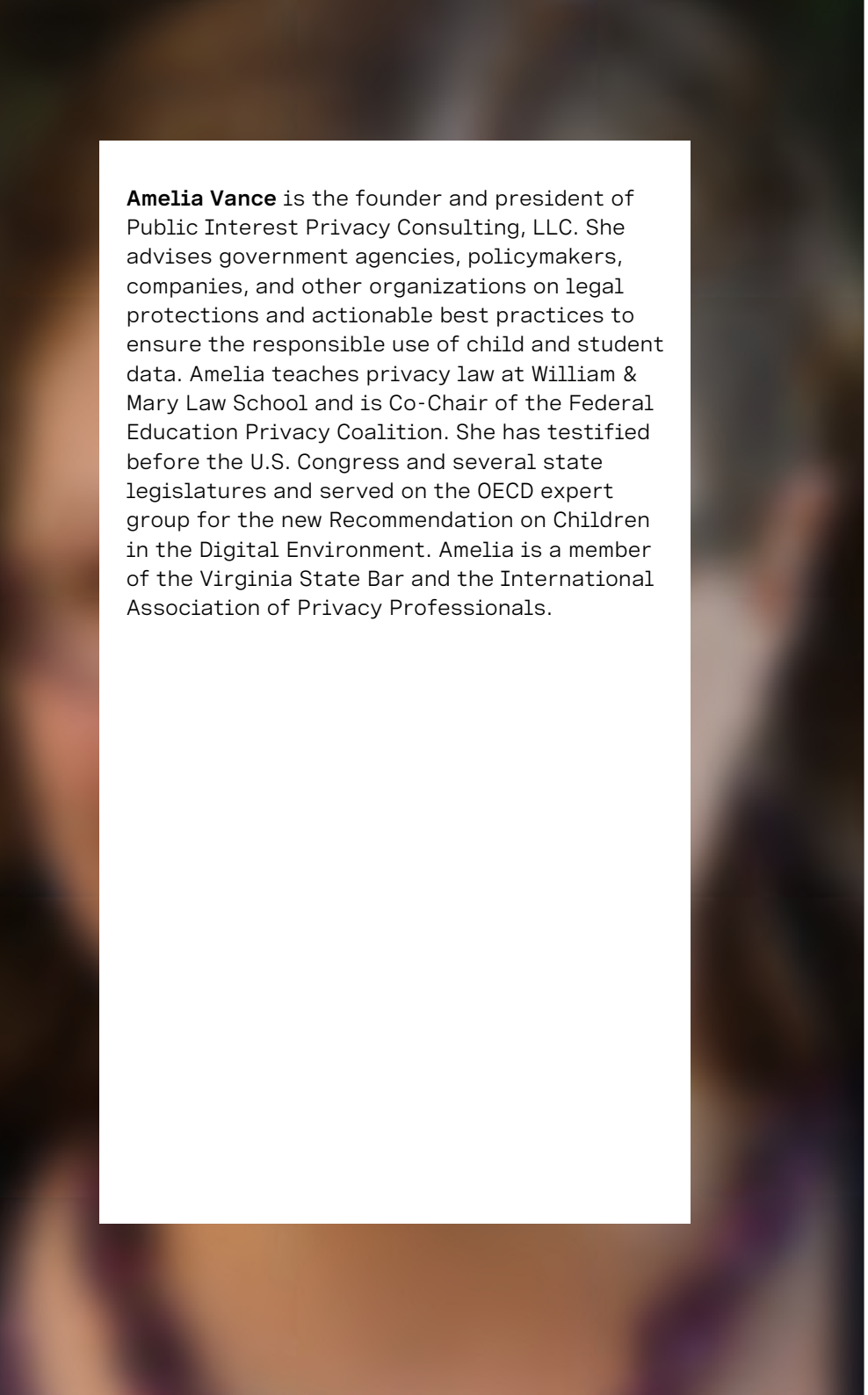

Amelia Vance is the founder and president of Public Interest Privacy Consulting, LLC. She advises government agencies, policymakers, companies, and other organizations on legal protections and actionable best practices to ensure the responsible use of child and student data. Amelia teaches privacy law at William & Mary Law School and is Co-Chair of the Federal Education Privacy Coalition. She has testified before the U.S. Congress and several state legislatures and served on the OECD expert group for the new Recommendation on Children in the Digital Environment. Amelia is a member of the Virginia State Bar and the International Association of Privacy Professionals.

