Sci Eng Ethics (2016) 22:1473–1496
DOI 10.1007/s11948-015-9692-7

ORIGINAL PAPER

Users or Students? Privacy in University MOOCS

Meg Leta Jones[1] · **Lucas Regner**[1,2]

Received: 16 March 2015 / Accepted: 10 August 2015 / Published online: 19 August 2015

Abstract Two terms, student privacy and Massive Open Online Courses, have received a significant amount of attention recently. Both represent interesting sites of change in entrenched structures, one educational and one legal. MOOCs represent something college courses have never been able to provide: universal access. Universities not wanting to miss the MOOC wave have started to build MOOC courses and integrate them into the university system in various ways. However, the design and scale of university MOOCs create tension for privacy laws intended to regulate information practices exercised by educational institutions. Are MOOCs part of the educational institutions these laws and policies aim to regulate? Are MOOC users students whose data are protected by aforementioned laws and policies? Many university researchers and faculty members are asked to participate as designers and instructors in MOOCs but may not know how to approach the issues proposed. While recent scholarship has addressed the disruptive nature of MOOCs, student privacy generally, and data privacy in the K-12 system, we provide an in-depth description and analysis of the MOOC phenomenon and the privacy laws and policies that guide and regulate educational institutions today. We offer privacy case studies of three major MOOC providers active in the market today to reveal inconsistencies among MOOC platform and the level and type of legal uncertainty surrounding them. Finally, we provide a list of organizational questions to pose internally to navigate the uncertainty presented to university MOOC teams.

Keywords Privacy · University research · Technology policy · Higher education · Education law

✉ Meg Leta Jones
ma1318@georgetown.edu

[1] Communication, Culture and Technology Department, Georgetown University, 3520 Prospect NW, Suite 311, Washington, DC 20057, USA

[2] American University, Washington, DC, USA

Introduction

Technology in higher education currently seems to exist in the large shadows cast by expectations of massive open online courses (MOOCs). By breaking down logistical walls like limited seats and rising tuition fees, universities can gain certain benefits. But it is not yet clear what those benefits might be, and what might be given up in their pursuit. Although MOOCs are generally geared toward an adult learner population, the POLITICO article "Data Mining Your Children" sums up the reasons why some worry about the big data trend and MOOCs in higher education:

> The [National Security Agency] has nothing on the ed tech startup known as Knewton. The data analytics firm has peered into the brains of more than 4 million students across the country. By monitoring every mouse click, every keystroke, every split-second hesitation as children work through digital textbooks, Knewton is able to find out not just what individual kids know, but how they think. It can tell who has trouble focusing on science before lunch — and who will struggle with fractions next Thursday (Simon 2014).

The structure and scale of university MOOCs create tension for privacy laws intended to regulate information practices exercised by educational institutions. MOOCs offered through universities give users anywhere exposure to costly quality lectures and exams for free. While MOOCs exemplify innovative and disruptive teaching and learning technologies, academic institutions will need to address many issues in short order, including privacy issues raised by the data collected with, shared by, and processed through MOOCs. It is this "big data" that offers the most value to universities, promising better administrative decisions about how resources are allocated and increased understanding into the way in which people learn. However, MOOC students that provide this valuable data may not receive the privacy protections extended to traditional tuition-paying university students.

The issue of consumer protection in the context of digital classrooms offered by universities has garnered the attention of the White House. In a press release from January 12, 2015, President Obama outlined the executive office's strategy to "[Safeguard] Student Data in the Classroom and Beyond":

> The President is releasing a new legislative proposal designed to provide teachers and parents the confidence they need to enhance teaching and learning with the best technologies – by ensuring that data collected in the educational context is used only for educational purposes. This bill … would prevent companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school … (The White House 2015).

In order to understand how relevant education and privacy laws may protect a user's privacy in educational contexts or regulate MOOCs and big data in higher education, it becomes important to understand the phenomenon to which the privacy legislation might apply. The first section of the article discusses what a MOOC is,

how it relates to other types of education, what type of data MOOCs create, and the current state of MOOCs in the US, focusing on those offered by accredited universities. Next, the article introduces the reader to privacy in education by analyzing the laws and policies related to user data in university MOOCs: Fair Information Privacy Practices (FIPPS), the Family Educational Rights and Privacy Act (FERPA), and new state laws aimed at regulating MOOCs. The third section of this article focuses on three case studies of MOOC platforms. It includes a description of the structures of the relationships between universities and the three MOOC providers we analyzed: Coursera, EdX, and Blackboard CourseSites. We explore data policies and practices for each and discover that a variety of for-profit, non-profit, public, and private institutions are involved, which creates even greater complexity for applicable privacy protections. The case studies reveal a deep level of variation and uncertainty surrounding MOOC user data as student data. The fourth section provides a list of internal discussion points to guide university MOOC faculty and staff toward developing courses, systems, and partnerships that fit their vision of MOOCs. We do not argue a normative solution but intend to firmly and precisely lay out areas of uncertainty surrounding university MOOCs in relation to privacy so as to provide the tools for MOOC researchers and technologists to navigate the issues within their intention for the platform, as these teams will be instrumental in shaping the future of education and student privacy.

MOOCs

MOOCs are, in essence, a combination of electronically delivered video and audio lectures, text documents, and assignments graded automatically by a computer or by peers enrolled in the same course. The material is structured according to a traditional syllabus and is accessible to students online. Because of this core structure, there are no institutional or pedagogical limits to the number of students that can enroll in any given course. Another characteristic of MOOCs is that they are taught with "minimal involvement by professors" (What You Need To Know About MOOCs 2014). Adamopoulos (2013) wrote that the idea of MOOCs had been conceived of already in the early 1960s, at that time described as an "industrial scale educational technology" (p. 2).

Like so many movements in education, the modern-day MOOC was born out of a single classroom experiment. In 2008, Professors George Siemens and Stephen Downes were teaching a course on connectivism in learning (called CCK08) and found it illustrative of the subject matter to open the course beyond those physically attending to thousands of students online. The course was a success with a physical enrollment of twenty-four students and virtual enrollment of 2200 (Downes 2009). A novel concept, suitable simply for a specific class, was given a name (Cormier 2008) and the ability to be replicated. In 2012, Stanford University opened three of its classes, most notably CS 221—Introduction to Artificial Intelligence, to any student interested, free of cost, via the web. Stanford's offering differed in two important respects from the original MOOC. Whereas CCK08 did not collect assignments from virtual students, CS 221 maintained strict deadlines for weekly

assignments, a midterm and a final, and which were graded for all students. Additionally, Stanford intentionally chose an already popular course, taught by well-known professors, and marketed the course heavily resulting in an enrollment exceeding 160,000 students (Leckart 2012).

Today, both the number of MOOCs (the courses themselves) and MOOC platforms (the organizations that host and offer the MOOC courses) have proliferated, and multiple actors connected specifically with accredited universities have emerged: three of the major ones being the EdX consortium, Coursera, and Blackboard's CourseSites. Today's MOOCs have a global reach. Nesterko et al. (2013) reported "MOOC students came from 194 countries," and an analysis conducted by the same authors on students registered for HarvardX's[1] MOOCs showed three main characteristics of MOOC students as of September 2013:

1. 42 % of registrants were from the United States, representing the largest population enrolled, however, countries from all continents were represented in the top ten (with India on second place and Canada on third) (Nesterko et al. 2013: p. 2);
2. Men were overrepresented worldwide, constituting an estimated 63.4 % of all registrants. (Nesterko et al. 2013: p. 4);
3. There is a large discrepancy between registration for a course and obtaining a certificate of completion: in relation to registrants from each country, only 3.7 % of registered US MOOC students earned a certificate at the end of the course, indicating completion. European MOOC students, however, had a much higher level of completion, with for example 12 % of all Greek and Spanish students. In this regard, MOOCs differ considerably from traditional university courses.

