2017

Beyond Compliance

Cecelia Parks
University of Mississippi, cparks@olemiss.edu

Recommended Citation

Parks, C. (2017). Beyond compliance: Students and FERPA in the age of big data. Journal of Intellectual Freedom and Privacy 2(2), 23-33.

Preprint of:
Parks, C. (2017). Beyond compliance: Students and FERPA in the age of big data. *Journal of Intellectual Freedom and Privacy 2*(2), 23-33.
https://journals.ala.org/index.php/jifp/issue/view/636

Beyond Compliance: Students and FERPA in the Age of Big Data

Abstract

Privacy is governed by an array of laws in the United States, and this paper examines one facet of privacy regulation: the privacy of students' academic records. The Family Educational Rights and Privacy Act (FERPA) protects the privacy of these records, but how do students understand their rights under FERPA, especially with the development of big data and learning analytics technologies that demand unprecedented sharing of student data? This paper begins to answer that question by examining existing literature on privacy in general and with regards to FERPA specifically. It suggests that FERPA places most of the power in controlling student data in the hands of educational institutions but is ultimately unable to address many legal and ethical concerns around current uses of student data. FERPA's ineffectiveness makes it imperative that students understand their rights and are able to protect their own privacy, yet many students are probably not fully aware of their rights and privileges under FERPA. However, further empirical research is needed to explore exactly how students understand their FERPA rights and the implications of student perceptions of academic privacy.

Introduction

Privacy concerns abound with the development of big data technologies that collect and analyze everything we do online, the explosion of social media, and increasing security breaches into corporate and governmental troves of data. Though individuals may be aware of some basic strategies to protect their personal privacy, most are less likely to be aware of the safeguards in place around specific types of records—such as their academic records—or their rights associated with those safeguards. In the United States, the Family Educational Rights and Privacy Act of 1974 (FERPA) governs the privacy of academic records. FERPA can be a useful tool for protecting personal information in academic contexts, but those who are not higher education professionals often do not understand its full implications or even its general purpose as it applies to people learning and working in institutions of higher education. It is key that students in particular understand their privacy rights under FERPA to ensure those rights are protected.

FERPA itself has been well documented from the points of view of many different higher education professionals and legal scholars, but those it is designed to protect—college students—have largely been neglected in the scholarship about FERPA. This paper brings together different existing strands of literature to begin to fill that gap. I will start by discussing American privacy law and FERPA generally, then examine scholarship on FERPA, on how students' data is being used in higher education contexts, and on college students' perceptions of privacy in other contexts. I conclude that FERPA is unable to address many legal and ethical concerns around current uses of student data—making it imperative that students understand their rights and are able to protect their own privacy—yet many students are probably not fully aware of their rights

and privileges under FERPA. Though the extant literature tentatively supports this conclusion, additional empirical research is necessary to confirm it.

Privacy as a Legal Right in the United States

Though the right to privacy is not specifically mentioned in the U.S. Constitution, the United States has signed a number of international treaties in which the right to privacy is protected, including the Universal Declaration of Human Rights (1948), the American Declaration of the Rights of Man (1948), the International Covenant on Civil and Political Rights (1966), and the Convention on the Rights of the Child (1989). Warren and Brandeis (1890) first articulated the right of privacy in the United States in its modern form, arguing that privacy protections went beyond protections from purely physical intrusions to include the "right to be let alone" in all aspects of life. Privacy protections have since evolved from the definition articulated by Warren and Brandeis to include the more active right of individuals to control their own information (Langenderfer and Miyazaki 2009, 381). The right of privacy is also interwoven through the Constitution; the Supreme Court ruled in *Griswold v. Connecticut* that a "penumbra" of privacy protections emanates from the Bill of Rights, especially the First, Third, and Fourth Amendments (*Griswold v. Connecticut* 1964).

Legal precedent has established that the Constitution offers general privacy protections, but there is no single, comprehensive privacy law in the United States. There is a strong precedent of privacy litigation in civil cases (torts), in which one individual can sue another for infringing upon their privacy, but these torts have not been officially codified. One of the more broad-reaching pieces of privacy legislation in the United States is the Privacy Act of 1974, which protects all private information collected and distributed by federal agencies. While this legislation is comprehensive in that it protects all such information, it is limited in that it only applies to information collected by the government. It has no bearing on the vast amounts of information collected by private entities (Privacy Act of 1974). Most existing privacy legislation in the U.S. only addresses one type of information; for example, the Right to Financial Privacy Act of 1978 protects financial information, while the Health Insurance Portability and Accountability Act of 1996 includes provisions to protect sensitive health information.

The Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA) is one of the laws created to protect individuals' privacy in a specific area, namely the privacy of academic records. FERPA was enacted in 1974 to create a unifying national policy for dealing with educational records. "Academic records" are defined by the U.S. Department of Education as "those records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution." A student's academic record contains information specifically about them, such as grades and disciplinary violations. In this paper, "academic records" and "student data" are used interchangeably, in recognition of the recent expansion of the types of information that comprise academic records. Prior to FERPA, academic records were subject to state laws, which created a confusing patchwork of governance that often gave students and parents little access to academic records while allowing access to outside authorities without consent from or notification of the student themselves

(Elliot, Fatemi, and Wasan 2014, 36). Today, FERPA gives the student (or the student's parents or guardians) access to and control of their academic records.

FERPA grants parents or legal guardians the right to control their child's records until the student reaches the age of eighteen, at which point that right transfers to the student. These students are referred to as "eligible students." However, institutions can release information to parents without an eligible student's consent if the student is claimed as a dependent on the parent's income tax statement ("FERPA General Guidance" 2015). Control over academic records under FERPA has three main aspects:

1. Parents or eligible students have the right to review their academic records.
2. Parents or eligible students may request correction of the record if they believe an error has been made.
3. Educational institutions may not release those records (with a few exceptions) without written consent of the parent or eligible student.

Educational institutions are allowed to share "directory information," including the student's name, address, date of birth, dates of attendance, and honors or awards given to the student, without consent. Parents or eligible students can choose not to have that directory information shared, but they must submit an official request to the university. Full academic records may be shared with other entities under certain circumstances; law enforcement officers, for example, can access student academic records without parent or eligible student consent.

In addition to guaranteeing parents and eligible students the rights outlined above, FERPA compliance includes mandatory annual notification of all parents and eligible students of their rights guaranteed by law. This notification must include the institution's disclosure of directory information and any other potential disclosures of students' academic records, and inform parents or eligible students how to opt out of that disclosure (Family Educational Rights and Privacy Act 1974).

FERPA in Practice

Though FERPA establishes minimum federal requirements for the protection of students' academic records, in practice it places almost all power in implementing those protections in the hands of the educational institutions, and leaves individual students with few realistic options for determining how their records are shared. One of the major ways that this power dynamic plays out is in the lack of a meaningful enforcement mechanism. The only penalty specified by FERPA that the offending institution can receive for improperly releasing academic records is the loss of all federal funding, a punishment so severe that it has never been implemented. As the Supreme Court ruled in *Gonzaga University v. Doe* (2002), FERPA creates no "personal rights to enforce" provisions of the law, so students cannot use FERPA to sue a private university for releasing their academic record to unauthorized persons. The only options available to students who feel their information has been improperly disclosed to a third party are either to file a written complaint with the Family Policy Compliance Office (though there is no guarantee that their complaint will be addressed) or to sue under a relevant state law (though not all states have such laws) (Sidbury 2003, 676). The lack of options for complainants means that the Department of Education and educational institutions hold most of the power in deciding how and when disclosure of student information to third parties is acceptable, and institutions have been moving

towards allowing increased disclosure to a variety of parties in recent years (Rotenberg and Barnes 2013, 57).

Loopholes that allow for the disclosure of student information to third parties also minimize the amount of control that students have over their own records. Sometimes that disclosure is done in the name of national security and personal safety. The terrorist attacks on September 11, 2001, and the Virginia Tech shooting in 2007 each reignited the debate on how much student information institutions should be required to disclose to law enforcement officials, parents, and other third parties (Khatcheressian 2003, 479). Both led to expansions of how and when student records can be shared in situations that affect the health and safety of an individual student or the community, thus expanding the discretion granted to institutions in disclosing students' academic records without their consent (Humphries 2008, 149).

FERPA in the Digital Age

While it is difficult to argue against increased information sharing in service of safety and security, institutions have been presented with other challenges to protecting the privacy of student records that are less straightforward, and FERPA does not offer clear guidance on how to proceed. One significant issue is that FERPA was created in a time of paper educational records and is based on the idea of controlling access to those physical records. Today, student records are almost all digital, and digital records present a different paradigm for privacy protection than physical records—one that FERPA does not address. It is much easier to create and share digital records that contain much more information than physical records (Zeide 2016, 342); for example, digital records can amalgamate electronic data from different services across campus and share those records in an instant, while physical records are much more siloed. Technological factors, such as the software used to create, maintain, and share digital records, also play a significant role in how privacy protections are actually implemented due to the limitations they impose and the institutional norms they embody (O'Donnell 2003, 680). Additionally, even experts on FERPA disagree on what kinds of information now being collected (such as geolocation data collected through ID card swipes or browsing data from campus Wi-Fi use) count as part of the "academic record" and are thus protected under FERPA, again giving institutions significant latitude in how they collect and share student records (Wasson 2003, 1358).