Lessons learned from the Family Educational Rights and Privacy Act

Amelia Vance, Public Interest Privacy Consulting†

For decades, the Family Educational Rights and Privacy Act (FERPA) was one of the only laws in the world created to protect student privacy. Passed in 1974, it was one of the earliest privacy laws passed in the USA. This essay offers an overview of FERPA, including why it was developed, its provisions, its application to K-12‡ schools, its strengths and limitations, how it works in practice, and how it can be improved. The goal is to learn lessons from FERPA and provide best practices for other countries considering new student privacy protections.

The advent of FERPA: a necessary law amid government scandal

FERPA came shortly after the 1972 Watergate scandal in the USA, in which President Richard M. Nixon's administration was caught wiretapping and stealing documents from the Democratic National Committee's offices and subsequently attempted to cover it up. According to the bill's sponsor,

† The author thanks Stephen Hardy, Ashleigh Imus, Katherine Sledge and Elana Zeide for their assistance on this essay.

‡ The US equivalent of primary and secondary education in the UK.

Senator James Buckley, the Watergate scandal 'underscored the dangers of Government data gathering and the abuse of personal files, and ha[s] generated increased public demand for the control and elimination of such activities and abuses' (120 Cong. Rec. 14580, 1974). In addition, around this time, states and schools had begun to adopt computerised record systems (120 Cong. Rec. 13953-13954, 1974). Few school systems had policies on the use or disclosure of student records by school personnel (Wheeler, 1976, p. 49) or policies about access to records by third parties (p. 56). Student records were broadly shared with local, state and federal law enforcement, but parents (including caregivers) and students were more likely to be denied access to their records than any other stakeholder (Wheeler, 1976, p. 56). To combat these harms and abuses, Senator Buckley introduced FERPA to 'restore parental rights and to protect privacy'.

The lack of student data policies in US public schools indicated the need for a student privacy law, but the fraught political context and rapid passage of FERPA led to unintended consequences, necessitating several amendments to the law early on. Thus, although FERPA outlines key protections for students' data, gaps have always existed in its provisions.

FERPA provisions

As the law is written, FERPA guarantees parents or guardians and eligible students (generally defined as students over 18) access to their education record and the right to challenge information in those records as inaccurate or no longer relevant. It also intends to prevent unauthorised disclosure of education records without consent, with a few exceptions. The law requires certain safeguards in the absence of parental consent, such as the responsibility for schools acting as data controllers to oversee and have substantive control of their data processors, strict limitations on further processing of data beyond the original purpose, and legal contracting requirements.

Some student privacy advocates claim that FERPA's exceptions undercut the law's protections, because schools frequently use these exceptions to process student data instead of obtaining parental consent (e.g., Electronic Privacy Information Center, 2011, pp. 7, 13; Reidenberg et al., 2013, pp. 61). Advocates also argue that FERPA's exceptions do not have sufficient privacy governance requirements and protections (e.g., Electronic Privacy Information Center, 2011, pp. 7, 13; Reidenberg et al., 2013, pp. 61). These perceptions are not entirely accurate - FERPA exceptions to consent require documentation and safeguards. However, these requirements do not always translate well into practice. For example, the audit and evaluation exception - often described by advocates as being overly broad and not inclusive of necessary privacy protections and data-sharing restrictions (Electronic Privacy Information Center, 2011, pp. 10-13) - has incredibly detailed data governance documentation requirements, more than are required under any of FERPA's other exceptions (US Department of Education, 2015). In practice, FERPA is confusing, poorly understood and almost impossible for schools to follow, especially at a time when schools routinely share information with third party companies.

The next section explains the value of a law dedicated to student privacy and the complexities and problems that have arisen in FERPA's implementation.

