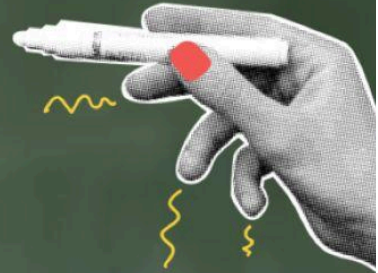




# PAYING TWICE TO LEARN



How higher education students may be forced to sacrifice privacy for digital learning tools

**Lead Author**

Ariel Fox Johnson

**Contributors**

Meghan Land,  
Emory Roane,  
Julian Sanghvi,  
Sriraksha Srivatsav,  
John Ying

**About Privacy Rights Clearinghouse**

Privacy Rights Clearinghouse is a 501(c)(3) non-profit organization dedicated to increasing access to information, policy discussions, and meaningful rights so data privacy can be a reality for everyone. Learn more about us at [privacyrights.org](https://www.privacyrights.org).

# Acknowledgements

We thank Michelson 20MM Foundation for providing Spark Grant funding to support this project. Special thanks to the Consumer Protection Public Policy Order at the UC Berkeley School of Law for supportive research for this report, to SPARC for their work maintaining the Textbook Billing Contract Library, and to all of the education sector experts who graciously shared time and insights with us.

# Our Approach

We took a multi-pronged approach to better understand higher education students' experiences with digital instructional materials and data privacy.

To determine where higher education courseware fits into the legal landscape, we analyzed applicable federal and California law. California is a state leader with respect to consumer data privacy law. Residents have a constitutional right to privacy, California was the first state to enact a comprehensive privacy law, and the state has enacted educational technology laws in the K-12 space.

We reviewed and analyzed popular textbook products' sign-up experiences, to the extent public, and their privacy statements. We reviewed privacy statements up through August 1, 2024, with the dates of the policy review noted. Our analysis of these privacy statements reflects a snapshot of industry practices. Companies may change their statements and policies on a regular basis.

We spoke with higher education officials and experts in privacy and technology as well as those separately researching this issue. We reviewed reports of student experiences with digital instructional materials, and law students at UC Berkeley surveyed 40 undergraduate and graduate students about their awareness and experiences. It is important to note that the survey of UC Berkeley students represents a small sample. The survey's purpose was to provide context and serve as a starting point for conversations about student perspectives concerning this issue, though the results are consistent with reporting on this issue.

We also analyzed contracts available in public contract libraries and those made available to us following public records act requests. Though we spoke with educational privacy professionals in other states, our contract review was limited to public schools in the University of California, California State, and California Community College systems.

# Key Takeaways

**Limited Protections:** Higher education students are often required to use and pay for access to digital instructional materials, yet they have extremely limited access to data privacy rights and protections. Federal law has not kept pace with technology, and relevant state laws focus on K-12 students or rely on consent—an element notably absent in this context.

**Lack of Transparency:** The data privacy practices surrounding digital instructional materials in higher education are largely opaque. Neither students nor instructors have a clear understanding of how personal data is collected, used, stored, or shared. Companies rarely provide clear information in public policies, and institutions are not required to make vetting processes readily available for review.

**Inconsistent Policies and Practices:** There appears to be no data protection standard or accepted best practices in place across educational institutions or companies providing digital instructional materials. Even the existence of contracts between institutions and providers varies. Data practices and privacy protections seem to be largely left to the ed-tech companies' discretion.

**Significant Room for Improvement:** Higher education institutions and ed-tech companies have substantial opportunities to better protect students' data. This could involve adopting state or federal legal requirements, implementing institution- or system-wide contracting and review practices, and obtaining clear commitments from companies to protect student data.














# Table of Contents

|   |           |
|---|-----------|
| <b>I. INTRODUCTION</b>  | <b>5</b>  |
| <b>II. RELEVANT PRIVACY LAWS</b>  | <b>6</b>  |
| <b>A. Family Educational Rights and Privacy Act (FERPA)</b>   | 6         |
| 1. Disclosures of Personally Identifiable Information under FERPA                                       | 7         |
| 2. Modern Day FERPA   | 9         |
| <b>B. Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA)</b> | 10        |
| <b>C. California Privacy Laws</b>   | 11        |
| 1. Student Privacy Laws   | 11        |
| 2. The California Consumer Privacy Act (CCPA)   | 11        |
| <b>III. HIGHER EDUCATION INSTITUTION PRACTICES</b>  | <b>13</b> |
| <b>A. Selecting Digital Instructional Materials</b>   | 14        |
| <b>B. Contracting for Digital Textbooks</b>   | 15        |
| 1. Institutional Contracts with Publishers and Distributors   | 16        |
| <b>C. The Role of Campus Bookstores</b>   | 17        |
| 1. Bookstore contracts  | 17        |
| <b>D. Learning Management Systems</b>   | 18        |
| <b>IV. STUDENT EXPERIENCES WITH COURSEWARE DATA PRACTICES</b>   | <b>19</b> |
| <b>A. Accessing Digital Textbooks</b>   | 20        |
| 1. Student “Consent”  | 20        |
| <b>B. Courseware Information Collection</b>   | 22        |
| 1. From Students and Student Activity   | 22        |
| 2. From Non-Student Sources of Information  | 23        |
| <b>C. Information Use and Sharing with Educational Institutions and Third Parties</b>                   | 24        |
| 1. McGraw Hill Connect  | 24        |
| 2. Pearson MyLab  | 25        |
| 3. Cengage MindTap  | 26        |
| <b>D. Treatment of Higher Ed Students vs. Younger Students</b>  | 27        |
| <b>E. Use of Student Information for Advertising and Marketing</b>                                      | 28        |
| <b>F. Why Do Publishers’ Data Practices Differ?</b>   | 28        |
| <b>G. Data Breaches &amp; Exposure of Student Information</b>   | 29        |
| <b>V. RECOMMENDATIONS &amp; CONCLUSION</b>  | <b>30</b> |
| <b>A. A Murky Landscape</b>   | 30        |
| <b>B. A Better Model</b>  | 32        |
| 1. Pass Laws That Protect Higher Ed Students’ Privacy   | 32        |
| 2. Target Key Institutional and Corporate Actors To Change Policies                                     | 34        |
| 3. Raise Awareness and Build Grassroots Support   | 34        |
| <b>C. Conclusion</b>  | 35        |

# I. INTRODUCTION

Higher education students are often required to use educational technology tools, such as digital textbooks and other instructional materials, in their courses. These tools—broadly referred to as courseware—can offer students personalized learning experiences and rapid feedback. However, they also enable educational institutions and ed tech companies to collect and access vast amounts of data about students.

## In the context of digital instructional materials, courseware providers may collect data including:

- |   |  |
|---|--|
|  students' keystrokes                  |  biometric data             |
|  highlighted text                     |  financial information     |
|  time spent on different pages       |  behavioral details       |
|  personally identifiable information |  disciplinary information |
|  web browsing histories              |  health information       |
|  IP addresses                        |  classroom data           |
|  geolocation data                    |  |

---

Without adequate protections, this information may be used in ways unrelated to the classroom context in which it is collected. Students could be labeled and categorized into sensitive profiles of which they are completely unaware. Their data might be sold or shared without meaningful consent, or it could be stored in a manner vulnerable to data breaches.

This report aims to explore critical data privacy questions involving a courseware market that charges students for access to digital instructional materials with immense data collection capabilities. Students may effectively be paying twice—once with money and again with their personal information. What happens to the information courseware collects in the higher education context? What responsibilities do institutions and companies have with respect to this information? And do students have any awareness or choice over the matter?

Focusing on California public institutions, this report:

- Describes relevant laws;
- Examines institutional practices and policies with respect to digital instructional materials (e.g., digital textbooks);
- Considers the student experience with digital instructional materials and their privacy practices; and
- Offers recommendations for reform.

There are many opportunities to improve students' experiences with digital instructional materials and courseware more generally. Our recommendations include advocating for laws to protect higher education students' privacy, encouraging institutions and corporate actors to change and implement system-level policies, and raising awareness from the ground up.

## II. RELEVANT PRIVACY LAWS

There are a handful of state and federal education-specific and broader privacy laws that offer some protections for students in higher education. It is important to note, however, that the postsecondary sector lacks many of the specific ed-tech-focused laws that states have enacted for K-12 students over the past decade.<sup>1</sup>

### A. Family Educational Rights and Privacy Act (FERPA)

The primary federal student privacy law is the Family Educational Rights and Privacy Act (FERPA),<sup>2</sup> a privacy and access law that has been in place since 1974. FERPA applies to “education records”—defined as “records, files, documents, and other materials which contain information directly related to a student”—that are “maintained by an educational agency or institution or by a party acting for the agency or institution.”<sup>3</sup> FERPA is enforced by the U.S. Department of Education, which has also issued FERPA rules.<sup>4</sup>

---

<sup>1</sup> See, e.g., Student Privacy Compass. *State laws*. <https://studentprivacycompass.org/state-laws/>.

<sup>2</sup> Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

<sup>3</sup> Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

<sup>4</sup> 34 CFR § 99: Family Educational Rights and Privacy.

Personally identifiable information under FERPA includes:

- (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."<sup>5</sup>

Most states have their own FERPA-like laws covering student records at educational institutions. For instance, California's Education Code addresses the privacy of student records at community colleges in a manner consistent with FERPA's federal regulations.<sup>6</sup>

In the higher education context, FERPA grants students rights to:

- Access and inspect records,
- Request amendments to their records, and
- Exercise "some control over the disclosure of personally identifiable information from the education records."<sup>7</sup>

Institutions also must provide an annual FERPA notice.

