professors create informal school official relationships with outside service providers.[102]

There is also the issue of liability if an outside vendor fails to protect the confidentiality of student data when no contract exists between the institution and the vendor.[103] As a workaround, some edtech providers include a statement in their clickwrap agreement whereby a teacher creating a class account affirms they possess the requisite authority to bind the school to the contract.[104] However, it is unclear whether such acknowledgement is sufficient to satisfy FERPA.

Under the third element, the use of the edtech must replace a function typically performed by regular school employees. To satisfy this prong of the exception, the faculty member would need to justify adopting the edtech product as alleviating a teaching or

---

[101] *PTAC Model Terms of Service*, *supra* note 54, at 4–7.

[102] Zeide, *supra* note 24, at 343.

[103] *See* Christine L. Borgman, *Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier,* 33 BERKELEY TECH. L. J., 368, 402 (2018).

[104] *See, e.g.*, *Socrative TOS*, *supra* note 63. (The section entitled Educational Users provides in part as follows: "[A]s a teacher in a[n] Educational Institution, You represent and warrant that: You have permission from Your school board or Educational Institution to enter into this Agreement and to use the Services as part of Your curriculum . . . and You are entering this Agreement on behalf of Your school board or Educational Institution; and You have authority to bind such entity to the terms of this Agreement.")

administrative burden placed on the faculty member. At the very least, the faculty member should be able to demonstrate that the edtech product directly relates to or improves the delivery of course content, but this may be difficult if the edtech product is being used purely as a student engagement tool or an interactive game.

B. Directory Information Exception

To simplify access to an edtech product, the faculty member may decide to share a portion of students' PII with the external edtech provider to set up a class account or create profiles for students enrolled in a particular course. If the PII being disclosed by the faculty member is limited to students' names and email addresses, the information may be considered directory information, which is not subject to FERPA privacy requirements.[105] But proper reliance on FERPA's directory information exception would require the faculty member to compare the edtech vendor's terms of service agreement with the school's annual FERPA notice to confirm that the student information being shared matches the notice's description of directory information.[106]

Prior to creating student profiles or an account for the entire class, the faculty member would also need to review institutional records to determine whether any students have opt-out notices on file for the sharing of directory information, and eliminate those students from the class account.[107] The faculty member would then need to provide a separate mechanism to allow other students to opt-out of the contemplated class-level sharing.[108] Unless the faculty member undertakes the required steps to satisfy the directory information exception, there is no basis for bypassing FERPA requirements.[109]

---

[105] 20 U.S.C. § 1232g(a)(5)(A).
[106] *Id.*
[107] 34 C.F.R. § 99.31(a)(1)(11).
[108] 20 U.S.C. § 1232g(A)(5).
[109] *See PTAC Requirements and Best Practices*, *supra* note 37, at 11 (describing an example of a FERPA violation where a teacher creates user accounts for all students via a clickwrap agreement, including those who opted out of directory information).

C. Sharing De-Identified Information or Obtaining Student Consent

To avoid acting as an intermediary, a faculty member may instruct students to sign up directly with the vendor to access an edtech product, believing that a student consenting on their own to the vendor's terms and privacy policies avoids any potential liability under FERPA.[110] But even when a student creates their own account, there is a real question as to whether a student is freely consenting to the vendor's data and privacy policies if the edtech product is required for completion of class activities. It is difficult to claim that consent is authentic unless the student is given the opportunity to opt-out of using that technology and the faculty member offers an alternative method to complete course activities. The University of Richmond, for example, cautions faculty against requiring students to access external, third-party links and sites to complete class activities unless the student voluntarily signs a separate consent form.[111] Noting that clickwrap agreements will not suffice and that students must explicitly consent, the University of Richmond states "the form must specify records to be disclosed, [the] purpose for their disclosure, persons to whom they will be disclosed[,] and signed and dated by [the] student."[112]

Another potential method to accomplish a class-level edtech adoption within the framework of FERPA would be for the faculty member to select only edtech products that do not require registration or the creation of an account to access the product, or to only use products that permit students to register under an alias or a nickname.[113] FERPA does not apply to de-identified student information that is shared with an edtech provider,[114] so, in theory, students' anonymous interactions with edtech providers should not

---

[110] 20 U.S.C. § 1232g(b).