Formal Versus Non-formal Education

Notice the language used to distinguish students in this Article: MOOC users or MOOC students. The distinction relates to the concept of formal versus non-formal education, defined as:

> Formal education is highly institutionalized, bureaucratic, curriculum driven, and formally recognized with grades, diplomas, or certificates … the term non-formal has been used most often to describe organized learning outside of the formal education system. These offerings tend to be short-term, voluntary, and have few if any prerequisites. However they typically have a curriculum and often a facilitator (Merriam et al. 2007: pp. 29–30).

MOOCs and their predecessors have traditionally fallen into the category of non-formal education. They are organized and dressed up as formal education, but lack components of recognition in the formal higher education bureaucracy. However,

[1] "HarvardX" is Harvard University's MOOC brand name. All the EdX Consortium members adopt the "X" to denote their EdX MOOC offerings, for example Georgetown University (GeorgetownX).

this state of affairs is challenged on several fronts. As discussed below, the state legislatures of Florida and California have both introduced bills that suggest that certain MOOCs should yield credits that may count towards a higher education degree. For purposes of this Article, we chose to define a university MOOC as (1) a free educational course—(2) delivered entirely online—which is (3) designed and taught by professors at accredited universities yet (4) not necessarily part of a degree program or resulting in credits that can be counted towards a degree. Our definition effectively excludes platforms like Khan Academy (Noer 2012), Code Academy, and other actors within the realm of informal learning and education.

Two states' legislative bodies have looked into incorporating MOOCs into the formal, credit-yielding curriculum: California (SB-520, 2013) and Florida (H.B. 7029, 2013). The California bill was later dropped (Gardner and Young 2013; Young 2013) as the California public higher education system responded quickly by expanding its online course offering. In Florida, however, a version of the original bill became law in 2013, although implementation remains unclear (Inside Higher Ed 2013). Completion of a MOOC course can generally not be counted towards a degree, although higher education representatives like Cathy Sandeen of the American Council on Education (ACE) has publicly discussed such an option (Sandeen 2013). In 2013, ACE recommended five MOOCs for credits, but it remains up to the universities themselves to decide whether they accept the credits or not (Kolowich 2013c). ACE's recommendations, coupled with some states efforts to include MOOCs in the formal education system, might constitute a game change in terms of whether MOOC students should be treated with same privilege as traditional students in regards to student privacy.

MOOC Data

"Only 2.6 % of higher education institutions currently have a MOOC, another 9.4 % report MOOCs are in the planning stages," reported Allen and Seaman (2013: p. 3) in the online education Sloan-C consortium's report *Changing Course: Ten Years of Tracking Online Education in the United States*. This shows that only a few institutions are involved in creating and offering MOOC courses, with 55 % of institutions reporting that they are still unsure whether they will offer MOOCs in the future and 33 % explicitly stating they will not. The report also states that "academic leaders… do have concerns that credentials for MOOC completion will cause confusion about higher education degrees" (Allen and Seaman 2013: p. 3).

Universities that offer MOOCs are still debating why they should expend resources on creating free, high-quality educational materials. For instance, Allen and Seaman (2013) reported that "academic leaders remain unconvinced that MOOCs represent a sustainable method for offering online courses, but do believe they provide an important means for institutions to learn about online pedagogy" (p. 3). The potential of MOOCs are the aggregated data that MOOC students leave behind when interfacing with the courses, promising new insights into learning and decision-making support in institutional matters. For example, researchers have experimented with MOOC data to create models that can help predict anything from student retention (Adamopoulos 2013) to developing algorithms for peer-grading

corrections (Piech et al. 2013). The promise of the "MOOC big data" might, in the end, be the return that makes the universities' investments worthwhile.

Introduction to Education Privacy

In light of innovative technological initiatives in education like MOOCs, education privacy concerns have been loudly raised in the last 3 years, gaining political interest, funding opportunities, and rich scholarship. The Berkman Center for Internet & Society has published a series of articles as part of its Student Privacy Initiative including a number of white papers (Berkman 2015). The Future of Privacy Forum has also done significant work in the area of student privacy, creating a Student Privacy Pledge, conducted surveys with parents, and published a number of policy papers (Future of Privacy Forum 2015). The International Review of Information Ethics has published an entire volume dedicated to "The Digital Future of Education (Britz and Zimmer 2014). These authors have made significant headway in describing and analyzing the high level debates surrounding new education technology and privacy concerns, focusing mostly on the K-12 systems. We chose to look at the privacy concerns in MOOC systems, because they have been largely overlooked and many researchers and faculty members are regularly exposed to fast-moving MOOC initiatives without guidance on privacy or data protection issues. We also chose to look at MOOCs as in-depth case studies, as opposed to considering them in generalities, to be able to show specific examples and precise locations where uncertainty and inconsistently exist.

Like many open platforms made possible in the Digital Age, MOOCs place strains on legal categories by creating activities that exist in between well established legal domains. It is difficult to determine how existing legal protections will or should apply to emerging technologies and their uses in order to protect threatened values like autonomy and privacy. This section analyzes privacy protections relevant to university MOOCs and is followed by three case studies of existing MOOC systems that reveal a great deal of uncertainty represented by varied treatment privacy and user data. While many legal issues arise with MOOCs including intellectual property rights and contract issues, we focus on the overlooked issues related to the use and abuse of personal information. These issues are particularly relevant as our society continues to develop new ways of understanding personal data and its relationship to innovation in a rapidly changing technological landscape. This section begins with the concepts that underlie student privacy, and deals with particular principles, federal legislation, and state legislation that may regulate MOOCs in the sub-sections that follow.

"The notion that certain aspects of a person's life should be [free] from public scrutiny, or at least be subject to only limited scrutiny underlies the concept of privacy. An interest in privacy becomes even more vital when scrutiny of a person's life results in records compiled and retained by public entities, such as school districts. When records are kept by school districts, the immediate question is who will have access to those records," explained Mawdsley and Russo (2002). This is why the Family Education Rights and Privacy Act (FERPA) was passed in 1974—to

prevent schools from abusing student privacy (20 USC § 1232(g) and 34 CFR part 99). At the time, a number of studies showed that parents, to a large extent, were granted less access to their children's complete school records than authorities like the law enforcement agencies and health departments. Additionally, it sought to deal with the widespread practice of collecting survey information from students without parental knowledge or oversight. Survey questions included in the Congressional Record of the Senate adoption of FERPA read "Would you like to run away from home?" and "Do your parents say they don't love you or warn you that they will stop loving you?" (O'Donnell 2003).