In addition to technological factors, legal decisions have also changed how institutions can share student information under FERPA. Changes to the "School Official Exception" in 2008 allowed institutions to share student information with third parties without disclosure or consent. Under this exception, institutions have discretion to share information with third parties as long as sharing serves a "legitimate educational interest," provided that the third party also takes measures to secure the student records (Zeide 2016, 343). This provision originally existed to simplify sharing student information with different units across campus, but it now covers contractors, consultants, volunteers, and any other group or individual to whom the institution has outsourced services or functions (360). The exception was revised in response to the proliferation of third parties that work with everything from dining services to attendance to learning management systems (LMS), all of which require access to FERPA-protected student data. Institutions are now free to share any information in a student's academic record with any third party that they designate a "school official," and FERPA does not obligate them to obtain student consent, thus further shifting the balance of power in controlling student records away from the students.

Big Data, Learning Analytics, and Student Privacy

An emerging trend in higher education that FERPA does not adequately address and that continues to tip the balance of power over the privacy of student data towards institutions and third parties is the use of big data and learning analytics to drive institutional decision-making and improve student learning outcomes. "Big data" refers to datasets that are distinguished by their volume, variety, and velocity—that is, they contain unprecedented amounts of data that comes from many different sources, and the data can be analyzed and shared quickly (Executive Office of the President 2014). In the higher education context, big data techniques allow the collection, synthesis, and analysis of data from disparate systems across campus to create comprehensive profiles of students that go beyond the traditional "academic record."

Learning analytics are a particularly promising aspect of big data's implementation in higher education. Slade and Prinsloo (2013) define "learning analytics" as "the collection, analysis, use, and appropriate dissemination of student-generated, actionable data with the purpose of creating appropriate cognitive, administrative, and effective support for learners" (1512). Learning analytics offer the promise of providing institutions and instructors with more detailed, accurate assessments of student progress, learning, and engagement that can contribute to better recruitment and retention as well as create personalized learning experiences tailored to the needs of each individual student.

Despite the pedagogical potential of learning analytics, they present significant ethical issues that have not been resolved, especially as many learning analytics systems are developed and implemented by parties outside the institution of higher education. These issues do not preclude the use of learning analytics, as there are real institutional and individual benefits to be derived from them, but the ethical concerns should be considered as learning analytics systems are implemented. Slade and Prinsloo (2013) note three areas of concern in particular: the "location and interpretation of data; informed consent, privacy, and deidentification of data; and the management, classification, and storage of data" (1511). Similarly, Pardo and Siemens (2014) detail four principles that must be addressed in the implementation of learning analytics: transparency, student control over data, right of access, and accountability and assessment. Rubel and Jones (2016) hold that autonomy—control over personal information—is an important condition of privacy, and learning analytics systems remove data from student control and thus violate students' autonomy. These papers bring up issues of privacy that are not addressed by FERPA, especially in regards to institutional and student access to and control of information that is collected, analyzed, and stored by third parties. Removing this data from direct institutional control removes transparency from the process of information collection, storage, and use, and leaves data more vulnerable to exploitation and unauthorized sharing.

Deidentification of student records when they are handed over to a third party has been proposed as a way to mitigate privacy concerns, but this has proved to be an impractical solution. Rubel and Jones (2016) point out that learning analytics must link to personal student information to provide a truly customized experience, so deidentifying information given to the providers of learning analytics systems defeats the purpose of those systems (144). Additionally, big data technologies like those employed in learning analytics actually have the capability to create new identifying information or reveal identifying information that had been previously removed (Young 2015, 550). Therefore, even student records shared with a provider of learning analytics with the best intentions may share students' personal information without their knowledge.

Even though such sharing of student information would seem to be a violation of student privacy because personal data is shared outside of the institution without students' explicit consent, institutions are still compliant with FERPA under these conditions as long as the provider of learning analytics is designated a "school official." Students have little recourse to protect their records or prevent such information sharing due to the lack of meaningful enforcement provisions in FERPA, and large-scale data collection and analysis has become so commonplace in higher education that escaping it entirely is nearly impossible. Participation in the system of higher education in the United States now implicitly requires that students consent to sharing their personal information with third parties with little transparency or control over their own information. Big data and learning analytics continue to shift the balance of power over student privacy away from students and towards institutions.

Institutional privacy policies are currently designed to keep the university in compliance with a law that does not adequately address the way that student data is collected, shared, and used, not to give students autonomy over their own data. Therefore, some argue that institutions have a moral and ethical obligation to take steps beyond what is mandated by FERPA to protect students' privacy and give students more control over their own records. Prinsloo and Slade (2015) state that institutions "have a moral obligation to not only make students aware of the implications [of sharing data with learning analytics systems], but also to provide a platform for empowering students with civic agency regarding their data" (89). Similarly, Tene and Polonetsky (2013) argue that "individuals must be offered meaningful rights to access their data in a usable, machine-readable format," noting that current access rights under FERPA are not easy to employ or particularly useful, as requests are not answered quickly and records are often provided in hardcopy only (242). These actions would shift the balance of power away from institutions and towards students, giving students more autonomy over their own data and empowering them to determine how and when their data is collected and shared.