## **1. Disclosures of Personally Identifiable Information under FERPA**

Generally FERPA prohibits the disclosure of personally identifiable information without consent. However, when adult students interact directly with ed-tech tools, their use of such tools may be interpreted as giving consent to the disclosure of their information, assuming FERPA even applies to that information (see discussion below). Additionally, there are broad exceptions to FERPA that permit disclosures without consent. Two key exceptions relevant to ed tech are the school official exception and the directory information exception.<sup>8</sup>

### **a) School Official Exception**

---

<sup>5</sup> 34 CFR § 99.3: Definitions.

<sup>6</sup> Cal. Education Code § 76240-76246. (Higher Ed); California Education Code § 49073-49079.7 (K-12).

<sup>7</sup> U.S. Department of Education Privacy Technical Assistance Center. (2015). *Responsibilities of Third Party Service Providers under FERPA*. [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/Vendor%20FAQ.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf)

<sup>8</sup> U.S. Department of Education. 34 CFR § 99.31(a)(1) and (a)(11): Under what conditions is prior consent not required to disclose information?



Under this exception, institutions may allow “school officials” to access personally identifiable information in education records without student consent, provided the institution has determined that the school official has a “legitimate educational interest” in the information. The Department of Education generally interprets the term to include educators, administrators, attorneys, board members, and contractors to whom the school has “outsourced institutional services or functions.”<sup>9</sup> In other words, school officials are third parties acting in a capacity that the institution or its employees otherwise would.

To qualify as a school official, the third party must:

- Perform a service or function the institution would otherwise handle,
- Be under the direct control of the institution,
- Use education records only as authorized by the institution, and
- Meet criteria in an institution’s annual FERPA notification for being a school official with a legitimate educational interest.<sup>10</sup>

Technology vendors often fall within this exception. Although the Department of Education encourages institutions to have a contract in place with a school official designated party, this is not a FERPA requirement.<sup>11</sup>

In addition, the school would respond to student requests for information since it is considered to be in control of the information (as it must be in order to share with a school official).

#### **b) Directory Information Exception**

FERPA also allows institutions to disclose “directory information” without consent if they provide students with a notice and the opportunity to opt out (typically in an annual FERPA notice).<sup>12</sup> The Department of Education defines directory information as “information that is generally not considered harmful or an invasion of privacy if released.”<sup>13</sup> This includes: names, addresses, telephone numbers, dates of birth, and school activities or honors.

This exception allows institutions and others to publish student information in, for instance, news stories, honor rolls, and programs. However, once directory information is shared, it is no longer protected by FERPA.

---

<sup>9</sup> 34 CFR § 99.31(a)(1)(B): Under what conditions is prior consent not required to disclose information?

<sup>10</sup> U.S. Department of Education Privacy Technical Assistance Center. (2015). *Responsibilities of Third Party Service Providers under FERPA*. [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/Vendor%20FAQ.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf)

<sup>11</sup> U.S. Department of Education. *Must a school have a written agreement or contract with a community-based organization to which it non-consensually discloses PII from education records?*

<https://studentprivacy.ed.gov/faq/must-school-have-written-agreement-or-contract-community-based-organization-which-it-non>

<sup>12</sup> U.S. Department of Education. *Are educational agencies and institutions required to notify parents and eligible students of their rights under FERPA?*

<https://studentprivacy.ed.gov/faq/are-educational-agencies-and-institutions-required-notify-parents-and-eligible-students-their>

<sup>13</sup> U.S. Department of Education. *Directory Information*. <https://studentprivacy.ed.gov/content/directory-information>

Institutions may provide a global opt out for directory information sharing or adopt more granular directory information practices, such as restricting information sharing to specific purposes or parties.<sup>14</sup>

California updated its guidance in 2012 for K-12 to include email address in the definition of directory information and remove place of birth, but no such related changes have been made for higher education.<sup>15</sup>

## 2. Modern Day FERPA

FERPA, now over 50 years old, is often criticized for being outdated in the context of modern technology. For instance, it is unclear how FERPA applies to technical information collected by ed tech services such as courseware administering online assignments, and whether that constitutes part of an education record.<sup>16</sup> Critics also contend that directory information sharing is overly broad and that students should be able to have more granular control over their data. Additionally, there are calls for updated security requirements, such as administrative, physical, and technical safeguards, and security training.<sup>17</sup>

Despite discussions of FERPA reform for at least the past decade, no substantial updates have occurred. In the absence of such, the Department of Education established a Privacy Technical Assistance Center (PTAC) in 2010, which has issued guidance on privacy in the digital age, including advice on best practices with ed tech vendors.

For example, PTAC has:

- Issued guidance advising when metadata may constitute personally identifiable information, and how such data may be used, if at all;<sup>18</sup>
- Advised that as a best practice, “both the provider and the school or district should post contracts or agreements on their public facing websites, including a list of data elements shared with the provider, and an explanation of how they are used and for what purpose”;<sup>19</sup>

---

<sup>14</sup>Orange County Department of Education. (2015). *Student records: Confidentiality and preservation workbook*. <https://ocde.us/LegalServices/Documents/Student%20Records%20-%20Confidentiality%20and%20Preservation%20Workbook%20June%202015.pdf>

<sup>15</sup> Orange County Department of Education. (2015). *Student records: Confidentiality and preservation workbook*. <https://ocde.us/LegalServices/Documents/Student%20Records%20-%20Confidentiality%20and%20Preservation%20Workbook%20June%202015.pdf> (referring to Cal. Education Code section 49061(c))

<sup>16</sup> Common Sense Media. (2016). *Are your child's privacy and data at school safe?*

<https://www.common sense media.org/kids-action/articles/are-your-childs-privacy-and-data-at-school-safe>

<sup>17</sup> Common Sense Media. (2021). *Privacy matters for kids*.

[https://www.common sense media.org/sites/default/files/featured-content/files/2021\\_privacy\\_one\\_pager\\_leave\\_behind.pdf](https://www.common sense media.org/sites/default/files/featured-content/files/2021_privacy_one_pager_leave_behind.pdf)

<sup>18</sup> U.S. Department of Education Privacy Technical Assistance Center. (2015). *Responsibilities of Third Party Service Providers under FERPA*. [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/Vendor%20FAQ.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf)

“Indirect identifiers, metadata about students’ interaction with an app or service, and even aggregate information can be considered PII under FERPA if a reasonable person in the school community could identify individual students based on the indirect identifiers together with other reasonably available information, including other public information.”

<sup>19</sup>U.S. Department of Education Privacy Technical Assistance Center. (2015). *Responsibilities of Third Party Service Providers under FERPA*. [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/Vendor%20FAQ.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf)

- Told ed-tech providers that their “use of PII from education records should be limited to only those purposes specified in the contract or agreement”,<sup>20</sup>
- Acknowledged that properly de-identified data can be used for other purposes, but has cautioned that providers “should be clear about their methodologies for de-identification” and should prohibit re-identification of deidentified data if it is shared with other parties.<sup>21</sup>

## B. Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA)

Even when other sectoral privacy laws apply to higher education institutions, FERPA compliance often satisfies privacy obligations with respect to students.

For instance, higher education institutions receiving federal student aid must comply with the Gramm-Leach-Bliley Act (GLBA). The GLBA is a federal law that generally addresses privacy and safety of personal information with financial institutions. The Federal Trade Commission has stated that compliance with FERPA satisfies the GLBA privacy requirements.<sup>22</sup> However, educational institutions must still comply with GLBA security requirements (the Safeguards Rule), and in recent years the Office of Federal Student Aid of the U.S. Department of Education has reiterated that educational institutions must report compliance with the GLBA and meet cybersecurity requirements.<sup>23</sup>

In addition, while the Health Insurance Portability and Accountability Act (HIPAA) applies to higher ed institutions that act as healthcare providers, in the sense that they may be “covered entities” under the law, typically students’ health information is covered under FERPA as a “treatment record” or an “education record” and it is FERPA, not HIPAA, that applies.<sup>24</sup>

---

<sup>20</sup> U.S. Department of Education Privacy Technical Assistance Center. (2015). *Responsibilities of Third Party Service Providers under FERPA*. [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/Vendor%20FAQ.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf)

<sup>21</sup> U.S. Department of Education Privacy Technical Assistance Center. (2015). *Responsibilities of Third Party Service Providers under FERPA*. [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/Vendor%20FAQ.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf)

<sup>22</sup> Privacy of Consumer Financial Information, 65 F.R. 33648 (May 24, 2000) (to be codified at 16 C.F.R. § 313.1). <https://www.govinfo.gov/content/pkg/FR-2000-05-24/pdf/00-12755.pdf>

<sup>23</sup> U.S. Department of Education Federal Student Aid. (2023, Feb. 9). *Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements*. <https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements>

<sup>24</sup> U.S. Department of Health and Human Services & U.S. Department of Education. (2019, Dec.). *Joint guidance on the application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to student health records*. <https://www.hhs.gov/sites/default/files/2019-hipaa-ferpa-joint-guidance.pdf> “The HIPAA Privacy Rule requires covered entities to protect individuals’ health records and other personal health information the entities maintain or transmit, known as protected health information (PHI), by requiring appropriate safeguards to protect privacy, and setting limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients certain rights with respect to their health information, including rights to examine and obtain a copy of their health records, and to request corrections (amendments).”

## C. California Privacy Laws

Although state-specific ed-tech privacy laws typically do not apply to higher education, California's comprehensive privacy laws offer some protection for student data.