Although there is little legislative history to guide practice or interpretation (Johnson 1993), Senator Buckley, who introduced the FERPA, gave a speech to the Legislative Conference of the National Congress of Parents and Teachers explaining his motivation:

> [M]y initiation of this legislation rests on my belief that the protection of individual privacy is essential to the continued existence of a free society. There has been clear evidence of frequent, even systematic violations of the privacy of students and parents by the schools through the unauthorized collection of sensitive personal information and the unauthorized, inappropriate release of personal data to various individuals and organizations. In addition, the growth and use of computer data banks on students and individuals in general has threatened to tear away most of the few remaining veils guarding personal privacy, and to place enormous, dangerous power in the hands of the government, as well as private organizations (O'Donnell 2003).

The pendulum has since swung the other direction; schools have recently been criticized for being too heavy handed with FERPA, taking advantage of its broad language to avoid disclosing information to the public. Law professor Mary Margaret Penrose argued, "For years, schools have been hiding behind FERPA and intentionally preventing disclosure of records to third parties" (Penrose 2012). This opaqueness occurs at the same time as data collection increases in granularity and reveals far more about students than it did decades ago. However, the promises of big data in education rely on large, shared data sets, third party applications, and data generated off school grounds. In order to move forward with better administrative decisions and learning analytics, existing privacy issues must be addressed. While FERPA is most relevant to university MOOCs, fundamental data protection principles and new MOOC-specific state regulations are also important to understanding where MOOCs fit in the increasingly unstable policy landscape that is student privacy, which we explore in detail in the sub-sections below.

Fair Information Practices Principles

The United States takes what is called a secular approach to privacy, meaning that unlike the horizontal approach taken by the European Union and national regulations based on its model, the US does not have a universal set of data protection laws. Instead, American law addresses privacy concerns in specific

arenas dealing with specific concerns like health (e.g., the Health Insurance Portability and Accountability Act), government intrusion (e.g., the Fourth Amendment), and children's data (e.g., Children's Online Privacy Protection Act). However, the US does utilize the Fair Information Practices Principles (FIPPs) to guide general data protection, whether enshrined in state law, industry self-governance, or internal corporate ethics.

All those engaging in modern big data practices share many of the privacy issues facing MOOCs and are encouraged to utilize the FIPPs to guide their information practices. There are a number of different versions of FIPPs; the Consumer Privacy Bill of Rights is a recent example (The White House 2012). The following is a list of FIPPs from the Consumer Privacy Bill of Rights applied to contexts of university MOOCs. The principles help us analyze where university MOOCs may have problems meeting basic privacy expectations.

1. Individual control: Users should be able to exercise control over what personal data MOOCs collect from them and how the MOOCs use it. Terms of service are notoriously unread and incomprehensible (Solove 2013). Popular web platforms like Google and Facebook provide users with tools to control, in limited fashion, their data. However, in the MOOC context, this may mean a data dashboard for MOOC students, for the MOOC to gain extra permissions (e.g., click through opt-in) for additional data collection or use, or provide a level of control over data that has been shared.
2. Transparency: Users should be presented with easily understandable and accessible information about privacy details and security practices. No matter how much care is taken with MOOC terms of service and privacy policies, it will be difficult to explain complex and unforeseen data practices.
3. Respect for context: Users should be able to expect that MOOCs will collect, use, and disclose personal data in ways that are consistent with the context in which users provide the data. Excitement surrounding MOOCs is rooted in its potential to inform education and learning through data sharing, but MOOC data will be valuable outside of the initial institution and education context as well, such as marketing services in a variety of fields such a consumer products, political campaigns, and media outlets.
4. Security: User data should be handled in a secure and responsible manner. MOOC initiatives often involve a large number of faculty, staff, and student assistants and security measures can be lost in the shuffle, particularly because of the seemingly low risk associated with data.
5. Access and accuracy: Users should be able to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to the user if the data is inaccurate. The stakes are relatively low in MOOCs (compared to social service benefits or credit scoring for instance), but MOOC teams and platforms may not be prepared to offer MOOC students their data in a fashion that allows them understand and correct their data.
6. Focused collection: Users should expect reasonable limits on the personal data that MOOCs collect and retain. This is one of the principles that MOOC teams

may find particularly challenging. The data that provide insights into learning and educational success are not always confined to data created in an educational setting. There is a great deal of unexpected correlation in the big data realm, which motivates designers and researchers to collect as much as possible and combine datasets. Question we must ask is "from the MOOC students' perspective, is this collection practice reasonable given the context?"

7. Accountability: Users should have personal data handled by MOOCs with appropriate measures in place to assure they adhere to these principles. Oversight and leadership should be in place within MOOC systems so that the MOOC provider, faculty, and student assistants involved are accountable to the established principles and aware of whom to seek out when questions arise. However, because of the pace at which MOOCs are moving and uncertainty regarding their future, these systems of accountability are to date not transparent to the MOOC student.

The challenges of complying with the FIPPs that all big data initiatives are also faced by MOOCs, but additional privacy concerns place another layer of challenges on university MOOCs.

FERPA

As MOOCs challenge broad fundamental privacy protections, it may be tempting to simply categorize them with other web applications that do the same. But MOOCs are in the education space, and they may be held to a higher standard than most other web service providers out there. The Family Educational Rights and Privacy Act (FERPA) regulates how educational institutions treat *student* data. FERPA has been amended repeatedly since 1974; it was changed in 1979, 1986, 1990, 1992, 1994, 1998, 2000, 2008, and 2011, as well as affected by other laws like the USA PATRIOT Act of 2001. Today its provisions include the following relevant sections. FERPA requires schools to grant parents and eligible students (18 or in postsecondary institutions[2]) four basic rights:

1. to control disclosure of their educational records;
2. to inspect and review their educational records;
3. to request amendment of their educational records; and
4. to file a complaint with the US Department of Education regarding alleged FERPA violations.

FERPA applies to educational agencies and institutions, which are defined as any public or private agency or institution that provides educational services and is the recipient of federal funds under any applicable program [Section 1232 g(a)(3)]. Virtually every primary and secondary school, college, and university receives

[2] FERPA rights transfer from the parent to the student, when a student turns 18 *or* enters a postsecondary institution (Department of Education n.d.).

federal financial support (e.g., federal student loans) and is therefore subject to FERPA (Daggett 2008).

FERPA applies to the policies of these educational institutions, as opposed to instances of mismanaged information. Educational institutions must have in place "policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information…) of students"[3] (34 C.F.R. § 99.3). FERPA coverage is limited to education records, defined as "those records, files, documents, and other materials which (I) contain information directly related to a student; and (II) are maintained by an educational agency or institution or by a person acting for such agency or institution" [§ 1232(a)(4)(A)]. Educational institutions cannot disclose individually identifiable information (more commonly referred to as personally identifiable information, "PII") without written consent, with numerous exceptions. PII includes a student's name, her parents' names and family members, home address, identifiers like social security numbers, student numbers, date of birth, biometrics (any biological or behavioral record that can be used for automated recognition—e.g., fingerprints, DNA, facial characteristics, handwriting), and…

> … 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] 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 (34 CFR § 99.3).

The exceptions to the disclosure prohibition are particularly relevant as more and more educational efforts involve integrating networked technologies and services in attempts to provide personalized learning targeted at individual students. A postsecondary institution may disclose PII from the education records without obtaining prior written consent of the student including:

1. *To other school officials*, including teachers, within the [School] *whom the school has determined to have legitimate educational interests*. This *includes contractors*, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in § 99.31(a)(1)(i)(B)(1)—(a)(1)(i)(B)(2) are met [§ 99.31(a)(1)],
2. To officials of another school *where the student seeks or intends to enroll*, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of § 99.34 [§ 99.31(a)(2)].