Students and Privacy

The purpose of this paper is not to argue how or why FERPA should or should not be amended, but rather to examine FERPA's impact on those it is designed to protect: students. Any amendments to FERPA or changes in institutional policy, especially those designed to give students more control over their own records, can only be successful if students are aware of how their data is collected and used and of their rights under FERPA and institutional policies. Currently, very little scholarship exists to confirm or deny if students understand how their academic data is being collected and used, or what their legal rights and privileges to that data are.

However, several studies have been conducted on young adults' (college-aged individuals) awareness of online privacy more broadly, and students' awareness of privacy issues online can be used to gain insight into their awareness of other aspects of privacy, though the comparison is not perfect. The traditional freshman class of 2017 was mostly born in 1998-1999; they likely do not know of a time before the Internet. This means that most college students, having grown up with the Internet, have some idea of privacy issues online. Several studies have demonstrated that students are concerned about their privacy and aware of potential threats to their privacy or security in the online environment, but that awareness is not often translated into action to protect their privacy (Bryce and Fraser 2014; Hargittai and Marwick 2016; Johns and Lawson 2005; Soffer and Cohen 2014; Youn 2005).

Many students often do not take action to protect their privacy for a variety of reasons. Most college students today grew up in the Internet age, so privacy threats have been normalized; data collection is routine, so it is not perceived as truly threatening (Bryce and Fraser 2014, 304). In a study conducted by the Pew Research Center, several of the college-aged participants spoke casually about privacy risks. One stated, "If someone pays enough, nothing is really private. Only way I see to really keep private, you have to stay off [the] Web" (Madden et al. 2014). Later comments show that the participant does not seem willing to take the drastic step of staying off the Web entirely, demonstrating that the threats to their privacy are not serious enough to deter online participation.

Another reason many students continue to use online services that threaten their privacy is that they perceive the benefits as outweighing any potential loss of privacy. They may recognize that in signing up for a website or using a service, they are allowing an outside party to access their personal information, but that loss of privacy is not enough to deter them from using the service (Youn 2005, 104). Social networking sites (SNS) like Facebook and Twitter are among the top websites used by college students that have potentially serious consequences for personal privacy. Soffer and Cohen (2014) note:

> Although adolescents are concerned about their security, the merits of having an SNS profile and participating in social networks is so important for students that they are willing to cope with a certain degree of privacy threats… Students are willing to act in opposition (e.g., by signing an online petition) if an action is threatening their privacy; but only very few students are willing to quit an SNS, despite the identification of privacy threats (153).

Many students are often aware of the privacy risks associated with social networks, but the social capital associated with using social media overrides any privacy concerns. This combined with the prevalent view of online privacy invasions as routine means that college-aged individuals often act in opposition to their privacy rights.

However, students' privacy behavior may not only be caused by a simple disregard of the risks. Privacy notices and disclosure statements are notoriously complex and difficult to read, which means that they are often skimmed or skipped entirely. They thus do not fulfill their intended purpose: to tell users how their information may be collected and used; in other words, what potential threats the website or service poses to users' privacy. The Gramm-Leach-Bliley Act of 2001 requires all financial institutions to explain their information-sharing practices, and many non-financial entities collecting user information also employ similar notification policies. However, the policies detailing information disclosure practices are often written in legalese and are designed to protect the entity from future litigation, not to empower the user to make informed decisions about their privacy (Milne and Culnan 2004, 24).

Proctor, Ali, and Vu (2008) analyzed 100 different privacy policies and found that the typical policy requires thirteen years of education to fully comprehend. Though that is equivalent to some college education, most college students could not pass the comprehension tests administered by the researchers (326). Even entities that participate in "privacy seal programs," in which they display a graphic on their website that supposedly demonstrates their commitment to privacy protection, often have complex privacy policies that do not necessarily align with the values communicated by the seal (Larose and Rifon 2007, 128). The readability issues with most privacy policies mean that few people actually read them—most just click through because

accepting the terms and conditions (including the privacy policy) is required for use of the website. If the privacy policy looks too complex, even someone who is concerned about his or her privacy is unlikely to read it (Milne and Culnan 2004, 24).

The ubiquity of privacy policies contributes to the normalization of privacy risks, especially to college students who have existed in the online space their entire lives. All of the above factors contribute to students' general awareness of privacy issues, but also to their limited understanding of the actual privacy risks of this information age and the laws that exist to protect their privacy. Though Johns and Lawson (2005) found that 95% of students surveyed were concerned about their privacy (491), only a third of students were aware of the USA PATRIOT Act, arguably one of the most significant threats to privacy in recent years (490). These same students also agreed that universities should take steps to protect student data, including a 91% consensus that universities should not share student information with outside parties (492).