### 1. Student Privacy Laws

Beginning in the mid 2010s, many states enacted ed-tech-focused student privacy laws. Notably, these laws—especially those that apply directly to ed-tech providers of digital instructional materials— apply almost exclusively to the K-12 education space.

California has been a leader in enacting K-12 student privacy laws. The first vendor-focused student privacy law in the country was California's 2014 Student Online Personal Information Protection Act (SOPIPA). It prohibits ed tech apps and services designed, marketed, and used primarily for K-12 school purposes from using students' personal information for targeted advertising, to profile students, or for sale. SOPIPA also requires reasonable data security measures and the deletion of student information upon request.

The same year it passed SOPIPA, California also enacted AB 1584 requiring certain provisions and promises in contracts between schools and vendors to help ensure the privacy and security of student information.<sup>25</sup>

---

**That said, these California laws do not apply to postsecondary institutions. And for the dozens of states that have passed similar or related laws, such laws by and large also focus on K-12, leaving higher education largely unaffected.**

### 2. The California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act, passed in 2018 and amended by the California Privacy Rights Act in 2020 (together, CCPA), gives California residents baseline privacy protections, including rights to access, delete, and correct information, the right to opt out of the sale of data, and the right to object to automated decisionmaking.<sup>26</sup> These rights do apply to educational data, which is considered personal information. (Note that in some states, comprehensive privacy laws explicitly exclude any data covered by FERPA.<sup>27</sup>)

---

<sup>25</sup> See Cal. Education Code § 49073.1

<sup>26</sup> Cal. Business and Professions Code § 1798.100 et seq.

<sup>27</sup> Va. Code § 59.1-576

The CCPA also specifically states that it does not require businesses holding student tests on behalf of an institution to be deleted, or require access to assessments that would jeopardize the validity and reliability of such assessments.<sup>28</sup>

The California Privacy Protection Agency promulgates CCPA rules. The Agency has considered rules regarding opt-out rights with respect to automated decisionmaking, including with respect to automated decisionmaking in the educational context. For example, draft rules propose allowing students to opt out of automated decisionmaking that may result in access to or denial of an education enrollment or opportunity, or to opt out of automated technology that profiles them when they are acting as their capacity as students.

This could include “using keystroke loggers, productivity or attention monitors, video or audio recording or live-streaming, facial- or speech-recognition or detection, automated emotion assessment, location trackers, speed trackers, and web-browsing, mobile-application, or social-media monitoring tools.”<sup>29</sup>

Individuals have CCPA rights with respect to “businesses” who determine the means and purposes of information processing and meet certain thresholds.<sup>30</sup> In other privacy laws, entities that determine how to process personal information are commonly called “controllers.”

The CCPA also addresses “service providers”, who process information on behalf of “businesses” and act at the direction of businesses, with limited ability to use data outside of providing the requested service to the business. Service providers must assist businesses in responding to rights requests, but are not required to respond to such requests themselves. In other privacy laws, these service providing entities are commonly called “processors.”

---

<sup>28</sup> Cal. Business and Professions Code § 1798.145(q).

<sup>29</sup> California Privacy Protection Agency. (2023, Dec.). Draft Automated Decisionmaking Technology Regulations. [https://cppa.ca.gov/meetings/materials/20231208\\_item2\\_draft.pdf](https://cppa.ca.gov/meetings/materials/20231208_item2_draft.pdf)

Under the draft rules, a “[d]ecision that produces legal or similarly significant effects concerning a consumer” as “a decision that results in access to, or the provision or denial of, financial or lending services, housing, insurance, *education enrollment or opportunity*, criminal justice, employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services.” (emphasis added). And the draft rules propose enabling individuals to opt out of automated technology in the following situations:

“(1) For a decision that produces legal or similarly significant effects concerning a consumer;

(2) Profiling a consumer who is acting in their capacity as an employee, independent contractor, job applicant, or *student*. For example, this includes profiling an employee using keystroke loggers, productivity or attention monitors, video or audio recording or live-streaming, facial- or speech- recognition or -detection, automated emotion assessment, location trackers, speed trackers, and web-browsing, mobile-application, or social-media monitoring tools”#

<sup>30</sup> Cal. Business and Professions Code § 1798.140(d).

Government agencies are not subject to the CCPA. There is some ambiguity as to whether and how service providers to government entities are covered. Under CCPA regulations promulgated by the Agency, ed tech providers that otherwise meet covered “business” thresholds may have to comply with some CCPA obligations even if acting in service to a government agency: “(g) Whether an entity that provides services to a nonbusiness must comply with a consumer’s CCPA request depends upon whether the entity is a “business,” as defined by Civil Code section 1798.140, subdivision (d) (7050(g)).”

This creates a somewhat complicated CCPA situation for ed-tech businesses that may be acting as service providers to postsecondary institutions, or may be operating independently with students. Typically, institutions and vendors acting as service providers will also be acting as FERPA “school officials,” and will follow such rules with respect to student rights, requiring that students’ requests go through the institution (which would be consistent with service provider rules). If students are directly sharing information with an ed tech provider, and consenting to such sharing, and the ed-tech provider determines the means of processing, the provider may be a CCPA business, and therefore need to respond itself to student requests.

### III. HIGHER EDUCATION INSTITUTION PRACTICES

Higher education institutions are increasingly using courseware, especially in larger or introductory-level classes. Courseware serves many purposes, including providing access to class textbooks, administering quizzes and assignments, and hosting discussion forums. In 2022, approximately one-third of faculty reported using “access codes and adaptive learning products,” a number that has grown since the mid-2010s.<sup>31</sup> In the U.S., there are nearly 18 million enrolled college students.<sup>32</sup> Many millions of those use courseware, including digital textbooks. Major digital textbook publishers include McGraw Hill (Connect), Cengage (MindTap), and Pearson (MyLab).

---

<sup>31</sup> Swaak, T. (2003, July 18). The Substitute Teacher. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-substitute-teacher>

<sup>32</sup> *College enrollment statistics in the U.S.: Bestcolleges*. (2024, Feb. 7). BestColleges.com. <https://www.bestcolleges.com/research/college-enrollment-statistics/>.

---

While the numbers reported may not be distinct to the U.S., in 2023, **5.3 million students or educators** activated McGraw Hill's Connect product, Pearson sold **5.5 million units** across its main digital instructional material offerings, and Cengage boasted similar numbers of “unlimited” higher education digital instructional material users.<sup>33</sup>

## A. Selecting Digital Instructional Materials

Institutions exert varying levels of direction and control over digital textbooks. Based on interviews and available research and reporting, in California, it is most common for individual instructors to choose materials and any accompanying digital texts.<sup>34</sup> One expert estimated it at 90%, though noted that sometimes it is a departmental decision.<sup>35</sup>

Academic freedom is highly valued, allowing instructors to choose materials that provide the best pedagogical fit. However, this freedom means there is less formal institutional oversight over technology tools used. Vendor outreach also plays a role in influencing these decisions. As noted by students at UC Berkeley, “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.”<sup>36</sup>

Schools may provide support for selecting digital instructional material,<sup>37</sup> and may also have separate governance boards and guidelines regarding privacy practices and technology. These may provide lists of approved technology resources, though it appears uncommon for training to extend to choosing digital textbooks.<sup>38</sup>

---

<sup>33</sup> Swaak, T. (2003, July 18). The Substitute Teacher. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-substitute-teacher>; Swaak, T. (2023, July 20). The “Textbook” That Reads You. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-textbook-that-reads-you>. Cengage had over 5.5 million “unlimited” users (likely worldwide), which would seem to indicate higher ed not secondary. Cengage unlimited. Retrieved Aug. 10, 2024 from <https://www.cengage.com/unlimited/>.

<sup>34</sup> Julian Sanghvi & Sriraksha Srivatsav (2024). *Higher Education Student Privacy In CA: The Need for Separate and Stronger Laws*. U.C. Berkeley School of Law Consumer Protection Public Policy Order. On file with Privacy Rights Clearinghouse. “According to a comprehensive 2017 study, decisions regarding edtech in higher education are increasingly decentralized and made at the individual faculty level”

<sup>35</sup> J. Glapa-Grossklag. Interview, May 21, 2024.

<sup>36</sup> Julian Sanghvi & Sriraksha Srivatsav (2024). *Higher Education Student Privacy In CA: The Need for Separate and Stronger Laws*. U.C. Berkeley School of Law Consumer Protection Public Policy Order. On file with Privacy Rights Clearinghouse. See also Swaak, T. (2023, July 20). The “Textbook” That Reads You. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-textbook-that-reads-you>. “In many cases, individual instructors adopt and assign courseware to students without a formal approval process.”

<sup>37</sup> Swaak, T. (2023, July 18). The Substitute Teacher. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-substitute-teacher>.

<sup>38</sup> J. Glapa-Grossklag. Interview, May 21, 2024.

In some cases, educational institutions dictate which digital instructional materials must be used. As *The Chronicle of Higher Ed* reports, “[a]doption...is not always the faculty member’s choice, in many lower level courses, instructors are required—or encouraged—to use a predetermined courseware product to maintain consistency across sections.”<sup>39</sup> One study found that a quarter of faculty do not choose their own instructional materials.<sup>40</sup> And, institutions may participate in 1:1 programs that in a practical sense consolidate choices.<sup>41</sup>

## B. Contracting for Digital Textbooks

Courseware publishers may (or may not) have contracts in place with institutions. While institutions typically have policies, procedures, and procurement departments in place to safeguard student or employee data, and go through reviews before purchasing software that may live on institutional devices, such as school-wide learning management systems (LMS),<sup>42</sup> digital textbooks are a different story.