[111] *FERPA: Guidelines for Classroom Use of Third-Party Sites/External Links*, UNIV. OF RICHMOND REGISTRAR'S OFF., https://registrar.richmond.edu/ferpa/third-party-sites.html [https://perma.cc/VH4A-DF9F] (last visited July 20, 2022).

[112] *Id.*

[113] *Id.* (recommending faculty choose online vendors that offer students appropriate alias options, namely Pearson: MyEconLab, Mastering Chemistry; and Simbio: SImUText).

[114] 34 C.F.R. § 99.31(b)(1).

raise FERPA privacy concerns. Broader privacy concerns may be involved, however, when students share purportedly de-identified data with edtech providers. According to the findings of a recent investigation conducted by the International Digital Accountability Council ("IDAC"), many popular edtech products used by students did not follow best privacy practices in five key areas: (1) sharing location data and persistent identifiers with third parties; (2) exposing personal data in their URLs, raising security concerns; (3) allowing a large number of third parties to collect user information; (4) engaging in ID-bridging, a practice that allows apps to circumvent users' privacy controls; and (5) embedding potentially invasive and unnecessary software development kits.[115]

IDAC's findings regarding pre-installed third-party software development kits ("SDKs") is particularly troubling from a privacy perspective. SDKs "are pieces of code that developers embed in their apps to perform a specific task or function."[116] The IDAC investigation found that mobile analytics and advertising SDKs pose distinct privacy risks in edtech apps, and that many SDKs collect user information by default, sometimes without even the app developer's knowledge.[117]

While a single professor's decision to use edtech in a course may not be overly detrimental, the cumulative effect of ad hoc edtech adoptions by individual faculty members can lead to a significant erosion of student privacy by channeling vast amounts of data into the hands of student data brokers. Students' use of edtech products creates a large amount of metadata, which captures information about how a student interacts with a product, how long a student stays on task, and which websites or pages students visit from the edtech webpage.[118]

---

[115] Quentin Palfrey et al., *Privacy Considerations as Schools and Parents Expand Utilization of Ed Tech Apps During the COVID-19 Pandemic*, INT'L DIGIT. ACCOUNTABILITY COUNCIL (Sept. 1, 2020), https://digitalwatchdog.org/wp-content/uploads/2020/09/IDAC-Ed-Tech-Report-912020.pdf [https://perma.cc/6CV3-EL6S].

[116] *Id.* at 14–16.

[117] *Id.*

[118] *PTAC Requirements and Best Practices*, *supra* note 37, at 2–3.

As technologies become more sophisticated, the collection of metadata by edtech providers can lead to the re-identification of the data subject. The risk of re-identification of the metadata generated by faculty overuse of class-specific edtech products poses a serious threat for exploitation by student data brokers.[119] According to a multi-year study conducted by the Fordham Law Center on Information Law and Policy, there is an overall lack of transparency and regulation of the commercial marketplace for the exchange of student information, and "data brokers obtain and aggregate student information from a variety of sources, but there is often a lack of . . . detail as to what these specific sources are."[120] [121]Citing this report, Senators Edward J. Markey (D-Mass.), Dick Durbin (D-Ill.), and Richard Blumenthal (D-Conn.) sent letters to numerous edtech companies and data brokers inquiring about their student data collection practices. The senators raised concerns that the companies' learning tools posed serious privacy risks due to the potential for personal information to be stolen, collected, or sold without permission or knowledge.[122]

VI. RECOMMENDATIONS FOR IMPROVING STUDENT PRIVACY PROTECTIONS IN HIGHER EDUCATION

The FERPA framework in existence at most K–12 institutions customarily delegates authority to school administrators to accept the data collection practices of edtech vendors on behalf of students. This practice has carried over to higher education, and faculty members routinely make unilateral decisions requiring students to utilize edtech products for class via online clickwrap agreements. Faculty members are often not aware that their activities may violate

---

[119] N. Cameron Russell et al., *Transparency and the Marketplace for Student Data*, 22 VA. J. L. & TECH. 107, 118 (2019) ("[I]nformation outside of FERPA protection may be highly valuable to data brokers, such as metadata collected when students interact with a third-party app or service.").