[3] See also Carey v. Me. Admin. Sch. Dist. 17, 754 F. Supp. 906, 923-24 (D. Me. 1990) (involving a claim that the school violated FERPA by providing the media with confidential information about an "unnamed" special education student who brought an automatic weapon to school).

3. To authorized government representatives[4] (§§ 99.31(a)(3) and 99.35),
4. In connection with *financial aid* [§ 99.31(a)(4)],
5. To *organizations conducting studies for, or on behalf of, the school*, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction [§ 99.31(a)(6)].
6. To parents of an eligible student if the student is a dependent for IRS tax purposes [§ 99.31(a)(8)].
7. To comply with a judicial order or lawfully issued *subpoena* [§ 99.31(a)(9)],
8. Information the school has designated as "directory information" [§ 99.31(a)(11)].

For the purposes of big data education efforts, FERPA does not prevent the disclosure of aggregate data and statistics as long as student identities' are not "easily traceable," or of individually identifiable information to contractors that fall within the school official exception, as well as organizations performing education research. However, exceptions that allow for the disclosure of PII for non-educational purposes often create privacy concerns for the user that should also be considered (e.g., disclosure in response to a subpoena that may reveal information relevant to a civil suit).

FERPA is enforced by the Department of Education's Family Policy Compliance Office (FPCO), which investigates complaints but does not otherwise monitor educational institutions for violations. FPCO is authorized only to pursue voluntary compliance through the withholding of federal assistance payments. Additionally, most states provide legal recourse to seek compensation for those harmed by the unauthorized disclosure of private education records (Toglia 2007). While 80 % of complaints filed are resolved informally (Fischer et al. 1995), FERPA litigation does occur and provides additional insight into the scope and strength of the legislation. Because only the Department of Education can enforce a FERPA claim related to wrongful disclosure (meaning a student cannot sue the university directly for such a violation), FERPA's privacy protections are understood as a tool for governing educational institutions through resource allocation.

MOOCs challenge FERPA's application to universities in a number of ways including placing a strain on the definitions of educational institutions, eligible students, education records, and third party disclosure and access to information. However, because of its limited legislative history, courts have been divided about whether FERPA is intended to protect student rights or prevent institutional abuses (Blanchard 2007).

The first question is whether FERPA applies to MOOCs, which requires us to look at whether the MOOC relationship with the university qualifies as an educational institution and whether MOOC students are eligible students. The second question is which relevant FERPA exceptions apply to MOOCs.

[4] Including the US Comptroller General, the US Attorney General, the US Secretary of Education, or State and local educational authorities, such as a State postsecondary authority that is responsible for supervising the university's State-supported education programs.

Eligible Students

Generally, universities are educational institutions, because they receive federal money in one way or another. A great deal of data collected on MOOCs would qualify as an educational record because it is directly related to a student (assuming for the moment that MOOC students are students) and maintained by an educational agency or institution (the university) or by a party acting for the agency or institution (the MOOC organization or university project team). The exception to this section relates to records such as those created by the law enforcement unit of the educational institution, physician records, employee records, peer graded papers before they are turned in, none of which are relevant to our discussion on MOOC privacy.

The most important question is then whether MOOC students are "eligible students" under FERPA. "*Eligible student* means a student who has reached eighteen years of age or is attending an institution of postsecondary education." (§ 99.3) Attending is the key term in this definition. "Attendance" includes but is not limited to "in person or by paper correspondence, videoconference, satellite, Internet, or other electronic information and telecommunications technologies for students who are not physically present in the classroom." (§ 99.3) Online learning is clearly protected by FERPA. While MOOCs may be viewed as university public outreach, the Federal Register entry explaining the 2008 amendment on attendance that addressed the integration of technology in modern learning environments is problematic: "We do not agree that the definition of attendance should be limited to receipt of instruction leading to a diploma or certificate, because this would improperly exclude many instructional formats" (Department of Education 2008). Whether MOOCs fall into the type of instructional formats the Department of Education seeks to cover is unclear. In order to disclose personally identifiable student education records, educational institutions and school officials (discussed below) must acquire written, signed consent that specified the records to be disclosed, the purpose of the disclosure, and the parties to whom the disclosure is made [§ 99.30(a, b)]. Consent may be procured electronically, as long as it is sufficiently authenticated [§ 99.30(d)].

School Officials

Although university credit for MOOC completion creates a moving target for the definition of an eligible student, we will discuss third party disclosures based on the possible direction and structure of MOOCs in the future. Disclosure to third parties is the most uncertain aspect of FERPA, but analogies can be drawn from the Department of Education's communications on the use of cloud services. Storing student information in the cloud is permitted as long as certain measures are taken to keep the information secure and private. This falls under the exception for school officials to the general rule that students/parents must consent before education records are disclosed to another party; contractors must often be used to perform functions that the school would otherwise use an employee or its own resources to perform. The exception requires contractors to access only those student records for

which they have a legitimate educational interest in accessing, and the school has to set up proper technological and administrative controls to prevent unauthorized access. Specifically:

1. The school must directly control the contractor's use and maintenance of education records;
2. The contract must be for services or functions the school would have otherwise used its employees to perform;
3. The contractor must be published in the school's annual FERPA notification of rights and meet the criteria for "school officials with legitimate educational interests"; and
4. The contractor must be subject to FERPA use and re-disclosure limitations (the university, its officials, and contractors all must adhere to FERPA, and the contractor may further be limited by the purposes outlined in the contract).

The contractor cannot use FERPA protected information to develop products and services not intended for use by the school, but may engage in such development to improve the products the school was using or intended to use.

Therefore, if MOOCs were to be deemed online instruction and MOOC students were to be deemed students according to FERPA's definition, third party disclosures of personally identifiable information would need to be restricted and narrowed all the way down the line (whether it be the initial MOOC, analytics vendors, media platforms used within MOOCs like YouTube, etc.). MOOCs may fall outside of the scope of FERPA until MOOCs begin to offer more formalized credit, a federal loan arrangement is created for payment systems that may exist in the future, or MOOC organizations receive federal funds through grants or other means. However, MOOCs incorporated into the formal higher education realm (outlined below) may already be sufficiently integrated as to require compliance with FERPA. On a final note, data generated by MOOCs must meet the minimum legal requirements for general online services where they apply, such as Children's Online Privacy Protection (COPPA), Institutional Review Boards (IRBs), and security standards.[5]