Students understand that they should be concerned about their privacy. They understand that online participation comes with privacy risks. However, they are often unaware of the specific risks posed by different online entities, and they are unwilling to cease use of a website or service if they perceive the benefits of using that service to outweigh the risks—even if their perception of the risks is not in line with reality. If students are unaware of the privacy risks they face with the online services they use on a regular basis, then how do they understand the privacy risks associated with their academic records and the laws designed to minimize those risks?

How Students Understand FERPA

Most college students are demonstrably interested in their privacy; however, while studies of young adults' perceptions of their privacy generally or in online settings can give researchers some insight into how college students perceive and manage their privacy, they cannot completely explain how students understand the privacy of their academic records. The higher education setting presents different challenges to protecting privacy than social media or other online settings, causing students' perceptions and expectations of privacy to change. For example, a student may be upset about unflattering photos circulating on the Internet, but they may be much more perturbed about their grades or disciplinary records being shared without their knowledge or consent due to the sensitive nature of those records and the expectation that their institution of higher education should protect those records. These records can have a significant impact on students' future employment prospects and their reputation in general, so students' understanding of how their academic data is collected and used and of their FERPA rights to control and protect that data is crucial.

Despite the implications for students, scholars have rarely researched if and how students think about their academic records and, relatedly, how they understand their FERPA rights. Authors such as Rubel and Jones (2016, 154) and Slade and Prinsloo (2013, 1516) assert that students lack awareness of how their academic data is being used but do not adequately support their claims. Anecdotal evidence (including the author's personal experiences as an academic advisor) and interviews collected by the Pew Research Center (Rainie and Anderson 2014) support this assertion, but very few studies have rigorously addressed this issue.

In 2011, Martin Dowding published one of the few studies of students' understanding of their academic privacy, concluding that students were not concerned about their privacy as a right and did not understand laws designed to protect the privacy of their academic records. Dowding used focus groups to evaluate students' comprehension of a Canadian law passed in

2006, the Freedom of Information and Protection of Privacy Act (FIPPA). FIPPA includes provisions similar to FERPA that require Canadian educational institutions to protect the privacy of their students' records. Dowding's results showed four major issues in how students thought about the privacy of their academic records:

1. Students were fairly uninformed about their privacy rights in general.
2. Students knew very little about laws designed to protect their privacy, including FIPPA.
3. Students expressed interest in several ways for the university to disseminate information about privacy, but were unaware that those means were already being utilized.
4. Students did not necessarily think of privacy as a right (25).

Each of these issues contributes to a lack of concern and understanding by students about the privacy of their academic records. Though Dowding studied Canadian students, and the law in question is much newer than FERPA, I posit that similar issues exist in American higher education.

Several recent studies have examined students' perceptions of sharing their data with learning analytics systems independent of their knowledge or understanding of existing privacy protections. Many students are accustomed to the online learning environment, and expect learning analytics systems to offer a broad variety of academic support, such as self-assessments, personalized learning activities, and content recommendations (Ifenthaler and Schumacher 2016, 933). Most students surveyed understood that their data has educational value (Arnold and Sclater 2017), and did not have significant reservations about allowing their data to be used in learning analytics systems (Sclater, Peasgood, and Mullan 2016). In this case, students' feelings about allowing their academic data to be used are similar to their perceptions of their online privacy: they accept some decrease in personal privacy because they see value in how their information is used.

However, students did express a desire to maintain some level of control over the data they shared, similar to the suggestions made by Slade and Prinsloo and Tene and Polonetsky. Most did not object to sharing academic data, such as grades and LMS data, but were reluctant to share more personal data, such as data harvested from social media sites (Ifenthaler and Schumacher 2016, 934). Big data and learning analytics techniques are now capable of collecting and synthesizing such data with academic data, so such a choice would require a more sophisticated mechanism to opt-out of data sharing beyond just restricting the use of their directory information, as well as an improved informed consent process (Slade and Prinsloo 2015, 26).

Though these studies are useful in that they address what students might hypothetically be willing to share, they either ignore existing policies to protect student privacy altogether or explain those policies as part of the study. They do not assess student's prior knowledge of FERPA and the protections it does (or does not) grant them, nor do they assess students' understanding of how their academic records are actually being shared and used. Thus, they do not allow us to confirm or deny the conclusion that students do not understand how their academic records are collected, shared, and protected under FERPA.