A textbook publisher that wants to integrate directly into an LMS may go through a structured review and contracting process. Otherwise, it likely would not. IT and privacy departments may prefer the ability to negotiate contracts with all ed tech vendors—including digital text publishers—and assess for security and privacy, as well as other features like accessibility. But in many cases, institutions may not even know which publishers are being used by instructors.

When an instructor independently selects digital instructional materials, there may or may not be contracts in place with the institution. It may be recommended, but not required, by either the school or the publisher. Or it may be officially recommended but not a requirement that the school enforces. In records requests made to a California Community College, a University of California, and a California State institution for contracts between the institution and three large digital textbook providers and two large bookstores, only contracts with bookstores—Follett, specifically—were returned. Two other contracts—involving McGraw Hill and Cengage and California higher ed institutions—were also examined<sup>43</sup>.

---

<sup>39</sup> Swaak, T. (2023, July 18). The Substitute Teacher. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-substitute-teacher>.

<sup>40</sup> Swaak, T. (2023, July 19). The Homework Tax. *The Chronicle of Higher Education*. Julian Sanghvi & Sriraksha Srivatsav (2024). *Higher Education Student Privacy In CA: The Need for Separate and Stronger Laws*. U.C. Berkeley School of Law Consumer Protection Public Policy Order. On file with Privacy Rights Clearinghouse. Noting “UCLA has its Board on Privacy and Data Protection, whereas the University of Chicago looks to its Data Stewardship Council for guidance.” <https://www.chronicle.com/article/the-homework-tax>.

<sup>41</sup> See, e.g., The Ohio State University Office of Technology and Digital Innovation Digital Flagship Program. Retrieved Aug. 10, 2024 from <https://it.osu.edu/digital-flagship>.

<sup>42</sup> The HECVAT provides a useful tool for review that many interviewees referenced. It is security focused, but has a few questions about privacy, focused on HIPAA but also about if the vendor can comply with IT’s privacy and data protection policies and has its own privacy policy. [Educause. \(2024, June 2021.\) Higher Education Community Vendor Assessment Toolkit. https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit](https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit)

<sup>43</sup> SPARC. Textbook Billing Contract Library database. <https://sparcopen.org/our-work/automatic-textbook-billing/contract-library/>.



If institutions work directly with publishers, or mandate specific digital textbooks, it is likely there will be an institutional level contract in place. Publishers that contract directly with schools typically agree to data use terms that limit the use of student data they obtain through the course.<sup>44</sup> In the ed tech space, these contracts directly with institutions may indicate that the school is sharing information with the provider and such sharing falls under the FERPA school official exemption and student information remains under the direction and control of the school. Anecdotally, some publishers have also claimed to not be FERPA officials, such as in circumstances when dealing with the fallout of a breach or exposure of student data. This is also evident in some contracts which fail to mention FERPA altogether.

### **1. Institutional Contracts with Publishers and Distributors**

Contracts between institutions and publishers take different approaches to student information and privacy. In a 2017 contract between McGraw Hill and San Diego State University for online educational products, McGraw Hill agreed to act as a FERPA school official. McGraw Hill also agreed to only use data for facilitating the performance, delivery, or use of the services, and the personally identifiable information of end users is considered the institution's confidential information.<sup>45</sup> The contract, however, also notes that end users (students) will be required to agree to a terms of use and privacy notice separately, and if McGraw Hill products are integrated into an LMS then the McGraw Hill "campus terms of use" apply, not the terms of the agreement.<sup>46</sup>

In contrast, a 2020 contract between Cengage and UC Davis for educational course materials (including Cengage EBook or Courseware) contained standard information confidentiality requirements and a data security appendix, but did not acknowledge that students' personal information may be transmitted or reference FERPA.<sup>47</sup> Instead, in the section regarding the institutional information that may be transmitted, the lowest security protection level is applied, and the explanation typed in is "Dept is only buying books." Regarding data elements that may be transferred, personally identifiable information and "Student data, whether or not subject to FERPA" are both boxes left unchecked, and in the applicable laws section—neither FERPA nor CCPA or any privacy law is marked.<sup>48</sup>

This purported lack of data collection from ebooks and digital texts seems to reflect a misunderstanding of how courseware operates, and it is at odds with the disclosures

---

<sup>44</sup> Meinke, B. (2018, March 21.) Student Data Grabbers. <http://billymeinke.com/2018/03/21/student-data-grabbers/>

<sup>45</sup> McGraw Hill and San Diego State University, MHE Subscription and Product Purchase Agreement. (2019). SPARC. Textbook Billing Contract Library database. <https://sparcopen.org/our-work/automatic-textbook-billing/contract-library/>.

<sup>46</sup> The campus terms of use URL is no longer a valid link and McGraw Hill no longer appears to have "campus" terms of use.

<sup>47</sup> Cengage and UC Davis, Purchase Agreement (2020). SPARC. Textbook Billing Contract Library database. <https://sparcopen.org/our-work/automatic-textbook-billing/contract-library/>.

<sup>48</sup> Cengage and UC Davis, Purchase Agreement (2020). SPARC. Textbook Billing Contract Library database. <https://sparcopen.org/our-work/automatic-textbook-billing/contract-library/>.

Cengage makes in its posted privacy policy online (though it is possible that the institution negotiated an agreement in which no information was collected and the textbooks were configured in an entirely unique way).

Cengage's freedom to do what it wishes with student information, however, is consistent with its online promises to students, discussed below.

Thus, there appears to be a wide variation in what institutions require and negotiate from those offering digital courseware to their students, even when looking at a narrow range of institutional contracts.

And, as seen in the McGraw Hill contract, even such institutional level contracts may indicate that if a student separately agrees, a courseware provider may be governed by a different set of rules.

## C. The Role of Campus Bookstores

While in many (if not all) instances digital texts can be purchased or accessed from the publisher's website, students are often directed to campus bookstores to obtain their digital instructional materials.<sup>49</sup> It appears standard for the campus bookstore to have contracts with the institution—perhaps not surprising because the bookstore typically also has a physical space and contracts need to address much more than the provision of digital materials and data collection.

In addition to potentially costing the student more because of retail mark ups, especially if the publishers do not offer wholesale pricing to the bookstore,<sup>50</sup> the use of the bookstore exposes student information to yet another vendor. Common higher-education bookstore distributors include Barnes & Noble, Vital Source, and Follett.

### 1. Bookstore contracts

Sometimes bookstore contracts limit the bookstores' ability to use student information, and sometimes they fail to address it at all.

The student bookstore contracts examined—both with Follett—each referenced privacy laws and receiving student data to varying degrees. The bookstore contracts address

---

<sup>49</sup> Swaak, T. (2023, July 19). The Homework Tax. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-homework-tax>. Per *The Chronicle*, this may be due to institutional contracts with the bookstore or leadership pressure.

<sup>50</sup> See Swaak, T. (2023, July 19). The Homework Tax. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-homework-tax>.

more than simply digital instructional materials and also addresses physical and online stores.

A Cal State Northridge bookstore contract that was last updated in 2023, contained security and IT requirements that were added in 2019. These provisions acknowledge that personal information and student records may be transferred under the contract. They noted that such information may be subject to the CCPA, require data confidentiality, and limit the ability of the bookstore to disclose such information.

In a UC San Diego contract last updated in 2023, there is a 2021 amendment which states Follett may only use and disclose information as directed by the institution, notes that student records and information covered by FERPA are confidential, and requires an agreement by Follett to protect the privacy of information. There is also a Data Security Appendix from 2021 that references personally identifiable information, student data, CCPA, and FERPA.

It defines Institutional Information to mean “[a]ny information or data created, received, and/or collected by UC or on its behalf, including but not limited to: application logs, metadata, and data derived from such data”, a requirement for limiting access, use, and disclosure of information “to the least invasive degree necessary required to provide the Goods and/or Services.” There are clear prohibitions including against using student information for marketing or advertising unless approved:

“1. Supplier may not access or use Institutional Information and IT Resources for any purpose except to provide the Goods and/or Services. 2. For the avoidance of doubt, Supplier may not access, use, or disclose Institutional Information and IT Resources outside the scope of the Agreement for purposes of, including but not limited to: marketing, advertising, research, sale, or licensing unless expressly approved in writing by UC”

There is a copy of Follett’s information security plan and even an addendum addressing information if it is subject to European privacy law.

## **D. Learning Management Systems**

Another courseware middleman between digital texts and bookstores is the Learning Management System (LMS). Approximately 75% of the market is covered by three LMS

companies.<sup>51</sup> While largely outside of the scope of this report, LMS typically have contracts with institutions. Researchers and journalists have filed records requests that surfaced contracts with learning management systems (LMS), like Blackboard, which house digital materials—including texts, instructor syllabi, recorded classes, and other materials—for an institution.

## IV. STUDENT EXPERIENCES WITH COURSEWARE DATA PRACTICES

Students access courseware, including digital textbooks, in various ways, but they typically have some form of individual sign-up where they must consent to data practices in a privacy policy.<sup>52</sup>

**These policies, often written in legalese, differ by publisher and may carve out capabilities for digital text providers to use higher education students' information for marketing and commercial purposes.**

These data practices also involve the collection of a large volume of information, which can be vulnerable to data breach.