[5] This includes a number of other regulations and restrictions. The Children's Online Privacy Protection Act (COPPA) applies only to commercial entities—not non-profits or schools. MOOCs challenge these distinctions. While MOOC organizations may be non-profits or provided directly by the school, some MOOC providers are commercial entities. COPPA also only applies to sites that collect data from users with actual knowledge the user is under 13 or target children under 13. COPPA requires these MOOCs obtain verifiable parental consent prior to the collection of personal information from children under 13, as well as disclose to parents the information collected, provide a right to revoke consent and deletion, and provide a detailed privacy policy. The FTC recently released an FAQ on COPPA providing more insight into the school exception (Federal Trade Commission 2014). The Protection of Pupil Rights Act (PPRA) grants rights to parents to gain access to federally funded experimental instructional material as a way to address the unsettling circumstances when schools administered sensitive surveys to students without parent knowledge. However, 60 Fed. Reg. 4696-01 (Aug. 28, 1995) explains that PPRA differs from FERPA in that the latter applies to postsecondary institutions whereas the former only applies to K-12 settings. See Daggett (2008). Student Privacy and the Protection of Pupil Rights Act as Amended by No Child Left Behind. UC Davis J. Juv. L. & Pol'y, 12, 51; O'Donnell (2003). FERPA: Only a piece of the privacy puzzle. JC & UL, 29, 679. A 1998 case filed by a law student claiming that the law school's disciplinary decision requiring him to undergo psychiatric treatment violated PPRA moved forward as if the PPRA *did* apply to postsecondary institutions. The court eventually determined that psychiatric

MOOC State Laws

While the current MOOC models in place (discussed more fully in Section III) may or may not extend FERPA protection to MOOC users as eligible students, the models are also changing based on the market, data from MOOCs, and pressure on universities—all which have led to state legislatures in rare, but likely more frequent in the future, instances addressing MOOCs. Florida passed a law in June 2013, that requires the Florida Board of Governors and the State Board of Education to "adopt rules that enable students to earn academic credit for online courses, including massive open online courses, prior to initial enrollment at a postsecondary institution" (H.B. 7029, 2013). Almost a year later, neither Board has provided much in the way of guidance as to how the law should be interpreted or implemented (Straumsheim 2014).

California Senate Bill 520 would have compelled universities in the state to accept credits for low-level, high-demand classes students earned through MOOCs (SB-520). The bill was shelved in August 2013, when the California State University system moved to provide more online offerings to meet the demand for these courses, and the issue of MOOC credit was set to be reexamined (Kolowich 2013b). As of July 2013, no MOOC students had sought to redeem coursework on edX, Coursera, or Udacity for university credit.[6]

Neither of these laws addresses user privacy but both speak to the legitimacy of MOOCs as extensions of university-provided education. If universities must accept credits earned in MOOCs, it does not necessarily follow that user data from that MOOC must be treated as student data according to FERPA, but it does suggest that the universities' MOOC data is attributed to an "eligible student" in the state where such a law exists. The MOOC platform could easily be considered a contractor for providing a service that university employees otherwise would have provided to the student, and thereby need to comply with FERPA regulations.

Footnote 5 continued
treatment was not administered by the Department of Education and therefore beyond the scope of PPRA. A 2001 PPRA claim filed by a medical student was dismissed for procedural errors related to the appeal, and the court again did not discuss the applicability of PPRA to higher education. Finally, whether university researchers need to obtain approval from their institutions internal review board (IRB) is handled within the university and many IRBs offer clear guidance on academic assessment data. Many universities have datasets available on their students for research purposes, which can muddle whether approval is need for the use of data collected through university courses. By way of example, the Virginia Tech academic assessment research page informs researchers that before collecting data from enrolled students researchers should consider whether they intend to disseminate findings in ways other than to provide feedback to students, improve a course or program, or report finding to university administration or accrediting agencies. If the researcher intends to disseminate findings beyond these recipients, IRB approval should be sought (Virginia Tech IRB 2015). In addition, because MOOC student records may not be educational records for the education institution, researchers may be considered collecting data on human subjects in the general public and should be get cleared by their IRB.

[6] Credit for completed MOOC course was offered by Colorado State, but no one has taken the university up on its price reduced ($89 vs. $1050) credits) (Kolowich 2013a).

MOOC Platforms and User Data

A look at the various privacy policies and practices in place shed light on the lack of uniformity on the subject of university MOOC privacy. Case studies of Coursera, EdX, and Blackboard's CourseSites MOOCs were undertaken to determine the way in which each treats certain information: age restrictions, trackers, personal information collection and disclosures, data access and correction, and security. The MOOCs' terms of service and privacy policies were analyzed. The Ghostery extension was used to detect the number and source of trackers on certain pages. Finally, we registered for courses on each MOOC to determine age restrictions and trackers used within the actual course space.

The Platform: University Relationships

The relationship between accredited higher education institutions and the MOOC platforms becomes important when analyzing the legal implications for MOOC students' privacy. Each of the platforms assessed below have a different relationship with associated universities.

Coursera is a for-profit organization that refers to the universities, government agencies, and NGOs who offer courses on the platform as "partners," constituting over one hundred organizations to date. As part of their business model, they offer special certification, proctoring services, and tutoring for a charge (Young 2012). Coursera's relationship with the university is defined as follows:

> You agree and acknowledge that nothing in these Terms of Use or otherwise with respect to your access or use of any Online Course or Site (a) establishes any relationship between you and any university or other educational institution with which Coursera may be affiliated, (b) enrolls or registers you in any university or other educational institution, or in any course offered by any university or other educational institution, or (c) entitles you to access or use the resources of any university or other educational institution beyond the Online Courses provided by the Sites.

EdX, on the other hand, is a non-profit consortium of Universities, NGOs, and private businesses founded by MIT and Harvard University, headquartered in Cambridge, Massachusetts. All xConsortium members, over thirty organizations to date, take part in governing EdX. Each xConsortium member gets access to its own courses' data, with the option to share with other xConsortium members. In its terms of service, EdX explains:

> When you take a course through edX, you will not be an applicant for admission to, or enrolled in, any degree program of the X University as a result of registering for or completing a course provided by such X University through edX. You will not be entitled to use any of the resources of the X University beyond the online courses provided on the Site, nor will you be

> eligible to receive student privileges or benefits provided to students enrolled in degree programs of the X University.[7]

Blackboard's CourseSite is a publicly listed company that allows anyone to use their MOOC platform to teach courses. However, in 2013, Blackboard reported that twenty-six higher education institutions would formally offer MOOCs through their platform, although any institutions using the Blackboard's learning management system will have access to it (Sheridan 2013). This means that institutions using the learning management system Blackboard will automatically be able to offer MOOCs through Blackboard's CourseSite. However, there is no formal number of MOOCs offered through Blackboard CourseSites, and university affiliated professors could offer courses through Blackboard's CourseSites without the support of their university, creating the possibility for "rogue MOOCs" alongside "university MOOCs".

However, Blackboard has an established relationship with the universities it provides the MOOC platform for, and privacy practices are established as a vendor for purposes of FERPA. The company has, to this point, been protecting students enrolled in non-open courses well within the confines of FERPA. But, Blackboard's MOOC platform extends beyond the bounds of the university, allowing registration through social networking site accounts (Facebook, Twitter, LinkedIn, Google, Microsoft, and Yahoo) in lieu of creating a unique Blackboard account. EdX also allows a user to register using a Google account and a Facebook account. This could complicate to the application of student privacy protections.

As noted, FERPA does not have a vendor exception for these organizations—vendors must adhere to the same restrictions as FERPA institutions. The Department of Education has recognized the integration of technology into the classroom and how FERPA may apply to those operating the technology:

> Some types of online educational services do use FERPA-protected information. For example, a district may decide to use an online system to allow students (and their parents) to log in and access class materials. In order to create student accounts, the district or school will likely need to give the provider the students' names and contact information from the students' education records, which are protected by FERPA (Duncan 2014).

As discussed above, the agency has also extended the application of FERPA to virtual classrooms. But the Department of Education has not considered whether FERPA applies when there is no classroom.