[120] *Id.* at 141.

[121] Valerie Strauss, *Legislators Ask 50-Plus Firms to Explain How They Use the 'Vast Amount of Data' They Collect on Students*, WASH. POST (Aug. 20, 2019, 7:00 AM), https://www.washingtonpost.com/education/2019/08/20/legislators-ask-plus-firms-explain-how-they-use-vast-amount-data-they-collect-students-which-ones-facebook-google-blackboard-etc/ [https://perma.cc/3LWU-8DAS].

[122] *Id.*

FERPA. Even when a faculty member does have FERPA concerns, these are likely diminished by asking students to consent on their own to provide personal information directly to the edtech vendor. But if the use of edtech is required for the course and the professor does not offer a reasonable alternative, students have no actual choice but to accept the vendor's privacy policies and download the technology.[123] The Department of Education's historical lack of enforcement or sanctions for FERPA violations[124] has allowed course-specific edtech adoptions by faculty to proliferate unchecked. New privacy laws operate differently, however, and there may be consequences for student privacy violations in the future.

Although students in higher education have been largely complacent about data privacy in the past, attitudes are changing.[125] More students and their family members have been affected by

---

[123] Recital 43 of the EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 indicates that an imbalance of power between the parties is relevant when determining whether consent is freely given. A high school in Sweden was fined for using facial recognition to take student attendance. Although the school had asked for the students' consent in relation to the use of the technology, the consent was deemed invalid since the students were in a dependent relationship with the school. Laura de Vries, *Just Say Yes: GDPR Consent Is Not as Simple as It Seems*, INT'L ASS'N OF PRIV. PROS. (Oct. 1, 2019), https://iapp.org/news/a/just-say-yes-gdpr-consent-is-not-as-simple-as-it-seems/# [https://perma.cc/D4HV-4ERD].

[124] Zeide, *supra* note 93, at 503 (stating that "FERPA does not impose any direct accountability on schools for individual FERPA violations" and that the Department of Education "has never exercised its option to withdraw federal funding in the course of the statute's forty-year history").

[125] Jasmine Park & Amelia Vance, *Higher Education Voices: College Students' Attitudes Toward Data Privacy*, STUDENT PRIV. COMPASS (Oct. 25, 2021), https://studentprivacycompass.org/resource/higheredvoices2021/ [https://perma.cc/SW4Z-MVL7] (stating that a study conducted by the Future of Privacy Forum revealed that college students care deeply about privacy and their concern appears to be increasing). *See also* Jasmine Park & Amelia Vance, *Data Privacy in Higher Education: Yes, Students Care,* EDUCAUSE REV. (Feb. 11, 2021), https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care [https://perma.cc/DR87-4ZA3] (noting that college students have become more aware of data collection and have expressed concerns about limiting use of their data).

identity theft,[126] and recent high-profile data breaches and ransomware attacks targeting educational institutions have raised concerns about whether security measures in place at schools are adequate to protect sensitive data.[127] Comprehensive privacy legislation passed in California, Colorado, Connecticut, Utah, and Virginia, along with proposed legislation in other states and at the federal level, has garnered widespread media attention.[128] The recent focus on activities of student data brokers and the creation of data broker registries in Vermont[129] and California[130] have also shed light on the practices of entities that formerly existed in the shadows.[131] It will take time before young adults routinely question data privacy practices in the classroom, but pushback from students regarding the use of online proctoring software such as Respondus Lockdown and ProctorU signaled a shift,[132] and college faculty and higher education institutions should take note.

While faculty members may not possess a comprehensive understanding of student privacy issues, they can still play a key role in teaching young adults how to make careful and informed

---

[126] *The Increasing Threat of Identity Theft*, OFF. OF THE N.Y. STATE COMPTROLLER 3 (May 2021), https://www.osc.state.ny.us/files/reports/pdf/increasing-threat-of-identity-theft.pdf [https://perma.cc/X2S3-AZ3S] (showing that record numbers of identity theft cases were reported in New York and nationwide during 2020).