<sup>51</sup> Canvas, a widely popular LMS, is reported to be used by approximately 36% of North American higher education institutions, while platforms such as Blackboard and Moodle are used by a combined 40% of such institutions. Canvas, owned by the for-profit company, Instructure, reported revenue totaling \$128.8 million in 2023. Universities and colleges in California use LMS for online coursework, reading, quizzes, and grading assignments. Julian Sanghvi & Sriraksha Srivatsav (2024). *Higher Education Student Privacy In CA: The Need for Separate and Stronger Laws*. U.C. Berkeley School of Law Consumer Protection Public Policy Order. On file with Privacy Rights Clearinghouse.

<sup>52</sup> Online privacy policies are frequently updated—annually, or even semi-annual, updates are not uncommon. Technology companies update and introduce new products and practices, and seek to describe such updates in their policies. When privacy policies are cited in this report, the effective date of the policy examined is noted.

## A. Accessing Digital Textbooks

Three major digital instructional materials publishers all offer several methods of student access to their products. Schools may provide students with an access purchase code, when an institution itself purchases the digital texts. (This may be more common when an institution mandates certain digital texts and the publisher directly contracts with the institution.) Students are also able to purchase access themselves, enter by paying directly with a payment card, adding the cost to their school bill, or by purchasing temporary access while they await financial aid.<sup>53</sup>

### 1. Student “Consent”

Regardless of how digital instructional materials are chosen, contracted for, and paid for—students are themselves consenting to privacy policies and terms of use when they access such courseware. These policies and terms are opaque and difficult to parse—even for lawyers. In many instances, companies offer multiple overlapping policies. Over the course of our review, for many months, one policy appeared to be an almost finished draft.<sup>54</sup>

Only Cengage and Pearson purport to get consent for marketing to students. They may view this separate contract as a way to allow them additional freedom to use students’ information in ways that are not directly related to the institution or the students’ learning.

With Pearson, students must provide information like email, username, password, first and last name, and country, in order to create an account, and can search for a course or use a course ID. Students can pay via credit card, prepaid access codes, PayPal, or request temporary access. Pearson requires that students agree to its privacy policy and terms of use, and has a pre-checked box for marketing information.<sup>55</sup>

Cengage asks for similar information as Pearson, though it requests not country but birth year. Basic account information requested is the same regardless of whether students are purchasing the product then or have a code.<sup>56</sup> Cengage also requires consent to its privacy policy and terms of use, and also has a pre-checked marketing box.

---

<sup>53</sup> See Pearson Support Page. Retrieved Aug. 10, 2024 from [https://support.pearson.com/getsupport/s/document-item?bundleId=mlm-create-stu&topicId=Content/register\\_enroll.htm&\\_LA\\_NG=en-us](https://support.pearson.com/getsupport/s/document-item?bundleId=mlm-create-stu&topicId=Content/register_enroll.htm&_LA_NG=en-us); McGraw Hill Connect Access Code and Purchase FAQ. Retrieved Aug. 10, 2024 from <https://www.mheducation.com/highered/support/connect/smartbook/connect-access-code-and-purchase.html>

<sup>54</sup> Pearson’s policy, when reviewed before August 1, 2024, had in many instances bracketed language or a flag to “insert link”. Pearson Privacy Policy, last updated June 2023 version.

<https://www.pearson.com/en-us/privacy-center/privacy-notice/full-privacy-notice.html>. Pearson’s policy now posts an update date August 6, 2024, and may no longer be in draft. The relevant sections cited remain substantively the same.

<sup>55</sup> See Pearson Support Page. Retrieved Aug. 10, 2024 from [https://support.pearson.com/getsupport/s/document-item?bundleId=mlm-create-stu&topicId=Content/register\\_enroll.htm&\\_LA\\_NG=en-us](https://support.pearson.com/getsupport/s/document-item?bundleId=mlm-create-stu&topicId=Content/register_enroll.htm&_LA_NG=en-us).

<sup>56</sup> Cengage How To Register for Mindtap. Retrieved Aug. 10, 2024 from <https://startstrong.cengage.com/mindtap-not-integrated-ia-yes/>.

McGraw Hill requests slightly less information (no country, no birthdate); requires consent to its privacy policy, general terms of use and a “consumer purchase terms of use if applicable”; and in a meaningful distinction has no marketing checkbox.<sup>57</sup>

In addition to privacy policies, users agree to terms of use. These courseware terms offer limited, personal, non-transferable license to access and use services,<sup>58</sup> and as documented by the Chronicle, the concept that the products are for individual use only is a restriction that “is hard to circumvent; the products are often integrated directly into campus learning-management systems and linked to each student’s gradebook.”<sup>59</sup>

The notion of student consent in this context—for digital instructional materials, and for related technology like LMS—is questionable. Students themselves feel a lack of agency in the process, and also as if they have no choice.



**Consent appears to be neither informed nor freely given. In fact, if students choose to opt out, they may not be able to access their textbook or much of their coursework, which would in-turn impact their grade.**

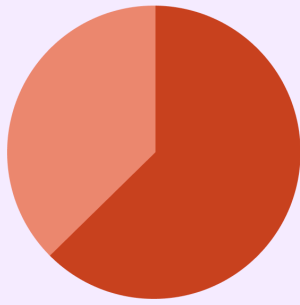
Anecdotally, institutional staff report that students typically don’t associate textbooks with privacy issues (students are more likely to voice concerns about accessibility and price). And according to a small qualitative study by UC Berkeley Law students, approximately 60% of the students surveyed were “not sure” if the LMS they use has a privacy policy. Some commented that in their “experience throughout college and university [they] have never been presented with or shown a privacy policy agreement to consent to when using a site like Canvas, or any courseware platform.”

---

<sup>57</sup> McGraw Hill Student Registration. Retrieved Aug. 10, 2024 from <https://accounts.mheducation.com/registration>.

<sup>58</sup> Pearson Terms of Use, last updated Sep. 29, 2023 version. <https://www.pearson.com/en-us/legal-information/terms-of-use.html>.

<sup>59</sup> See Swaak, T. (2023, July 19). The Homework Tax. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-homework-tax>.



**62.5%**

**of students surveyed believed that their grades depended on paying for access to ed tech platforms**

Also, 90% of them expressed that their university or professor has not discussed the privacy implications of registering with an ed tech platform. Further, approximately 67.5% of the students did not know or were not aware that personal and personally identifiable information was collected through these technologies. 87.5% did not know who receives their data and how it is being used/stored, and 70% of students were unaware that these platforms sometimes sell their data to other companies. What's more, many students did not feel they had a choice when it came to purchasing access to course materials—approximately 62.5% believed that their grades depended on paying for access to such ed tech platforms.

## **B. Courseware Information Collection**

### **1. From Students and Student Activity**

Standard courseware information requests include a student's contact information (email, phone, name), school identifiers, school, classes, and scores or progress or grades within course materials. Teacher comments, class participation, discussion forum, responses to quizzes, uploaded content, graduation date, and expected degree, may also be collected. Analytics and other technical information is also collected—this could include information like language and other device settings, movement through courseware, and so forth. Location information is collected at varying levels of specificity.<sup>60</sup>

---

<sup>60</sup> See Pearson Digital Learning Services Privacy Notice, effective Jan. 1, 2023. [https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy\\_en\\_US.html?cc=US&lang=en\\_US](https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy_en_US.html?cc=US&lang=en_US) ; <https://cengage.widen.net/view/pdf/hk69f4p7oq/cengage-privacy-notice-october-2020-1508150.pdf?t.download=true&u=lpaan>.

Audiovisual information may also be captured—while this would seem most applicable in situations where there is remote or online proctoring,<sup>61</sup> Cengage also notes it collects “ photographs and video and audio recordings that are captured when you participate in a course.”<sup>62</sup> For students purchasing software, financial information is also collected as part of that transaction. And, if students select that they need temporary access—perhaps because they are waiting for a financial aid award—that information may be collected as well.

This is a lot of information from the outset. Some of it seems inherently sensitive, and concerning in terms of potential opportunities to profile, label, or limit students. This includes information about a students’ eligibility or need for financial aid, specific location information, and grades. In addition, even information that may seem innocuous for a courseware provider to collect—such as progress through a course, or answers to quiz or homework questions—can be concerning, or especially sensitive. The Chronicle, for example, details invasive questions asked about students’ sexual history and practices for a gen-ed health-and-fitness class.<sup>63</sup>

## 2. From Non-Student Sources of Information

Courseware publishers also receive information about students that does not come directly or indirectly from students themselves. This information often comes from the educational institution or LMS. Pearson, for example, says it gets information from third parties such as schools or institutions that may “arrange for [student] access to our Services.”<sup>64</sup> However, information may come from unexpected third party sources as well. Cengage discloses that in addition to receiving information from a student’s educational institution, or from a learning management system,<sup>65</sup> it also receives student information from data brokers—in order to “enhance our files and help us better understand our customers.”<sup>66</sup>

---

<sup>61</sup> Proctoring software has been accused by many of violating student’s privacy –and in at least one case, found to violate constitutional rights. See, e.g., Electronic Privacy Information Center. (2020.) In re Online Test Proctoring Companies. <https://epic.org/documents/in-re-online-test-proctoring-companies/> and Bowman, E. (2022, Aug. 21). Scanning students’ rooms during remote tests is unconstitutional, judge. National Public Radio.