Treatment of Data

We investigated a number of different aspects of the three platforms, including age restrictions, trackers, personal information collection and disclosures, data access and correction. The case studies reveal a wide range of data policies and practices

[7] Available at https://www.edx.org/edx-terms-service.

Table 1 University MOOC data collection and policy

	Coursera	Blackboard CourseSites	EdX
Restricts age in terms of use?	Users must be 18, emancipated minors or with guardian consent. No under 13	Users must be 18 or have parental consent	No age restrictions
Collects age data?	No	No	Yes (optional)
Total number of cookies user experienced	8	10	5
Provides data dashboard?	Yes, limited	Yes, limited	No
Provides contact information for question regarding data?	Yes	Yes	Yes

relevant to privacy concerns and laws. Table 1 found at the end of the document organizes these findings.

Age restrictions are often found in terms of service to avoid compliance with cumbersome Children's Online Privacy Protection (COPPA) regulations, applicable when a site is directed at users under age 13 or a site knowingly collects data on users under age 13.[8] Other terms of service may restrict users under age 18 to maintain an adult environment. Coursera restricts its services to users over 18, emancipated minors, and those with guardian consent. Its terms of service further emphasize restrictions against users under 13 and include an additional Protecting Children's Privacy section. Coursera does not ask for age or date of birth at registration. Similarly, Blackboard's CourseSites restricts user to those over 18 and emphasizes that by using the site, users under 18 have obtained parental consent. It does not collect age information at registration. EdX does not restrict age in its terms of service, collects year of birth (optional) at registration, and allows users under 13 to register.

As outlined above, sharing student data is strictly limited by FERPA and limitations extend to third party contractors. Simple cookies can become problematic if FERPA applies to university MOOCs. Coursera added seven cookies on its homepage[9] and course offering pages and a Google Analytics cookie at registration and one in a course page. Blackboard adds two cookies on the homepage and course offerings pages,[10] seven at registration,[11] and one when using a course page.[12] EdX

[8] If a site collects birth date information and allows for the creation of an account for users under 13, it is considered to knowingly collect information on that child.

[9] Amazon Associates, Facebook Connect, Facebook Social Plugin, Twitter Badge, Twitter Button, Google +1, and Google Analytics.

[10] Twitter Badge and Google Analytics.

[11] AddThis, Google Analytics, Google+ Platform, Facebook Connect, Facebook Social Plugins, ScoreCard Research Beacon, and Twitter Button.

[12] Google Analytics.

includes five analytics cookies on its homepage, course-offering pages, at registration, and in courses.[13]

These and other third party disclosures are discussed in each of the three terms of service. Coursera shares personally identifiable information with business partners to perform certain functions and can transfer data if Coursera is sold, merges, or reorganizes. EdX shares information in connection with specific uses, which include cognitive science and learning behavior, compliance with subpoenas and court orders, upon merger or reorganization, and integration with third party services like YouTube. Blackboard does not disclose data to third parties other than "its agents," and these agents are only permitted access to information required to perform specific services, and Blackboard prohibits them from using the data for other purposes. However, the privacy policy explains that advertisers and websites linked to CourseSites may also collect personally identifiable information, which are not covered by the privacy policy and Blackboard takes no responsibility for the use of such data.

FERPA and FIPPs contain access provisions, granting users a level of participation in their data and restricting others from gaining access. Coursera provides users with a limited data dashboard and further information on contacting Coursera administrators to access user data. EdX simply provides an email address to request access to the information maintained for a user. Blackboard allows users to correct or change information provided at registration and provides contact details to access information not available through the user account.

Specific privacy law references are not made in Coursera. EdX on the other hand, states in its privacy policy, "[P]lease note that your education records are protected by the Family Educational Rights and Privacy Act (FERPA) to the extent FERPA applies." EdX and Blackboard also specifically address European data protection law, but otherwise do not do not reference any privacy laws. FERPA requires educational institutions to use reasonable methods to ensure the security of their information technology and should compare their security methods with those practiced by any vendor contracted to handle information technology services, similar to utilizing cloud services (Privacy Technical Assistance Center 2012). Security is treated the same across the board: commercially reasonable efforts, but do not guarantee security.[14] Considering the preceding analysis of privacy concerns in education, definitions of university MOOCs and MOOC students for purposes of privacy principles and FERPA, as well as the hands-on analysis of privacy aspects in three major MOOC platforms, we turn to how university MOOCs can move forward in this environment.

[13] ChartBeat, Google Analytics, MixPanel, New Relic, and Segment.io.

[14] Note also that the FTC enforces subpar security measures that lead to security breaches. Additionally, many states have laws that deal directly with the secure disposal of personal information that apply to business, private vendors of government agencies, and government agencies themselves. Almost all states have laws that create procedures for notifying individuals when a security breach of their personal information has occurred.

Are Your MOOC Users Students?

The variation among university relationships with MOOC platform providers, university MOOC policies, and data practices reveal that this uncertainty is more than a thought experiment. Some MOOCs allow for third party cookies from companies well known for sharing and selling data to other partners. Some specifically state that FERPA does not apply where others profess the opposite. The legal uncertainty and varied data practices described above can be an opportunity. While we could argue that MOOCs are the future of education and all users should be treated as formal students or that student privacy laws should be restructured for free online courses, we instead choose to support engaged conversations among MOOC researchers and technologist building and implementing these systems. If MOOC users should be considered students based on the mission of the team, researchers and technologists should feel justified in pushing for the legal legitimacy of their users as students. If MOOCs are not intended to revolutionize higher education but intended to expose everyone to high quality educational material in an engaging and social way, researchers and technologists should make policy, design, and partnership choices that represent a certain distance from the home university and be mindful of the policies and laws that apply to general data practices. University MOOC developers and associated experts from law, policy, ethics, and technology studies have an important role in how national and state policy will develop in this space.

1. Why are you building MOOCs?

Are you building MOOCs as the future of education? Do you and your team hope they represent the way in which people, no matter their financial or geographic situation, will be able to receive educational credit in the future? Users may be perceived and treated as students to meet this vision. Even if you only hope to provide a few courses to a few interested individuals, do you consider your MOOC users university students? What makes them so and what does not? It is possible that users would be more willing to engage in university MOOCs if their data was treated as student data, which would provide more certainty and legitimacy. In fact, privacy concerns have killed innovative education efforts like inBloom.[15] There is no doubt that FERPA would place burdens on existing MOOC relationships and data practices. But there is doubt as to whether requiring strict purpose limitations down the chain of data sharing would limit MOOC goals of providing free high quality courses to the masses, as well as providing enough data to innovate within the space. Keep in mind that there are legal risks to not treating users as students and compliance risks to treating users as students.

[15] inBloom was a non-profit that offered data solutions to help public schools achieve personalized learning and integration of new applications in day-to-day teaching. Its collapse is almost entirely due to privacy concerns (Horn 2014).

2. What is your university's vision for MOOCs?

The brick and mortar campus is predicted by some to fall, but these predictions are highly contested and controversial. "The physical campus will see changes… [P]rojects like MOOC U will be the end of the traditional for-profit college. A certificate and eventually a degree from MOOC and/or online classes from top faculty in the country will soon be a better credential than a degree from one of the existing for-profits, and will certainly cost less" (Lucas 2014). If your university has invested in creating MOOCs, why has it done so? Is it cannibalizing itself or simply trying to expose global users to high quality educational content? Hoping to divide its resources between online and traditional courses but need more data to develop the online experience and enrich traditional learning? Universities likely have various goals regarding the credit-granting nature of MOOCs and whether users should be considered. MOOC teams may need to align their visions with the university's vision, which may require treating MOOC students as users.