[127] According to a recent study, K–12 school districts and colleges/universities across the country have experienced over 1,850 data breaches between 2005 and 2020. 65% of these breaches involved post-secondary institutions and 87% of the more than 28.6 million records affected were from post-secondary institutions. Sam Cook, *US Schools Leaked 28.6 Million Records in 1,851 Data Breaches Since 2005*, COMPARITECH (Dec. 15, 2021), https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/ [https://perma.cc/PT79-XAUD].

[128] *See, e.g.*, Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER BLOG (Sept. 26, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/HZ3Z-CANH].

[129] 9 VT. STAT. ANN. §§ 2430, 2433, 2446, 2447.

[130] CAL. CIV. CODE § 1798.99.80.

[131] Russell et al., *supra* note 119; Strauss, *supra* note 121.

[132] Dennis Pierce, *Online Proctoring Keeps Remote Exams Secure but Raises Privacy Questions*, ECAMPUS NEWS (Sept. 4, 2020), https://www.ecampusnews.com/2020/09/04/online-proctoring-keeps-remote-exams-secure-but-raises-privacy-questions/2/ [https://perma.cc/N72F-F9Q9].

decisions regarding data protection by instituting basic privacy awareness measures in the classroom. College students generally agree that new learning technologies make the classroom experience more entertaining,[133] so faculty members have an obligation to counterbalance this enthusiasm by drawing students' attention to the underlying privacy challenges associated with using various learning technologies. At a minimum, faculty members should ask students to access course-specific technology only when the product will be used continually during the course, and should avoid sampling a wide variety of edtech tools that will only be used occasionally. Special care should be taken when asking students to use platforms such as Slack or Discord for class communications, since technologies designed for business or gaming communities typically have privacy policies that include broad data sharing permissions.[134]

Faculty can model responsible behaviors by conducting privacy evaluations of edtech products prior to their adoption for class use and reading a vendor's privacy policy together with students in class before downloading or accessing any new edtech products. Faculty can encourage students to remain vigilant about reducing their digital footprint by reminding them to periodically check their privacy settings for various apps, and to adjust data and location sharing options to the minimum necessary. Faculty can instruct students to delete and uninstall any edtech apps from their mobile

---

[133] Claudio Brasca et al., *How Technology is Shaping Learning in Higher Education,* MCKINSEY & CO. (June 15, 2022), https://www.mckinsey.com/industries/education/our-insights/how-technology-is-shaping-learning-in-higher-education [https://perma.cc/DSF6-CT32] (finding that 80% of students believe that using edtech for in-class exercises improves their grades and learning).

[134] For example, Discord's June 2020 Privacy Policy provided that advertising platforms, including Twitter and Facebook, whose SDKs are integrated within Discord's service, may collect information for optimizing advertising campaigns. *Privacy Policy*, DISCORD, https://discord.com/archive/privacy/june-2020 [https://perma.cc/89TL-T25L] (last visited Mar. 2, 2022). Discord's updated Privacy Policy does not specifically refer to third-party SDKs. *Privacy Policy: Information we receive from other sources*, DISCORD, https://discord.com/privacy#information-we-receive-from-other-sources [https://perma.cc/GRY2-R2M5] (last visited July 20, 2022).

devices when they are no longer needed for class activities, and faculty should consider adding statements to their course syllabi to reinforce the importance of privacy and to help students understand how to better protect their data.[135]

The increased reliance on edtech following the COVID-19 pandemic underscores the need for higher education institutions to rethink their traditional approaches to protecting data and to reassess their institutional policies regarding data privacy. Colleges and universities can begin by conducting thorough reviews of their existing procedures for the adoption and use of edtech to assure that any software or tools used in the classroom are first vetted by the appropriate administrator or school committee; colleges and universities may also consider creating lists of preapproved edtech products for this purpose.[136] These preapproved lists can be periodically updated by school administrators using resources available from PTAC, as well as the rating guide from Common

---

[135] Autumm Caines & Erin Glass, *Education Before Regulation: Empowering Students to Question Their Data Privacy*, EDUCAUSE REV. (Oct. 19, 2019), https://er.educause.edu/articles/2019/10/education-before-regulation-empowering-students-to-question-their-data-privacy [https://perma.cc/AB33-9QHB] (providing sample language that can be adopted for syllabus use); *Privacy Tips for Your Syllabus*, UNIV. OF CALIF. IT BLOG (Sept. 29, 2021), https://cio.ucop.edu/privacy-tips-for-your-syllabus/ [https://perma.cc/Z8XY-LQB7].