<https://www.npr.org/2022/08/25/1119337956/test-proctoring-room-scans-unconstitutional-cleveland-state-university/>  
<sup>62</sup><https://cengage.widen.net/view/pdf/hk69f4p7oq/cengage-privacy-notice-october-2020-1508150.pdf?t.download=true&u=lpaanbn>

<sup>63</sup> Swaak, T. (2023, July 20). The “Textbook” That Reads You. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-textbook-that-reads-you>

<sup>64</sup> See Pearson Digital Learning Services Privacy Notice, effective Jan. 1, 2023 version. [https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy\\_en\\_US.html?cc=US&lang=en\\_US](https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy_en_US.html?cc=US&lang=en_US)

<sup>65</sup> “Your educational institution or employer may provide us Identifiers about you if they purchase Cengage products for your use. We also receive Identifiers from learning management systems (LMS) and third-party products and services that integrate with or complement our Products.” Cengage Privacy Notice, updated Jan. 12, 2024 version at <https://cengage.widen.net/view/pdf/hk69f4p7oq/cengage-privacy-notice-october-2020-1508150.pdf?t.download=true&u=lpaanbn>.

<sup>66</sup> Cengage Privacy Notice, updated Jan. 12, 2024 version at <https://cengage.widen.net/view/pdf/hk69f4p7oq/cengage-privacy-notice-october-2020-1508150.pdf?t.download=true&u=lpaanbn>.



## C. Information Use and Sharing with Educational Institutions and Third Parties

**Courseware publishers collect, use, and share information from and about students. The collection and use is in many instances part and parcel of their tracking and monitoring of student progress.**

Courseware, and digital textbooks specifically, are inherently designed to share information with the educational institution in which the student is taking the course. Policies disclose sharing student information with institutions if courseware is part of an educational course, regardless of who purchased or contracted for the courseware. This information sharing appears impossible for a student to limit. There are no instructions within privacy statements of how students may limit such information sharing. When questioned about this by *The Chronicle*, a publisher explained it is up to the instructors themselves to set these options for limiting sharing to institutions themselves.<sup>67</sup>

Aside from institutions, digital instructional materials publishers share information with other sources. Courseware providers such as Cengage and Pearson report broad sharing with respect to analytics and other technical information. This is consistent with reporters finding, in testing, for example, that Pearson shared information with Google Analytics.<sup>68</sup> How broadly courseware publishers share information seems dependent on how they define themselves and if they offer special protections to higher education data.

### 1. McGraw Hill Connect

Among courseware publishers, McGraw Hill comes the closest to the paradigm of a “school official.” It has publicly stated it considers itself a school official,<sup>69</sup> and in the institutional contract examined it also agreed to as much.

---

<sup>67</sup> “McGraw Hill spokesperson wrote in a statement that instructors using Connect “can choose a ‘privacy option’ on assignments such as these, which give students the ability to opt out of their responses being stored. They can also choose a ‘responses saved’ option so responses are saved in aggregate for the instructor.” The spokesperson added that the company employs “sophisticated, cryptographic encryption” for data it stores.” Swaak, T. (2023, July 20). *The “Textbook” That Reads You. The Chronicle of Higher Education.* <https://www.chronicle.com/article/the-textbook-that-reads-you>

<sup>68</sup> “Every time the reporter logged in to Pearson MyLab and reached the course home page, web page details that included the user’s first and last name, along with the name of the college where the user was enrolled, were sent to Google Analytics. Whenever she viewed the account details page, Google Analytics got the user’s email address.

...

The *Chronicle* also recorded other cases of data disclosure that could theoretically be used to help a company like Google build a unique user profile. For one, among the personally identifiable data sent to Google Analytics was a unique, eight-digit user ID that the reporter observed on a handful of different pages within MyLab. As the reporter interacted with the Pearson eBook, too, Google Analytics gleaned the name of the book and chapter she was reading — even the blocks of text she highlighted, and the exact time that she did so.” Swaak, T. (2023, July 20). *The “Textbook” That Reads You. The Chronicle of Higher Education.* <https://www.chronicle.com/article/the-textbook-that-reads-you>

<sup>69</sup> Swaak, T. (2023, July 20). *The “Textbook” That Reads You. The Chronicle of Higher Education.* <https://www.chronicle.com/article/the-textbook-that-reads-you>

Its privacy statement confirms that it is a service provider to the institution.<sup>70</sup> (By contrast, the Chronicle notes that “Pearson and Cengage did not respond to specific questions about how they define themselves under [FERPA]”).<sup>71</sup> It appears that McGraw Hill acts as a school official whether the institution has provided the digital instructional materials or the student has purchased it. While its privacy policy notes there may be some circumstances in which students may be customers—creating some ambiguity as to a purchasing student’s position, in general, it has one policy and set of rules for anyone using the product “as part of a course of instruction.” It does not appear to matter whether they have purchased the product directly or not.

Relatedly, **McGraw Hill is also the most explicit in its privacy policies about limiting data use and practicing “data minimization.”** McGraw Hill promises that, “Except as described in this notice, we limit the use, collection, and disclosure of your PII to the minimum level necessary to deliver the service or information requested by you or your institution. We do not collect, use, or disclose PII that is not reasonably related to a legitimate business purpose necessary to serve you. Your information may also be used in order to maintain and/or improve our services.”<sup>72</sup> **(As acknowledged by McGraw Hill’s privacy officer, such high-level language, especially regarding “improving services,” still offers companies latitude, and it may be an area where tightening is desired.)**<sup>73</sup>

## 2. Pearson MyLab

In reviewing policies, **it is unclear when Pearson considers itself to be a “school official”** (or processor) who acts on behalf of the institution, and when it **considers itself to be acting in its own independent capacity with freedom to decide how to use student data.** It seems likely that sometimes, but not always, Pearson acts on behalf of the school. Pearson’s privacy notices simply state that when FERPA applies, it complies.<sup>74</sup>

---

<sup>70</sup> McGraw Hill Privacy Notice: End User, last updated Feb. 28, 2024 version, <https://www.mheducation.com/privacy.html?ot-policy=end-user>. “Since McGraw Hill is a service provider to your institution, your institution is best able to provide you with a full understanding of their privacy practices and more information on how their end user’s Personally Identifiable Information (PII) is collected, shared, and used. To obtain more detailed information about how PII is collected, used, and shared by your educational institution, please contact the appropriate individual at that institution.”

<sup>71</sup> Swaak, T. (2023, July 20). The “Textbook” That Reads You. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-textbook-that-reads-you>

<sup>72</sup> McGraw Hill Privacy Notice: End User, last updated Feb. 28, 2024 version, <https://www.mheducation.com/privacy.html?ot-policy=end-user>. “We will not sell PII to other organizations, nor will we market to students using the information from their educational records (education records are defined as records directly related to a student and maintained by an educational agency or institution, or by a party acting for the agency or institution).

McGraw Hill does maintain the ability to share information with a student’s institution and professors:

“Educational Institutions / Corporation – As we provide products and services to your institution / corporation, we share your data with approved individuals such as administrators or educators.”

<sup>73</sup> Swaak, T. (2023, July 20). The “Textbook” That Reads You. *The Chronicle of Higher Education*. <https://www.chronicle.com/article/the-textbook-that-reads-you>.

<sup>74</sup> Pearson Digital Learning Services Privacy Notice, effective Jan. 1, 2023 version. [https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy\\_en\\_US.html?cc=US&lang=en\\_US](https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy_en_US.html?cc=US&lang=en_US). “Pearson complies with all applicable provisions of the United States Family Educational Rights and Privacy Act, 20 U.S.C. 1232g, 34 CFR Part 99 (FERPA) in receiving and handling personally identifiable information from education records as a “school official” under FERPA.”

Pearson’s policies indicate “course data” will be processed for educational purposes, or processed at the direction of the school, for students registering for or purchasing educational courses.<sup>75</sup> The privacy statements indicate that Pearson has better data processing practices when it is acting as a processor to the school. (By contrast, when Pearson processes information for promotions, and targeted ads, it does so as a controller.) It seems Pearson is likely a processor or FERPA “school official” with educational institutional courseware generally, though Pearson does not definitively say this. Rather, it states that it processes data on behalf of institutions “commonly” when the courseware is “purchased,” though also sometimes when the student is “affiliated” with an educational institution.<sup>76</sup> Pearson does make clear that when it is a processor to an institution, it will not handle consumer access/deletion/consumer requests—and this seems to occur when education records or course data are involved.<sup>77</sup>

Even when Pearson acts on behalf of the school as a processor or school official, Pearson maintains (debatably limited) rights to process data as a controller—meaning it decides what happens and it is not acting as a service provider to the institution. One of the rights it maintains is to use data for analytics. This is consistent with reporting from *The Chronicle* which found that “in a review of Pearson MyLab, personally identifiable information, such as a student’s name and email, were sent to Google Analytics, along with notifications of what the student was reading and highlighting in their eBook.”<sup>78</sup>

### 3. Cengage MindTap

Cengage’s public-facing policies indicate that there are times it acts as a processor to institutions—meaning it should act only at their direction<sup>79</sup>—but it is not clear when those times are, and it is more clear that Cengage has carved out for itself rights to broadly process and share data. **Cengage does not say it processes data in compliance with**

---

<sup>75</sup> It bears acknowledgement that FERPA does not technically directly apply to ed tech providers; but it may apply to them in the sense that the information they handle is covered by FERPA and therefore they need to support educational institutions’ compliance. If students “register for or purchase educational courses...personal data will be collected and processed for the purpose of delivering such educational courses to you” Pearson Privacy Policy, last updated June 2023 version.

<https://www.pearson.com/en-us/privacy-center/privacy-notices/full-privacy-notice.html>. Pearson also states when processing “Course Data” it will provide and disclose student personal information to an Educator or Institution and “as otherwise directed by the Educator or Institution.” Pearson Digital Learning Services Privacy Notice, effective Jan. 1, 2023 version.