FERPA Notifications

Even if students are willing to share their academic data, FERPA in its current incarnation does not facilitate the kind of informed consent and opt-in procedures for which scholars advocate and some students seem to want. The legally mandated notifications could be

an avenue to educate students and clarify the procedures for opting out of the disclosure of directory information. Johns and Lawson (2005) state the importance of this mandatory notification: "Students' ability to opt out, or likelihood of doing so, depends on how aggressive the university is in informing the students about FERPA, or how aware the student is of the policy" (487). However, there are several major problems with the current system of notification that impact students' comprehension of their FERPA rights and their ability to opt out of disclosure. One is that FERPA notifications share many of the same readability issues of commercial privacy policies. Another issue is the lack of follow-up to the notification itself.

In order to cover all of the information required by law, FERPA notifications are long. They are also written in *legalese* to make sure the institution has met all of their disclosure requirements. These factors mean that FERPA notifications are often inaccessible to parents and eligible students due to their complexity. For example, the University of Maryland's 2015 FERPA notification email was over one thousand words long, and it had the highest estimated Flesch-Kincaid reading level possible, meaning that the user would need at least a high school education to understand it. The University of Maryland's FERPA notification is not an exception; it is in line with the readability of most other privacy notifications, which require on average thirteen years of education to fully comprehend (Proctor, Ali, and Vu 2008, 326).

That FERPA notifications are lengthy and complex has serious implications for their utility. FERPA notifications cover similar content and have similar problems as commercial privacy policies, which means that users are unlikely to read them at all or to read them thoroughly. Therefore, most people probably do not read their FERPA notifications closely enough to truly comprehend their rights under FERPA or how the educational institution uses and shares their academic records and personal information. Though the institutions are compliant with the letter of the law, they are not fulfilling the spirit of the notification requirement.

There are several other ways institutions communicate information about FERPA to students beyond the official FERPA notifications. One is the institutional website, which usually has a page that covers roughly the same information as the FERPA notifications. While the notification may link to this web page, it is not generally publicized or referred to on a regular basis at many institutions. FERPA rights may also come up in circumstances where they actually apply, such as an academic advising appointment with an eligible student whose parent(s) would like to participate. In that case, it is the responsibility of the university employee (the academic advisor) to explain the student's FERPA rights in that situation, and to have them sign the necessary waiver to allow the disclosure of their academic records to a third party.

While the information provided online can certainly be useful, and university employees are trained to deal with FERPA issues, neither of these methods of outreach about FERPA rights constitutes sufficient follow-up to the email notification ensure that students actually understand their rights. If students do not read or fully understand the official FERPA notification and only minimal follow-up is provided, then it is unlikely that students fully understand their rights. Few students are actually going to consult the university's website to learn more about FERPA; Dowding (2011) found that the students surveyed were unaware that such information was available online, even though they had been told about their institutions' online privacy resources. The students instead suggested a more personal approach, such as having someone speak to them at university orientation (25). If educational institutions are interested in ensuring that their students understand their privacy rights and can make informed decisions about their records, they need to go beyond what the law requires them to do and follow the official FERPA

notification with other, more personal, outreach. Right now, the notification system is not designed for students to understand their FERPA rights and how their data is used—it is primarily designed to keep the university nominally compliant with the law.

Implications for Institutions of Higher Education

The available evidence and ineffective FERPA notifications point to the conclusion that many students do not understand how institutions of higher education collect, use, and disclose their academic records, nor do they understand their rights to control their records granted to them by FERPA. Though this conclusion has not been affirmed in an American setting, students' lack of awareness may be beneficial to universities and third parties alike. Students hypothetically indicated that they would be open to sharing their data with learning analytics systems, but they may be more restrictive with the type or amount of data they would share if given the opportunity to fully understand what was being collected and to determine exactly what data was shared. Big data techniques rely on ingesting as much data as possible from many different sources to draw conclusions, and limiting the flow of data by giving students more control may limit the efficacy of learning analytics systems built with big data technology.

Additionally, increasing awareness of data collection and its uses may have a chilling effect beyond merely impacting what records some students allow to be shared with third parties. Dawson (2006) found that student behavior in an online learning environment changed to be more reticent and cautious when students realized that their behavior was monitored by institutional personnel beyond the instructor (80). If students are currently unaware of how their behavior in a LMS can be monitored, collected as data, and viewed and analyzed by someone outside of the class or even the institution, they may change how they interact with the LMS.

From a student privacy perspective, a change brought on by a better system of notification and informed consent constitutes increased student autonomy over their own data. However, from an institutional perspective, it represents a potential threat to the kinds of insights that can be gleaned from learning analytics, because institutions also rely on in-house analyses of student data to inform their own decision-making processes. Meanwhile, from a learning analytics developer perspective, it represents a potential threat to their business model. This is not to say that institutions and third parties have been colluding to keep students ignorant for nefarious purposes, but FERPA currently gives institutions most of the power in determining how student data is collected and shared, and shifting that balance of power would potentially have negative implications for institutions and the third parties that rely on student data.