[136] *See, e.g.*, *The Center for Teaching Excellence: Tech Tools*, BOS. COLL., https://www.bc.edu/content/bc-web/academics/sites/center-for-teaching-excellence/tech-tools.html [https://perma.cc/87MY-GL3S] (last visited July 20, 2022). The IT Assistance Center at Texas State University has developed a robust system for the evaluation and approval of external apps that can be integrated into the school's learning management system. Each tool must be evaluated for compliance with FERPA and the school's information security policies before being added. *External Apps in Canvas*, TEX. STATE UNIV. IT ASSISTANCE CTR., https://itac.txstate.edu/support/canvas/faculty-staff/lti.html [https://perma.cc/6A7X-87CC] (last visited July 20, 2022).

Sense Media.[137] To help facilitate this, Educause has developed a vendor evaluation toolkit specifically for higher education.[138]

The creation and communication of clear policies will help to prevent the unauthorized or accidental disclosure of students' FERPA-protected information by faculty at the classroom level. If it is economically feasible, higher education institutions should consider funding a separate privacy-focused administrative position devoted to handling privacy matters that arise on campus.[139] A dedicated Chief Privacy Officer could monitor compliance with existing and new laws regarding data protection, data storage, and data breach notifications. The Chief Privacy Officer can also act as a liaison with outside legal counsel where appropriate.[140] Schools can also promote a general culture of data privacy across the institution by sponsoring data privacy awareness events[141] and by improving, expanding, and modernizing privacy training for faculty, staff, and administrators.

VII. CONCLUSION

It will take some time before the focus in higher education shifts from data security to data privacy, but the ideal place to begin is within the college classroom. When faculty consider the privacy

---

[137] *See Privacy Evaluations*, COMMON SENSE PRIV. PROGRAM, https://privacy.commonsense.org/evaluations/1 [https://perma.cc/X4H8-FE8H] (last visited July 20, 2022). *See also Information Security Primer for Evaluating Educational Software*, COMMON SENSE PRIV. PROGRAM, https://privacy.commonsense.org/resource/infosec-primer/README [https://perma.cc/T4G6-3XUS] (last visited July 20, 2022) (providing a guide for evaluating the information security practices of educational software).

[138] *Higher Education Community Vendor Assessment Toolkit*, EDUCAUSE (Dec. 17, 2021), https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit [https://perma.cc/9YWH-8W6W] (providing questionnaire created by the Higher Education Information Security Council to measure vendor risk).

[139] Johnson, *supra* note 92.

[140] *See* Valerie Vogel, *The Chief Privacy Officer in Higher Education*, EDUCAUSE (May 11, 2015), https://er.educause.edu/articles/2015/5/the-chief-privacy-officer-in-higher-education [https://perma.cc/KCW4-ZM3S] (describing the chief privacy officer role on campus).

[141] *Data Privacy Week*, NAT'L CYBERSECURITY ALL., https://staysafeonline.org/data-privacy-week/ [https://perma.cc/S6ES-DQ4K] (last visited July 20, 2022).

implications for students before deciding which materials and resources to use for teaching a course, they acknowledge the complexity of issues surrounding the protection of student data. By critically evaluating edtech vendors' privacy policies, faculty can draw students' attention to the need to exercise their right to control how their personal information is collected, stored, and potentially shared. The regulatory environment surrounding student data privacy is starting to progress and mature, but students are making decisions on a daily basis that could negatively affect their data privacy for years to come. Faculty members have a unique opportunity to help protect their students' personal data by advocating for privacy in the college classroom.