FERPA: best practice and lessons learned

The value of a student privacy-specific law

The USA has traditionally approached privacy from a sectoral perspective, with laws that govern particular types of information. Legislators singled out student privacy for standalone legislation for three primary reasons:

1. **Students are required to attend school**. Parents are required to send their children to school and students are required to participate. Most school activities generate data. Because parents and students usually have no choice about having their sensitive data processed by schools, additional privacy protections are appropriate.

2. **Data collected by schools is generally about and from children**. Children are uniquely vulnerable to privacy harms and need additional protections.

3. **Data processing is an integral part of school responsibilities**. FERPA's exceptions exist because schools cannot operate without processing a significant amount of data about and from their students, so parental consent or opt-out is often not feasible. For example, obtaining parental consent every time teachers record attendance is unnecessary and cumbersome. To effectively educate students, schools must evaluate and track what students know and 'how quickly [they] are able to grasp new ideas or acquire new skills' (Wheeler, 1976, p. 29). It is also vital for schools to track student allergies, grades, test scores, parental contact information and custody status, as well as other data to audit whether students and families from marginalised communities are treated equitably to identify areas for improvement. For example, the US Department of Education (2016) collected and analysed such data and found that students of colour and students with disabilities endure higher rates of discipline in public schools compared to their white counterparts. The collection of this data has led to greater awareness and new initiatives to correct disproportionate rates of punishment (e.g., Amos & Manley, 2019).

Having a standalone federal student privacy law raises awareness of the sensitive nature of student information. It codifies the fundamental rights that parents and students should have when they cannot consent to data processing, although those fundamental rights may not adequately protect student privacy. Because the USA does not have an underlying data protection law, data not covered by FERPA may lack any legal protections. For example, when data is independently collected in schools by a law enforcement officer and not shared with school staff, that data is generally not covered by FERPA and could be broadly shared and not subject to access requests and other rights (US Department of Education, 2019, pp. 14-15).

Problems with reactive laws

As noted, however, FERPA also arose in part as a reaction to the Watergate scandal and to growing public concern about schools' unregulated collection of student data. For example, one widely shared magazine article, 'How secret school records can hurt your child', described how a black father discovered 'five pages of notes about his and his wife's "political activity"' in his child's record, and another case where parents were told their child would not be able to attend graduation ceremonies because her record showed she was a 'bad citizen' and were then refused access to the record explaining why (Divoky, 1974, as cited in 120 Cong. Rec. 13953-13954, 1974). Reacting to these concerns, legislators rapidly debated and passed the law, despite concerns raised during the short debate about the potential unintended consequences of ambiguous language in the law (120 Cong. Rec. 14579-14597, 1974).

For example, Senator Alan Cranston, of California, described the law's language as 'breathtaking in its sweeping generalities', arguing that the law 'could undermine attendance laws by allowing parents to refuse to have their child attend a class' whose content parents found objectionable (120 Cong. Rec. 14595, 1974). Other legislators pointed to the bill's 'strict limitations on sharing personal data, such as requiring a court order prior to sharing student information with law enforcement, and confusing regarding disclosing information to postsecondary institutions for financial aid' (Vance & Waughn, 2019, p. 523). Most of these and other concerns remained unaddressed before the law's passage (p. 524).

Thus, partly as a result of this context, framing and legislative process, FERPA is primarily a records management law, and not necessarily a privacy or data protection law; it was reactive and too focused on parental rights and consent as the primary mechanism for disclosure.

Consent as the cornerstone of FERPA

Consent is a key element of FERPA, the primary way that information can be disclosed. However, nearly 50 years after the law's passage, it is clear that parental consent as it currently exists is inadequate and ill suited to protect education data. Even when student information is disclosed

with parental consent, there are still serious privacy implications because consent removes all FERPA protections, including requirements for the use, minimisation, and sharing of data. Schools need to process data, and it is valuable, and sometimes essential, for them to use technology to do so. Most parents do not have time to investigate the privacy policies and practices of every educational technology (EdTech) product used by their children in school. When parents receive a consent form from the school to use EdTech, they likely lack the time and expertise to understand the rights and protections they are signing away, and they may assume that the school has already vetted the product. FERPA would be improved if there were underlying, unwaivable protections, such as those in the General Data Protection Regulation (GDPR) - the sale of student data and targeted advertising to children should generally not be waivable via consent, for example.