[https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy\\_en\\_US.html?cc=US&lang=en\\_US](https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy_en_US.html?cc=US&lang=en_US).

<sup>76</sup> See Pearson Privacy Policy, last updated June 2023 version.

<https://www.pearson.com/en-us/privacy-center/privacy-notices/full-privacy-notice.html> “Processing on behalf of institutional customers”

<sup>77</sup> Pearson California Privacy Statement, effective Jan. 1, 2023 version,

<https://www.pearson.com/en-us/legal-information/privacy-policy/california-supplement.html>. “Where Pearson is a service provider to an educational institution, your request for access, deletion or correction of your education records or course data should be directed to your school or University. Pearson cannot modify or delete education records or other records collected or processed by, or on behalf of, an educational institution unless directed to do so by the educational institution directly.

<sup>78</sup> Swaak, T. (2023, July 20). The “Textbook” That Reads You. *The Chronicle of Higher Education*.

<https://www.chronicle.com/article/the-textbook-that-reads-you>.

<sup>79</sup> Cengage says ““Note that in some cases we provide our products and services as a “processor” or “service provider” to your educational institution or employer, in which case we process personal information according to instructions from your educational institution or employer and our contract with them. In those instances, the information in this Privacy Notice is intended to provide transparency in relation to our privacy practices and you should refer to the privacy practices at your educational institution or employer.” Cengage Privacy Notice, updated Jan. 12, 2024 version at <https://cengage.widen.net/view/pdf/hk69f4p7oq/cengage-privacy-notice-october-2020-1508150.pdf?t.download=true&u=lpaan>. It is not totally clear when this applies.

**FERPA or that it supports schools' FERPA obligations.** (This is also consistent with the Cengage contract examined, which did not indicate FERPA covered data was being transferred.) In fact, it only mentions FERPA when it tells residents of certain states that those states' privacy rights do not apply when personal information is subject to FERPA.<sup>80</sup>

Cengage discloses that if students are "affiliated with an educational institution" Cengage will share information with instructors and institutional clients. (E.g., "If you are a student, your instructors will have access to the information generated by your use of a product for a class and certain information that you enter into the product.")<sup>81</sup> Who pays for the product does not seem to matter.

While it is not clear precisely what data practices Cengage engages in—according to the policy this is "[d]epending on your relationship with us" but not explicitly delineated—Cengage does carve out rights in their policy to communicate with users on social media, use photos and videos for social media, and engage in advertising as described below.

## **D. Treatment of Higher Ed Students vs. Younger Students**

---

**In the K-12 student space, there are many state laws to protect student data use, and to prohibit its sale or commercial use.**

It is informative that McGraw Hill treats higher ed students the same way it treats K-12 students, under one policy,<sup>82</sup> implicitly offering all higher ed students whatever protections are mandated under K-12 laws. Notably, Cengage and Pearson distinguish between K-12 students and higher ed students. Cengage has a separate policy for K-12. And Pearson references "Youth Users" vs. other Users who are 18 and over.

---

**Higher Ed students do not therefore appear to benefit from the protections applicable in the K-12 space at Cengage and Pearson.**

---

<sup>80</sup> See Utah or California Privacy Rights. Cengage Privacy Notice, updated Jan. 12, 2024 version at <https://cengage.widen.net/view/pdf/hk69f4p7oq/cengage-privacy-notice-october-2020-1508150.pdf?t.download=true&u=lpaan>.

<sup>81</sup> Cengage Privacy Notice, updated Jan. 12, 2024 version at <https://cengage.widen.net/view/pdf/hk69f4p7oq/cengage-privacy-notice-october-2020-1508150.pdf?t.download=true&u=lpaan>.

<sup>82</sup> McGraw Hill Privacy Notice: End User, last updated Feb. 28, 2024 version, <https://www.mheducation.com/privacy.html?ot-policy=end-user>.

## E. Use of Student Information for Advertising and Marketing

The publishers' approaches to marketing are consistent with the above described practices. McGraw Hill does not disclose use of higher ed student personal information for advertising or marketing, likely because it treats such information like K-12 student personal information and such information typically may not be used in such ways under law. Pearson reserves the right to send adult students marketing emails, as compared to under 18 students.<sup>83</sup> However, Pearson does indicate it will not use "course data" to serve marketing.<sup>84</sup> **Cengage says, early on and repeatedly in its privacy policy, that it may use information to deliver ads, including on social media platforms.**<sup>85</sup>

## F. Why Do Publishers' Data Practices Differ?

There seem to be varying levels of data protection offered by digital instructional materials publishers—McGraw Hill, in contracts and posted privacy policies, appears, for example, to make less commercial use of student data. The reasons for these differences are not clear.

While one may expect that a courseware publisher's practices vary depending on their relationship with the educational institution, as discussed above, it does not appear to matter much whether a publisher has a contract with an institution. As described above, contracts with institutions do not appear to be standard practice, and contracts that exist vary in terms of promises and protections.

---

<sup>83</sup> Pearson Privacy Policy, last updated June 2023 version.

<https://www.pearson.com/en-us/privacy-center/privacy-notice/full-privacy-notice.html>.

<sup>84</sup>9. Marketing Communications and Opting Out

Depending on our relationship with you, and the service you use we will send you marketing communications where you have not told us that you wish to unsubscribe from marketing, or where you signed up to receive such updates. Contact details for teachers, learners who are 18 or over, and adult subscribers to the Services may be used for these purposes:

i. to contact the user with more information about our Services and those of our group companies, except where the user has told us not to;

Pearson will not use Personal Information collected or processed by Pearson as a school service provider of a secondary school to send or direct marketing communications to Secondary Student Users. Pearson otherwise may use User Personal Information to market products, services and educational programs to a User, provided that (a) such use and marketing is consistent with applicable law and Pearson's legal obligations; (b) such Personal Information excludes Payment Data and Course Data; (c) the User has not opted out of receiving marketing; and (d) where required by applicable law, express or implied consent to marketing exists and has not been withdrawn. Pearson does not permit third-party ad networks or similar services to access or collect Personal Information within the Services. Users may change their marketing preferences at any time. Pearson will not knowingly direct or send marketing communications to a User who has expressed a preference not to receive marketing."

<sup>84</sup> Pearson Digital Learning Services Privacy Notice, effective Jan. 1, 2023 version.

[https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy\\_en\\_US.html?cc=US&lang=en\\_US](https://loginstatic.pearson.com/html/NA/PearsonPrivacyPolicy_en_US.html?cc=US&lang=en_US).

<sup>85</sup> Cengage Privacy Notice, updated Jan. 12, 2024 version at

<https://cengage.widen.net/view/pdf/hk69f4p7oq/cengage-privacy-notice-october-2020-1508150.pdf?t.download=true&u=lpaan>.

Whether a student purchases courseware out of pocket does not appear to influence how the courseware publishers protect student information as a school official or as a processor. What seems to matter most is if it is an educational course connected with an instructor and an institution, and then the company's general stance on treatment of information from such courses will apply.

Ultimately, the privacy protections the courseware publishers offer seem due to business decisions and preferences, not the method of contracting, payment, or procurement.

## **G. Data Breaches & Exposure of Student Information**

An additional important consideration regarding student information, courseware, and ed tech generally is the exposure of such information if there is a breach. Data breaches are common in the education space—schools and ed-tech companies have a lot of information, including sensitive information.

---

**Since 2005, our organization has recorded over 2,700 data breaches at educational institutions (this includes K-12 schools as well as higher education institutions).<sup>86</sup>**

However, schools are not the only entities being targeted. One notable Federal Trade Commission (FTC) data breach case is against Chegg, Inc., an ed-tech company who stored user data of largely high school and college students. The FTC alleged that Chegg failed to use reasonable security practices—such as multi factor authentication, unique logins, or threat monitoring—and exposed “40 million users’ names, email addresses, passwords and, for some, their religion, heritage, date of birth, sexual orientation, disabilities, and parents’ income range” along with additional sensitive information from employees.<sup>87</sup>

Of the six companies studied for this report, at least half have made news regarding security practices or data breaches. McGraw Hill reportedly left over 100,000 students’ information unsecured and available on the the internet—including student names, email addresses, and grades, during the summer of 2022.<sup>88</sup>

---

<sup>86</sup> Julian Sanghvi & Sriraksha Srivatsav (2024). *Higher Education Student Privacy In CA: The Need for Separate and Stronger Laws*. U.C. Berkeley School of Law Consumer Protection Public Policy Order. On file with Privacy Rights Clearinghouse.

<sup>87</sup> Federal Trade Commission (2022, Oct. 21) *FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers*. <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions>; Gressin, S. (2021, Oct. 31.) *Data Breaches Were Missed Learning Opportunities for Ed Tech Company*. Federal Trade Commission. <https://consumer.ftc.gov/consumer-alerts/2022/10/data-breaches-were-missed-learning-opportunities-ed-tech-company>.

<sup>88</sup> Leckrone, B. (2022, Dec. 22). *Student Information Exposed in McGraw Hill Data Breach: Report*. Best Colleges. <https://www.bestcolleges.com/news/student-information-exposed-mcgraw-hill-data-breach/>

Pearson Education Inc. suffered a data breach involving information from 55,324 individuals in 2022 as well.<sup>89</sup> Follett was the subject of a Wired article after a teen student hacker found bugs in their school security software.<sup>90</sup> The more information data courseware publishers and distributors collect, and the more third parties they share such information with—including educational institutions—the greater the risk to students’ privacy and security.