3. What do you collect and why?

Know what information you collect. Do you collect location data? Do you collect age? At this point, many universities are designing their first few MOOCs and decisions about what is collected may be the research interests or whim of a single or few researchers, but as more MOOCs are created with added interests from other sources, it may be easy to lose track of exactly what you are collecting and why. Unless you intend to sell it, collecting data for the heck of it is rarely worth the mess. Start by creating a standard MOOC data collection list that pulls in information generally agreed upon as valuable to the MOOC team and use the opportunity to revisit the implementation of this list when considering additional data collection.

4. To whom are you disclosing user data and why?

Know who has access to your MOOC data, to whom you are disclosing data. MOOC teams are often a small core group that work on many MOOCs as one of a number of other education technology projects. The instructing faculty member may be around to build the content but less involved down the line or heavily involved in course progression. Graduate students moving in and out of MOOC teams may be working on certain courses but not others. These parties are performing internal school functions, and may not understand the increased restrictions on education records. Outside institutions, researchers, and students may request access as well. If you are to treat MOOC users as students, their data (depending on the form) may be education records and thus require informed consent to share. Speak with your university security staff to set up a system to silo access between levels of users and ensure storage and sharing procedures meet the standards of users or students.

Know who is creating additional data derived from your MOOC. The case studies reveal that it is not just the platforms that are collecting additional data from users/students; it is also third party cookies that may be problematic under FERPA.

Match your platform partnership with you data use and MOOC vision and make sure you know what they collect, who they partner with, and what their partners collect, and how this data is handled and used.

5. What are the potential harms?

This is a challenging and ongoing question but perfect for the interdisciplinary projects like MOOCs. Evgeny Morozov refers specifically to three categories of big data harms that have been hot button issues within education for decades, yet now present themselves uniquely within MOOCs: predictive sorting, filter bubbles, and discrimination (Morozov 2012). The question is whether treating users as students (i.e., applying FERPA to university MOOC data) mitigates these potential harms. Predictive sorting occurs in big data systems when individuals are grouped together based on shared characteristics predicted to have a certain outcome (e.g., women between a certain age who have clicked on a particular color of running shoes are likely to purchase a particular style of yoga pants). Sorting can make educators, students, and parents uncomfortable, because it necessarily limits a student's exposure by placing her on a track that is intended to serve the best interest of child. The fear is that a "digital Matthew Effect"[16] will be an inevitable aspect of MOOCs and other data-driven learning environments.

Individualized and personalized learning also threaten to create "filter bubbles" (Pariser 2011), also known as "echo chambers" (Turow 2013), exposing students only to what is already defined as their interests and talents. A system wherein predictive sorting and personalization occur will have discrimination concerns to consider. Data analytics can have discriminatory impact by associating certain outcomes with certain characteristics (e.g., delivering certain content to certain users indirectly based on race), as well as have discriminatory datafication processes built in (e.g., only two gender choices). Assigning FERPA student rights to MOOC users may help to minimize the widespread impact of these three harms by limiting the distribution of the data—personalization can only be so personal if data is limited. But often more data can mitigate these issues. For instance, with more data, discriminatory effects and filter bubbles can be identified and dealt with.

MacCarthy (2014) has argued that student privacy should focus on retaining contextual integrity to prevent harms. FERPA restrictions on third party contractors intend to keep student data tightly within the education context, because a third party contractor cannot use FERPA protected information for services or products not intended by the school. By labeling university MOOC users as students, the often-flimsy confines of context can be solidified. However, solidification of context may be too inflexible for the nature of harms sought to be prevented and the potential benefits promised by university MOOCs. To curb concerns regarding personalization and privacy invasions, Jules Polonetsky and Omer Tene have encouraged user controls and "featurization" through dashboards (Polonetsky and

[16] The Matthew effect, coined by sociologist Alan C. Kerckhoff and Elizabeth Glennie, is a theory or explanation of why the "rich get richer" theory. When adapted for the purposes of education, the Matthew effect has caused many to question tracking structures in education systems (Kerckhoff and Glennie 1999).

Tene 2014), which would add additional design costs and time to MOOCs but would limit structural challenges related to how MOOC teams would handle requests for access and corrections. MOOC users could decide for themselves whether to be treated as students and signal to administrators through the system. Discuss whether these harms are potential risks for your data use and how you intend to mitigate or accept them.

After you work through these questions, draft your own FIPPs. Add an initial principle that reflects how user data will be treated in terms of their status as students, and draft the remainder of the principles keeping in mind potential restrictions you may want to add for treating users as students. Work with your university general counsel to draft a terms of service that expresses clearly your answers to these questions and your FIPPs.

Conclusion

Schools have a long history of holding sensitive student information, but often would be considered data rich and information poor. As that characterization changes with talented and motivated researchers engaging with user data, the question of who is a student becomes more and more important to the future of education. The emergence of MOOCs across campuses and large enrollment figures suggest that MOOCs have the potential to transform education in one way or another. Institutions, faculty, and MOOC users (or MOOC students) will determine the evolution of MOOCs. As more universities get involved with MOOCs, develop more courses, and create more tools and practices to gain insight, the privacy of users must not be left behind. The legal uncertainty created by the disruption of MOOCs outlined above does not allow for conclusive direction to be given, but we hope this article will support MOOC researchers and faculty to be actively involved in developing legal certainty that reflects the future of education they envision.

References

Adamopoulos, P. (2013). What makes a great MOOC? An interdisciplinary analysis of online course student retention. In *Proceedings of the 34th international conference on information systems, ICIS* (p. 13).

Allen, I. E., & Seaman, J. (2013). Changing course: Ten years of tracking online education in the United States. Sloan Consortium. http://onlinelearningconsortium.org/survey_report/changing-course-ten-years-tracking-online-education-united-states/. Retrieved 16 Feb 2015.

Berkman Center for Internet & Society. (2015). Student privacy initiative. https://cyber.law.harvard.edu/publications/2014/spi_publications. Retrieved 14 July 2015.

Blanchard, J. (2007). University tort liability and student suicide: Case review and implications for practice. *JL & Education, 36*, 461.

Britz, J., & Zimmer, M. (eds.). (2014). *International Review of Information Ethics*, 21.

Cormier, D. (2008). The CCK08 MOOC—connectivism course, 1/4 way. *Dave's Educational Blog*. http://davecormier.com/edblog/2008/10/02/the-cck08-mooc-connectivism-course-14-way/. Retrieved 5 Aug 2014.