Confusion and misinterpretation of FERPA

Unfortunately, despite numerous minor amendments to FERPA, there continues to be confusion about when schools can disclose information without consent. FERPA is a complicated law, and the answer to most questions about FERPA is, 'it depends'. For example, data collected by law enforcement in school is sometimes unprotected under FERPA and sometimes absolutely protected, depending on who is collecting the data, the capacity they are acting in, how the data is collected and who it is shared with (US Department of Education, 2019, pp. 14-15). With that many factors to analyse, it is unsurprising that many public school districts do not know about, misunderstand or fail to adhere to their privacy obligations, in part because they cannot afford legal counsel with expertise in privacy law. Due to the general lack of legal requirements for data collection in the USA, many companies in the education market are also unaware of, or misunderstand, student privacy requirements.

Moreover, judicial interpretations of FERPA over the years have further muddied the waters. For example, in 2002, the US Supreme Court found that peer grading was allowed under FERPA, stating that a homework assignment was not part 'education record' until it was turned in to the teacher to grade

(*Owasso Independent School District No. I-011 v. Falvo*). That decision was more practical than strictly adhering to the law: no one wanted to ban peer grading, and a school should not be expected to protect data before it is in their control, such as a paper on a student's computer. However, in many modern applications there is no clear distinction between in-progress and completed assignments, since student work is often performed in cloud-based software owned and accessible by the school at any point during the process. This Supreme Court ruling creates confusion about whether these in-progress assignments are protected by FERPA. This decision also allowed for a level of plausible deniability that student information was protected by FERPA until it was provided to the school.

Direct governance of third parties

As originally passed, FERPA foresaw the growth of digital records and, to an extent, regulated data sharing with third parties. However, the original drafters did not anticipate the extent to which private companies handle student data from schools. As EdTech use grew in the USA, there was confusion and ambiguity about which data was protected under FERPA, and whether there was any direct liability for companies mishandling it.

Under FERPA's school official exception, schools can share information with companies that:

- Do something that a school would otherwise use employees to do
- Are under schools' 'direct control'
- Do not use student information for additional purposes or share it further (34 CFR 99.31(a)(1)(i)(B)).

However, legal ambiguity and practical implementation challenges keep these FERPA protections from adequately protecting student information. For example, prior to 2014, many companies placed the onus of FERPA compliance on schools, despite a little-known potential punishment in FERPA: the US Department of Education can impose a five-year ban on third parties that violate the law (34 CFR § 99.67). However,

few, if any, companies were aware of this potential penalty (especially since the penalty has never been imposed). State policymakers found passing all legal obligations on to schools to be unacceptable, and began to pass laws with specific requirements and restrictions that companies must adhere to. These laws generally prohibited targeted advertising to students and the creation of student profiles for non-educational purposes; an acknowledgement that the school is the sole data controller (to use GDPR terminology); and limits on redisclosure of student data. These laws helped to lessen the power discrepancy between schools and companies, creating better privacy protections overall, and made it clear that companies must also be proactive regarding student privacy responsibilities.

Regulation of school use

FERPA limits how schools can use and share data internally without consent in daily educational encounters: the school must 'use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests' (34 CFR 99.31(a)); therefore, FERPA requires some level of access control. Schools must also explain, in an annual notice to parents, how they define 'legitimate educational interests'. However, the definition adopted by most schools is a catch-all that does not limit school discretion (Zeide, 2017, p. 515).

As privacy scholar Elana Zeide discusses, this limitation may not sufficiently serve the privacy and best interests of students since 'education purpose limitations equate educational functions with acceptable use' (2017, p. 515). Institutional interests could differ from student interests when it comes to the amount of information collected and retained in the first place. Schools - and the EdTech companies they partner with - can sometimes make better and more informed decisions when they have as much data as possible about a student's educational and non-educational experiences; assuming that all parties objectively act with a student's best interests in mind, having as much information as possible can allow more accurate and informed tailoring of curricular material, counselling and mentoring of students, and the overall wellbeing of students. But children may also become less willing to learn if they know that everything they do will be watched and retained (Zeide, 2017, p. 517).