Conclusion

FERPA was originally designed to protect the privacy of students' academic records, giving parents or eligible students the right to control if and how their information is distributed. However, the ways that FERPA functions in practice—especially in the lack of meaningful enforcement mechanisms and loopholes that allow institutions to disclose student records without informing students or getting their consent—tip the balance of power towards institutions and decrease the effectiveness of protections on individual students' records. With the development of big data and learning analytics, it is easier to collect, share, and analyze student data, and the demand to share that data and the insights gleaned from it is increasing. Learning analytics have useful pedagogical potential, but big data is big business for many third parties, and FERPA does little to give students input or choice in how their records are shared and used in this situation.

Because there are still many legal and ethical issues to be resolved around the use of student data in learning analytics, and FERPA is unable to address many of those issues around current uses of student data, it is imperative that students are able to protect their own data until some of the larger policy issues can be resolved. The ability to protect and control their own academic records requires students to understand the current system of how records are protected, created, shared, and governed. Without a basic understanding of how their academic data is collected and used, and of the policies in place to facilitate and regulate such collection and use, students will not be able to take meaningful action to protect their own data or advocate for changes to be made.

The available evidence does not point to a level of awareness or understanding that would allow students to take control over their own data. The limited research that has been done in this area suggests that many students are not very concerned about their privacy in general, though they may be willing to hypothetically share some of their data with learning analytics systems, and they do not understand the laws designed to protect their privacy and their rights guaranteed by those laws. This lack of awareness of and guidance from FERPA present an opportunity for institutions of higher education to help students become more digitally literate and autonomous in controlling and protecting their own data, but without further research on exactly what students understand, it is difficult to plan for such education.

However, these suggestions about students' understanding of their FERPA rights are largely speculative. They are based on limited research done on this specific issue and similar, more extensive research done on related issues. More research needs to be conducted on how students actually think about their academic records, privacy, and FERPA; a study similar to Dowding's 2011 project should be conducted in the United States to gain an understanding of student perception of how their academic records are collected, used, and protected. In an age in which privacy is continually questioned and threatened, it is imperative that educational institutions understand how students view their privacy. Institutional understanding informs what can be done to educate students on their legal rights to prepare them to make informed choices about their privacy for the rest of their lives.

References

Arnold, Kimberly E. and Niall Sclater. 2017. "Student Perceptions of Their Privacy in Learning Analytics Applications." *Proceedings of International Learning Analytics and Knowledge Conference*. doi: 10.1145/3027385.3027392.

Bryce, Jo and James Fraser. 2014. "The Role of Disclosure of Personal Information in the Evaluation and Trust in Young Peoples' Online Interactions." *Computers in Human Behavior* 30 (2014): 299-306.

Daggett, Lynn M. 2008. "FERPA in the Twenty-First Century: Failure to Effectively Regulate Privacy for All Students." *Catholic University Law Review* 58 (59): 59-114.

Dawson, Shane. 2006. "The Impact of Institutional Surveillance Technologies on Student Behavior." *Surveillance and Society* 4 (1/2): 69-84.

Dowding, Martin R. 2011. "Interpreting Privacy on Campus: The Freedom of Information and Personal Privacy and Ontario Universities." *Canadian Journal of Communication* 36: 11-30.

Elliot, Teressa L., Darius Fatemi, and Sonia Wasan. 2014. "Student Privacy Rights—History, *Owasso*, and FERPA." *Journal of Higher Education Theory and Practice* 14 (4): 34-47.

Executive Office of the President. 2014. *Big Data: Seizing Opportunities, Preserving Values*. Washington, DC: The White House. Accessed June 29, 2017. https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf.

"FERPA General Guidance for Students." 2015. *U.S. Department of Education*. Last modified June 26. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html.

Gonzaga University v. Doe. 536 U.S. 273 (2002).

"Gramm-Leach-Bliley Act." 2015. *Federal Trade Commission*. Last modified September 4. https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

Griswold v. Connecticut. 381 U.S. 479 (1965).

Hargittai, Eszter and Alice Marwick. 2016. "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy." *International Journal of Communication* 10: 3737-3757.

Humphries, Stephanie. 2008. "Institutes of Higher Education, Safety Swords, and Privacy Shields: Reconciling FERPA and the Common Law." *Journal of College and University Law* 35 (1): 145-216.

Ifenthaler, Dirk and Clara Schumacher. 2016. "Student Perceptions of Privacy Principles for Learning Analytics." *Educational Technology Research and Development* 64 (5): 923-938. doi: 10.1007/s11423-016-9477-y.

Johns, Steven and Karen Lawson. 2005. "University Undergraduate Students and Library-Related Privacy Issues." *Library and Information Science Research* 27 (4): 485-495. doi: 10.1016/j.lisr.2005.08.006.

Khatcheressian, Laura. 2003. "FERPA and the Immigration and Naturalization Service: A Guide for University Counsel on Federal Rules for Collecting, Maintaining, and Releasing Information about Foreign Students." *Journal of College and University Law* 29 (2): 457-484.