Daggett, L. M. (2008). Student privacy and the protection of pupil rights act as amended by no child left behind. *UC Davis J. Juv. L. & Pol'y, 12*, 51.
Department of Education. (2008). Family educational rights and privacy, 34 CFR Part 99.
Department of Education. (n.d.). Frequently asked questions about FERPA. http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpafaq.pdf. Retrieved 16 Feb 2015.
Downes, S. (2009). Access2OER: The CCK08 solution. *Half an Hour (Personal Blog)*. http://halfanhour.blogspot.com/2009/02/access2oer-cck08-solution.html. Retrieved 5 Aug 2014.
Duncan, A. (2014). Letter to Sen. Edward Markey. http://www.markey.senate.gov/documents/2014-01-10_Education_Privacy.pdf. Retrieved 16 Feb 2015.
Federal Trade Commission. (2014). Complying with COPPA: Frequently Asked Questions. http://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions. Retrieved 16 Feb 2015.
Fischer, L., Schimmel, D., & Kelly, C. (1995). *Teachers and the law* (4th ed.). White Plains, NY: Longman.
Future of Privacy Forum. (2015). Student privacy. http://www.futureofprivacy.org/issues/student-privacy/. Retrieved 14 July 2015.
Gardner, L., & Young, J. (2013). California's move toward MOOCs sends shock waves, but key questions remain unanswered. *Chronicle of Higher Education*. http://chronicle.com/article/A-Bold-Move-Toward-MOOCs-Sends/137903/. Retrieved 8 Aug 2014.
Horn, M. (2014). inBloom's collapse offers lessons for innovation in education. *Forbes.com*. http://www.forbes.com/sites/michaelhorn/2014/12/04/inblooms-collapse-offers-lessons-for-innovation-in-education/. Retrieved 16 Feb 2015.
Johnson, T. P. (1993). Managing student records: The Courts and the Family Educational Rights and Privacy Act of 1974. *West's Education Law Quarterly, 2*(2), 260–276.
Kerckhoff, A. C., & Glennie, E. (1999). The Matthew effect in American education. *Research in Sociology of Education and Socialization, 12*(1), 35–66.
Kolowich, S. (2013a). A university's offer of credit for MOOC gets no takers. *Chronicle of Higher Education*. http://chronicle.com/article/A-Universitys-Offer-of-Credit/140131/. Retrieved 8 Aug 2014.
Kolowich, S. (2013b). California puts MOOC bill on ice. *Chronicle of Higher Education*. http://chronicle.com/blogs/wiredcampus/california-puts-mooc-bill-on-ice/45215. Retrieved 8 Aug 2014.
Kolowich, S. (2013c). American Council on Education Recommends 5 MOOCs for credit. *Chronicle of Higher Education*. http://chronicle.com/article/American-Council-on-Education/137155/. Retrieved 8 Aug 2014.
Leckart, S. (2012). The Stanford education experiment could change higher learning. *Wired.com*. http://www.wired.com/wiredscience/2012/03/ff_aiclass/. Retrieved 5 Aug 2014.
Lucas, H. (2014). Disrupting and transforming the university. *Communications of the ACM, 57*(10), 32–33.
MacCarthy, M. (2014). Student privacy: Harm and context. *International Review of Information Ethics, 21*, 11.
Mawdsley, R. D., & Russo, C. J. (2002). Limiting the reach of FERPA into the classroom: Owasso school district v. Falvo. *West Education Law Reporter, 165*, 1–13.
Merriam, S. B., Caffarella, R., & Baumgartner, L. (2007). *Learning in adulthood: A comprehensive guide* (3rd ed.). New York: Wiley.
Morozov, E. (2012). In Soviet Russia, book reads you. *Slate*. http://www.slate.com/articles/technology/future_tense/2012/11/coursesmart_analytics_whispercast_the_danger_of_software_that_monitors_students.2.html. Retrieved 16 Feb 2014.
Nesterko, S. O., Dotsenko, S., Han, Q., Seaton, D., Reich, J., Chuang, I., & Ho, A. D. (2013). Evaluating the geographic data in moocs. In *Neural information processing systems*. http://nesterko.com/files/papers/nips2013-nesterko.pdf
Noer, M. (2012). One man, one computer, 10 million students: How Khan Academy is reinventing education. *Forbes.com*. http://www.forbes.com/sites/michaelnoer/2012/11/02/one-man-one-computer-10-million-students-how-khan-academy-is-reinventing-education/. Retrieved 8 Aug 2014.
O'Donnell, M. L. (2003). FERPA: Only a piece of the privacy puzzle. *Journal of College and University Law, 29*, 279–715.
Pariser, E. (2011). *The filter bubble: How the new personalized web is changing what we read and how we think*. New York: Penguin Books.

Penrose, M. M. (2012). In the name of Watergate: Returning FERPA to its original design. 14 *N.Y.U. J. Legis. & Pub.* Pol. 75, 96.

Piech, C., Huang, J., Chen, Z., Do, C., Ng, A., & Koller, D. (2013). Tuned models of peer assessment in MOOCs. arXiv preprint arXiv:1307.2579.

Polonetsky, J., & Tene, O. (2014). The ethics of student privacy: Building trust for Ed Tech. *International Review of Information Ethics, 21*, 31–32.

Privacy Technical Assistance Center. (2012). PTAC-FAQ. http://ptac.ed.gov/sites/default/files/cloud-computing.pdf. Retrieved 16 Feb 2015.

Sandeen, C. (2013). Integrating MOOCS into traditional higher education: The emerging "MOOC 3.0" Era. *Change: The Magazine of Higher Learning, 45*(6), 34–39.

Sheridan, K. (2013). Blackboard MOOC gains 15 more colleges. *InformationWeek*. http://www.informationweek.com/software/blackboard-mooc-gains-15-more-colleges/d/d-id/1110778. Retrieved 16 Feb 2015.

Simon, S. (2014). Data mining your children. *Politico*. http://www.politico.com/story/2014/05/data-mining-your-children-106676.html. Retrieved 5 Aug 2014.

Solove, D. (2013). Privacy self-management and the consent dilemma. *Har. L. Rev., 126*, 1880.

Straumsheim, C. (2014). Proactive on prior learning. *Inside Higher Ed*. https://www.insidehighered.com/news/2014/04/15/accept-moocs-credit-florida-international-u-may-set-prior-learning-assessment. Retrieved 16 Feb 2014.

The White House. (2012). Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy (Report). http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

The White House. (2015). FACT SHEET: Safeguarding American Consumers & Families (Press Release). http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families

Toglia, T. V. (2007). How does the family rights and privacy act affect you? *Tech Directions, 67*(2), 32–35.

Turow, J. (2013). *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven: Yale University Press.

Virginia Tech IRB. (2015). FAQ for Academic Assessment Research. http://www.irb.vt.edu/pages/assessment.htm. Retrieved 16 Feb 2015.

'Watered Down' MOOC Bill Becomes Law In Florida. (2013). *Inside Higher Ed.* http://www.insidehighered.com/quicktakes/2013/07/01/watered-down-mooc-bill-becomes-law-florida. Retrieved 8 Aug 2014.

What You Need to Know About MOOCs. (2014). *The Chronicle of Higher Education*. http://chronicle.com/article/What-You-Need-to-Know-About/133475/=. Retrieved 5 Aug 2014.

Young, J. (2012). Inside the Coursera Contract: How an upstart company might profit from free courses. *Chronicle of Higher Education.* http://chronicle.com/article/How-an-Upstart-Company-Might/133065/. Retrieved 16 Feb 2014.

Young, J. (2013). California puts MOOC bill on ice. *Chronicle of Higher Education: Campus Wired Blog*. http://chronicle.com/blogs/wiredcampus/california-puts-mooc-bill-on-ice/45215. Retrieved 8 Aug 2014.