Over-collection of data can also cut 'against the norms that early mistakes should not foreclose future opportunities', and as children mature, could limit their future opportunities (Zeide, 2017, p. 520). What school personnel may consider the best interests of the student body could actually be contrary to the best interests of an individual student: 'the wellbeing of the majority of students - the students who use the fewest resources and need the fewest interventions - may be prioritised over students with disabilities and students of lower socioeconomic status, who may need more resources and attention' (Selinger & Vance, 2020, pp. 42-43). School personnel may have biases related to students from marginalised populations or based on inaccurate beliefs about what a student's prior behaviour means about their future. Student privacy laws, such as FERPA, must include better guardrails to protect students when institutional interests may conflict with students' best interests.

Policymakers should also consider whether there is some collection or use of data that schools should not undertake at all because of the potential for privacy risks, inequities or abuse. For example, there are significant concerns in the USA regarding monitoring student use of the internet or activity on school devices for self-harm. While preventing self-harm is vital, the efficacy of these services is questionable; these services 'could exacerbate feelings of stigma and shame and could ultimately make students less likely to ask for help' and 'undercut the trust of students not only in their school generally but in their teacher [and] counselors' (Keierleber, 2021). The surveillance has also been criticised as it could prime students 'to accept surveillance as an inevitable reality', causing them to give up 'the ability to explore new ideas and learn from mistakes' (Keierleber, 2021).

In some cases, identification of a student's mental health crisis - whether accurate or not - can cause more harm than help (see The Southern Poverty Law Center, 2021; Vance et al., 2021). When extremely sensitive data is collected and used for purposes that could have a significant impact on a child's

life, wellbeing and future opportunities, additional privacy protections and restrictions should be incorporated into law to mitigate potential harms.

Training requirements are essential

Why should schools adhere to privacy protections in the first place? Many US schools reflect an overarching lack of understanding about why student data requires significant protection, with the exception of obviously sensitive information like medical data, special education services or a parent's financial data. Without proper training on the value of student data protection, school personnel cannot make informed decisions about data processing or the adoption of EdTech tools.

This is particularly important when teachers adopt new EdTech. After all, most apps may seem to only collect a student's name and email and their activity in the app, so teachers may ask why this is a privacy problem. If the only answer that school districts can provide is 'this is legally required', many teachers will choose to do what they think is best for their students' learning regardless of legal privacy protections. In many cases, this risk analysis may be accurate. However, teachers may not be aware of several factors that raise the risk level; for example, companies may sell data about student activity, which could lead to a student who is bad at maths receiving an ad in the future encouraging them to take out an exploitative loan.

Even seemingly innocuous information poses a threat to students: for example, releasing the name of a student who is involved in a domestic violence situation could alert an abusive parent to the student's location. And, of course, the information collected by EdTech can be far broader than just a name, email, and app activity; teachers might connect the app with the school's electronic student record system, and the app could then receive some or all of the record - including sensitive data, such as disabilities and disciplinary records - even though the app does not require that information.

Unfortunately, FERPA does not include a training requirement, and the federal and state governments provide little-to-no voluntary training. A survey from the advocacy group Common Sense Media found that 'only 25 percent of teachers who received professional development to support their use of educational technology were trained to understand student data privacy requirements and strategies' (Mandinach & Cotto, 2021, summarising Common Sense Media, 2019). Not only do most school personnel not know about the legal requirements; they also do not know why they should care about privacy protection in the first place. Similarly, companies may also not understand privacy risks and how the information they collect could be harmful. This lack of understanding leads them to deprioritise privacy, especially when they believe that the service they provide will be a net good in helping students.

Enforcement issues related to transparency

FERPA is often considered toothless. The US Department of Education has never imposed the law's ultimate penalty on any school - complete removal of all federal funds (of course, no one wants to take away education funds used to serve children). This is largely because FERPA requires the Department to work with schools before withdrawing funds, and schools understandably comply with the agency's conditions.