Langenderfer, Jeff and Miyazaki, Anthony D. 2009. "Privacy in the Information Economy." *The Journal of Consumer Affairs* 43 (3): 380-388. doi: 10.1111/j.1745-6606.2009.01152.x.

Larose, Robert and Nora J. Rifon. 2007. "Promoting i-Safety: Effects of Privacy Warnings and Seals on Risk Assessment and Online Privacy Behavior." *The Journal of Consumer Affairs* 41 (1): 127-149. doi: 10.1111/j.1745-6606.2006.00071.x.

Madden, Mary, Lee Rainie, Kathryn Zickuhr, Maeve Duggan, and Aaron Smith. 2014. "Public Perceptions of Privacy and Security in a Post-Snowden Era." *Pew Research Center*. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

Milne, George R. and Mary J. Culnan. 2004. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices." *Journal of Interactive Marketing* 18 (3): 15-29. https://doi.org/10.1002/dir.20009.

O'Donnell, Margaret L. 2003. "FERPA: Only a Piece of the Privacy Puzzle." *Journal of College and University Law* 29 (3): 679-718.

Pardo, Abelardo and George Siemens. 2014. "Ethical and Privacy Principles for Learning Analytics." *British Journal of Educational Technology* 45 (3): 438-450. doi: 10.1111/bjet.12152.

Prinsloo, Paul and Sharon Slade. 2015. "Student Privacy Self-Management: Implications for Learning Analytics." *Proceedings of the Fifth International Conference on Learning Analytics and Knowledge*: 83-92. doi: 10.1145/2723576.2723585.

Proctor, Robert W., M. Athar Ali, and Kim-Phuong L. Vu. 2008. "Examining Usability of Web Privacy Policies." *International Journal of Human-Computer Interaction* 24 (3): 307-328. doi: 10.1080/10447310801937999.

Rainie, Lee and Janna Anderson. 2014. "The Future of Privacy, Elaborations: More Expert Responses." *Pew Research Center*. http://www.pewinternet.org/2014/12/18/elaborations-more-expert-responses-4/.

Rotenberg, Marc and Khaliah Barnes. 2013. “Amassing Student Data and Dissipating Privacy Rights.” *Educause Review* 48 (1): 56-57.

Rubel, Alan and Kyle M. L. Jones. 2016. "Student Privacy in Learning Analytics: An Information Ethics Perspective." *The Information* Society 32 (2): 143-159. doi: 10.1080/01972243.2016.1130502.

Sclater, Niall, Alice Peasgood, and Joel Mullan. 2016. *Learning Analytics in Higher Education*. Bristol, UK: Jisc, 2016. https://www.jisc.ac.uk/reports/learning-analytics-in-higher-education.

Slade, Sharon and Paul Prinsloo. 2013. "Learning Analytics: Ethical Issues and Dilemmas." *American Behavioral* Scientist 57 (10): 1510-1529. doi: 10.1177/0002764213479366.

Slade, Sharon and Paul Prinsloo. 2015. "Student Perspectives on the Use of their Data: Between Intrusion, Surveillance and Care." *European Journal of Open, Distance and E-Learning* Best of EDEN RW8: 16-28. http://www.eurodl.org/index.php?p=special&sp=articles&inum=6&abstract=672&article=679.

Sidbury, Benjamin F. 2003. "*Gonzaga University v. Doe* and Its Implications: No Right to Enforce Student Privacy Rights Under FERPA." *Journal of College and University Law* 29 (3): 655-678.

Soffer, Tal and Anat Cohen. 2014. “Privacy Perceptions of Adolescents in a Digital World.” *Bulletin of Science, Technology, and Society* 34 (5-6): 145-158. doi: 10.1177/0270467615578408.

Tene, Omar and Jules Polonetsky. 2013. "Big Data for All: Privacy and User Control in the Age of Analytics." *Northwestern Journal of Technology and Intellectual Property* 11 (5): 239-274.

Warren, Samuel D. and Brandeis, Louis D. 1890. “The Right to Privacy.” *Harvard Law Review* 4 (5): 193-220.

Wasson, Jennifer C. 2003. "FERPA in the Age of Computer Logging: School Discretion at the Cost of Student Privacy?" *North Carolina Law Review* 81: 1348-1374.

Youn, Seounmi. 2005. “Teenagers’ Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach.” *Journal of Broadcasting and Electronic Media* 49 (1): 86-110. doi: 10.1207/s15506878jobem4901_6.

Young, Elise. 2015. "Educational Privacy in the Online Classroom: FERPA, MOOCs, and the Big Data Conundrum." *Harvard Journal of Law and Technology* 28 (2): 549-592.

Zeide, Elana. 2016. "Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPS." *Drexel Law Review* 8 (339): 338-394.