## V. RECOMMENDATIONS & CONCLUSION

### A. A Murky Landscape

—

**Students disclose personal information while doing coursework required by a professor, for a class that they pay for, using a textbook that they pay for (directly or indirectly). What happens to that personal information—whether it is appropriately protected, further monetized for other commercial purposes, or disclosed to additional parties for additional uses—is hard to decipher.**

Students themselves aren’t told how information is collected, by their institutions or in any meaningful way by the publishers. Reports indicate that faculty members themselves do not know. And even attorneys parsing posted privacy policies or combing through records-act-requested contracts may have trouble deciphering which policies or practices apply in a given situation.

---

<sup>89</sup> Privacy Rights Clearinghouse Data Breach Chronology. <https://privacyrights.org/data-breaches> references the Indiana Attorney General’s Office report found at <https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/2022-DB-Year-to-Date-Report-for-Website.pdf> (see item #280). Pearson was also charged by the SEC for misleading investors about a cyber breach in 2018 involving “the theft of student data and administrator log-in credentials of 13,000 school, district and university customer accounts,” available at <https://www.sec.gov/newsroom/press-releases/2021-154>.

<sup>90</sup> Greenberg, A. (2019, Aug. 9). This Teen Hacker Found Bugs in School Software That Exposed Millions of Records. *Wired*. <https://www.wired.com/story/teen-hacker-school-software-blackboard-follett/>

---

**What's more, publishers generally seem to require separate consent from the student. This consent is hard to call informed or freely given, based on the circumstances of why and how the student is obtaining the digital text in the first place. Indeed, if notice, choice, and consent is deemed a fiction in the broader consumer space, it is truly a fantasy in this educational context.<sup>91</sup>**

It's unclear whether publishers are school officials under FERPA or otherwise contracting with the school or a school bookstore to provide a digital product they offer via integration into the institutions' LMS, or if publishers believe they have separate consent for sharing because of the box checked.

Rather, the decision of whether to protect student information seems highly dependent upon publishers' own preferences and business models, and on whether or not institutions seek and obtain privacy protective contracts with those publishers.

---

<sup>91</sup> See note re same issues in K-12 space, Fox Johnson, A. (2020, Dec. 14). Protecting Children's Privacy at Home, at School, and Everywhere in Between. Day One Project.  
<https://fas.org/publication/protecting-children-s-privacy-at-home-at-school-and-everywhere-in-between/>



## B. A Better Model

### Ideally...



1

Students and faculty would understand how publishers use information, through clear, publicly-posted policies

2

Publishers would be required to properly safeguard student information and would be prohibited from using student information for non-educational purposes

3

The notion that students can give meaningful consent to additional uses would not persist.

There are a few policy levers that could be used to achieve this improved state:

- (1) Require it by law—require transparency around the use of students’ personal information, prohibit non-educational uses of students’ personal information (either directly, or by required contracts, or both), and prohibit reliance upon “consent” in this context. The law could also limit data retention.
- (2) Target key actors to update policies, including contracts, at the institutional consortium or industry level, such that the required institutional norm—and/or accepted industry best practice—is to be transparent about how students’ information is used and to limit its use to only educational purposes and not maintain such information indefinitely.
- (3) Raise awareness among institutional players, including faculty and administration, so they select more privacy-protective educational courseware, and explain practices to students.

### 1. Pass Laws That Protect Higher Ed Students’ Privacy

#### a) State Higher Ed Privacy Laws

There is a dearth of privacy regulation in the higher ed space. One option moving forward is to pass laws like those in the K-12 space that limit the commercial use of higher ed students’ personal information (like in California, SOPIPA), and that require contracts in place with certain restrictions between an institution and a publisher if students’ personal information is collected (like, in California, AB 1584). In addition, it

would be helpful to enact legislation requiring that these contracts are publicly posted and accessible. Laws should also specify that students' personal information cannot be maintained indefinitely—the longer it is kept the more likely it is to be misused or subject to a data breach. These laws could apply to ed tech publishers (prohibiting use of information) and institutions (contractual requirements, posting requirements). Given that publishers seek to separately obtain consent from higher ed students, these laws should not have a carve-out for when consent is obtained.<sup>92</sup> Any requirements for public institutions would benefit from being paired with additional funding.

#### **b) Modernize FERPA**

Another option would be to update and modernize FERPA. It should clearly apply to the personal information collected from students through modern educational technology. It should also be updated to close the directory information loophole, require that sharing under the FERPA school official exception means no commercial use of student information, and state that contracts are required. In addition, publishers should not be able to rely on “consent” as an avenue for additional commercial use of student information. They should be required to act as FERPA school officials, acting at the direction and control of the school, even if purporting to get separate student consent. And, FERPA could require reasonable security safeguards—and ideally provide some funding to help train and support institutions in this endeavor.

#### **c) Stronger Consumer Privacy Laws.**

Lastly, while education focused laws would be most effective, stronger consumer privacy laws that do not rely on a notice and choice model, but focus on data minimization and limiting the use of data for the purposes for which people provide it—in the educational context, in order to provide an education, not to target advertising or create commercial profiling, for example—would help improve the overall landscape and improve the educational ecosystem.

#### **d) Effective Enforcement**

Laws are only as effective as their enforcement. Any updates to laws would ideally be matched by enhancement of enforcement powers. Despite being in effect for a decade, SOPIPA has not resulted in any public enforcement actions, and FERPA is widely recognized as underenforced.

---

<sup>92</sup> California does not have carve outs, but other state student privacy laws sometimes have “consent” exceptions.

## 2. Target Key Institutional and Corporate Actors To Change Policies

In California, nearly 80% of students attend a public institution—the University of California, California State, or California Community College systems.<sup>93</sup> At a system level, these bodies are positioned to influence change that will flow down to their institutions. Standardization could put institutions on the same page, so master contracts with publishers are more consistent. Bodies like the Community College League of California could develop model contracts and contracting processes for ed tech publishers (as consortiums in the K-12 space have done) with respect to student information. These model contracts could limit use of students’ personal information to educational purposes and limit data retention of students’ personal information. They could require reasonable security. Contracts could be posted and shared. Institutions acting as part of a larger system will have improved bargaining power over publishers. Faculty members who may be motivated to decrease costs for students and choose open source materials may also find that they are limiting commercial surveillance of those students, and such a shift could be more broadly encouraged by highlighting to faculty the importance of safeguarding students’ information.

There are additional gatekeepers that could play an outsize role in improving the landscape as well. Institutional bookstores could require privacy protective contracts before offering digital publications to students. Alternatively, LMS—which themselves typically have contracts with institutions—could require a contract from the digital textbook provider—and require that contract to be privacy protective—before enabling a digital publisher to connect to its system.<sup>94</sup> Courseware publishers with better privacy practices could promote their services on this basis and demand better of their competitors. There is also the possibility that technology gatekeepers could build privacy protections into their systems, for example anonymizing data before it is shared with any external ed tech applications including publishers.<sup>95</sup>

## 3. Raise Awareness and Build Grassroots Support

Change could also occur from the ground up. Individual institutions could require publishers to act as FERPA school officials, prohibit them from using information for commercial purposes by contract, or publicly be more transparent with students.

---

<sup>93</sup>Cook, K. (2024, Jan.) California’s Higher Education System. Public Policy Institute of California. <https://www.ppic.org/publication/californias-higher-education-system/>

<sup>94</sup> While it seems typical for institutions to have policies with LMS, based on record requests to institutions, these policies may not be visible to students based on student authors’ experience, and it is unclear what policies and LMS has with publishers themselves

<sup>95</sup> See, e.g., Willlo (<https://www.willolabs.com/>). Willlo –which appears to be more widely adopted thus far in Canada, a country with stricter privacy rules—and bills itself as a privacy-preserving solution that links digital materials together (sometimes hundreds) and then integrates into an LMS. As explained by Willlo, Willlo creates anonymized and non-algorithmic credentials for individual users, and enables the institution to see the student matched with any progress or grades while sending to the hundreds of publishers or courseware providers anonymous information. This will limit the potential for data breaches if any of those hundreds of integrated publishers are hacked, and will also prevent students from getting marketing emails directly from publishers. Willlo can negotiate contracts with publishers, and may also contract with the bookstore or the institution. McKain, K. Interview, May 20, 2024.

In order for this to happen without top down directives, administrators and individual instructors who select digital publications could receive training on privacy, best practices, and the digital ecosystem that supports modern day learning. Raising general awareness about data collection practices, and privacy and security best practices, may assist instructors and institutions when choosing between learning offerings. Individual faculty champions within institutions can be very effective in changing faculty opinions. In addition, institutions could be more transparent with students.

For example, under law,<sup>96</sup> institutions are obligated to disclose the cost of required instructional materials to the extent practicable—institutions could also disclose the privacy practices of instructional materials. More awareness at the faculty and student level could ultimately lead to changed institutional policies.

Awareness campaigns and training would require financial support and funding. Lawmakers could pass budgets to expand technological expertise at the federal and California Department of Education, which could provide more support and guidance to institutions. Support could also be provided for civil society organizations to provide increased training and awareness to institutions.

## **C. Conclusion**

More and more students are using courseware on a daily basis. They and their instructors make use of such learning tools without full awareness or understanding of what this means for student privacy. Right now, whether a student's privacy is protected seems largely left to chance. Luckily, there are many paths forward to improve the courseware experience for students and institutions, and to better protect higher education students' privacy.

---

<sup>96</sup> Higher Education Opportunity Act of 2008, 20 U.S.C. § 1001 et seq.