The US Department of Education should be more transparent about its FERPA enforcement since most FERPA complaints are not resolved publicly. This lack of transparency creates the impression that FERPA does not adequately protect student privacy. Publishing aggregate information, such as the number of in-process complaints, how long it takes to process them and which issues frequently arise, would promote public trust.

Conclusion

Other jurisdictions crafting their own student privacy laws can find value in considering lessons learned from FERPA. A standalone student privacy law allows policymakers to consider education's unique facets, such as parents' and students' lack of ability to consent. However, unlike FERPA, new laws should be created proactively, with thorough consideration of the relevant privacy problems and consultation of diverse stakeholders such as educators, parents and students

themselves. A new student privacy law should be clearly written and mitigate privacy harms without unduly burdening school systems. It should include data minimisation, training for educators and transparent enforcement methods that put the onus of protecting student data on third parties, as well as work in conjunction with more general privacy laws.

In addition to looking at FERPA, international policymakers considering these laws could benefit from examining student privacy laws passed in US states over the past decade (Vance, 2016). These were largely passed due to perceived FERPA weaknesses - for example, by adding direct regulation of third parties that receive student information - and could therefore serve as a better template for new student privacy laws.

Even with these state laws supplementing FERPA, the USA's student privacy protections still need improvement. Schools should consider the best interests of each student, and weigh the risk of certain data processing against potential benefits. Legal requirements should prevent over-surveillance and data hoarding. Enforcement processes need to be more robust and transparent.

Regulating student privacy is difficult. There are great benefits and needs met by processing student data, but also many risks. A nuanced approach, built with feedback from stakeholders, is necessary to ensure effective student privacy protections.

120 Cong. Rec. 9371 (1974).

120 Cong. Rec. 13953-13954 (1974).

120 Cong. Rec 14579-14597 (1974).

34 CFR 99.31(a).

34 CFR § 99.67.

Amos, L., & Manley, M. (2019) Using data to identify and address inequities in school discipline. Mathematica Blog, 22 October

Common Sense Media. (2019). *The Common Sense census: Inside the 21st-century classroom* (pp. 45-46)

Divoky, D. (1974). How secret school records can hurt your child. Parade, 31 March. As cited in 120 Cong. Rec. 13953-13954 (1974)

Electronic Privacy Information Center. (2011). Comments to the Department of Education, 'Notice of Proposed Rulemaking', RIN 1880-AA86. 23 May

Keierleber, M. (2021). An inside look at the spy tech that followed kids home for remote learning - and now won't leave. The 74, 14 September

Mandinach, E. B., & Cotto, J. (2021). The case for including data privacy and data ethics in educator preparation programs. *Future of Privacy Forum*, 5 October

Reidenberg, J., Russell, N. C., Kovnot, J., Norton, T. B., Cloutier, R., & Alvarado, D. (2013). *Privacy and cloud computing in public schools*. Fordham Center on Law and Information Policy

Selinger, E., & Vance, A. (2020). Teaching privacy and ethical guardrails for the AI imperative in education. *Future EDge, NSW Department of Education, 3*, 30-53

Southern Poverty Law Center, The (2021). *Costly and cruel: Thousands of Florida children suffer the harm and indignity of involuntary, and often illegal, commitment to psychiatric facilities*

Vance, A., & Waughn, C. (2019). Student privacy's history of unintended consequences. *Seton Hall Legislative Journal, 44*(3), 515-557

Vance, A., Collins, S., Park, J., Reddy, A., & Sharifi, Y. (2021). The privacy and equity implications of using self-harm monitoring technologies. Future of Privacy Forum, 27 September

US (United States) Department of Education. (2015). *The Family Educational Rights and Privacy Act: Guidance for reasonable methods and written agreements*

US Department of Education. (2016). *School climate and discipline: Know the data*

US Department of Education. (2019). *School resource officers, school law enforcement units, and the Family Educational Rights and Privacy Act (FERPA)*

Wheeler, S. (1976). *On record: Files and dossiers in American life*. Transaction Books.

Zeide, E. (2017). The limits of education purpose limitations. *University of Miami Law Review, 71*(2), 494-515