STUDENT PRIVACY'S HISTORY OF UNINTENDED CONSEQUENCES

Amelia Vance and Casey Waughn[1]

I. INTRODUCTION

It is difficult to imagine a world in which schools cannot print students'

[1] Amelia Vance is the Director of Youth & Education Privacy at the Future of Privacy Forum, a nonprofit organization focused on emerging consumer privacy issues. Casey Waughn is a 3L at Washington University School of Law and a student contractor for the Future of Privacy Forum. The authors would like to thank the following individuals for their help and support with this publication and its various iterations: Sara Collins, Keith Earls, Ashleigh Imus, Mariam Khan, Jasmine Park, Tyler Park, Anisha Reddy, Alexis Shore, and Katherine Sledge.

names on the honor roll or in school playbills; announce student athletes' names, heights, and weights at the start of a game; and share financial aid information with appropriate institutions to ensure that students can finance their education. Yet, in the months following the enactment of the Family Educational Rights and Privacy Act (FERPA) of 1974, and forty years later in the wake of more than one-hundred new state student privacy laws, schools at all levels have struggled with the scope of new student privacy mandates. These mandates have raised questions about the schools' ability to perform long-standing functions.

The student privacy legal landscape over the past forty-five years tells a story of unintended consequences that have required legislative clarifications and changes. The story makes a case for nuance and careful deliberation in drafting laws, but also for creating a long-term culture of privacy that addresses real or potential harms, rather than responding to unfounded fears. Accordingly, this article examines the passage of the first major U.S. privacy law, FERPA. The article will address the initial questions FERPA raised as well as the concerns that prompted more than one-hundred new student privacy laws forty years after FERPA's passage and the unintended consequences of those laws. By analyzing the lessons from FERPA's first amendment and changes in recent student privacy laws, the article proposes strategies to avoid certain unintended consequences in privacy legislation. The evidence is derived from case studies of student privacy laws in Louisiana, Virginia, New Hampshire, and Connecticut, where significant unintended results of these laws occurred, prompting their amendment. The lessons from these cases also apply to wider current debates as the U.S. creates broad consumer privacy protections, including new and expanded privacy protections for children.

II. FERPA AND ITS FIRST AMENDMENT

A. The Landscape Before FERPA

FERPA was not subject to the scrutiny of committees or hearings before its passage into law because it was originally offered on the Senate floor as a rider to a broader education bill.[2] Its legislative history was largely post-dated, cobbled together from speeches and debates in Congress that occurred after it passed.[3] As FERPA was the first legislation that contemplated student privacy, both the original act and its first amendment are largely considered the birth of federal privacy rights for students.[4] On a

---

2 *See* 120 CONG. REC. 14579-95 (1974).

3 *See infra* Section B.

4 *See* SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 249-55 (2018).

larger scale, however, FERPA and its first amendment also demonstrate how unintended consequences have plagued the student privacy sphere since the inception of educational privacy rights.

The period leading to FERPA's enactment in August 1974 was fraught with concerns about government secrecy.[5] In the aftermath of Watergate and the disclosure of secret FBI files on U.S. citizens, including members of Congress, public trust in the government was at an all-time low.[6] Prior to his resignation, in his last State of the Union address, President Nixon said:

> As technology has advanced in America, it has increasingly encroached on one of those liberties that I term the right of personal privacy. Modern information systems, data banks, credit records, mailing list abuses, electronic snooping, the collection of personal data for one purpose that may be used for another—all these have left millions of Americans deeply concerned about the privacy they cherish. The time has come, therefore, for a major initiative to define the nature and extent of the basic rights of privacy and to erect new safeguards to insure [sic] that those rights are respected.[7]

Policymakers and the public began to express concerns about large government and business repositories containing personal information,[8] including repositories kept by schools.

In 1969, sociologists from the Russell Sage Foundation conducted a study of record-keeping practices in fifty-four elementary and secondary schools in twenty-nine states.[9] They found that the records contained a great deal of sensitive information, including student grades, attendance records, personality ratings, informal teachers' notes, and student diaries.[10] The study found that school personnel did not consistently maintain records.[11] Several of the districts surveyed also provided law enforcement—including juvenile courts, CIA, and FBI officials—with unfettered access to student records but prohibited parents from accessing the same information.[12]

---

5 *See id.* at 249–255.

6 *Id*. at 249.

7 H.R. REP. NO. 93-7, at 9345 (1974).

8 *See* IGO, *supra* note 4.

9 *See generally* David Goslin & Nancy Bordier, *Record-Keeping in Elementary and Secondary Schools*, *in* ON RECORD: FILES AND DOSSIERS IN AMERICAN LIFE, at 29–69 (Stanton Wheeler ed., 1969) [hereinafter "Goslin & Bordier Study"].

10 H.R. REP. NO. 93-7, at 9633–53 (1974).

11 S. REP. NO. 93-27, at 36528–31 (1974).

12 Goslin & Bordier Study, *supra* note 9, at 29–69; *see also* Russell Sage Foundation, *Guidelines for the Collection, Maintenance, and Dissemination of Pupil Records: Report of a Conference on the Ethical and Legal Aspects of School Record Keeping* 31 (1969)

In the same year, the Sage Foundation also convened a conference that produced a report titled "Guidelines for the Collection, Maintenance and Dissemination of Pupil Records."[13] The Guidelines produced by the conference noted that schools generally collected information in student records without obtaining informed consent, and even when consent was obtained, information was "often used subsequently for other purposes."[14] The Guidelines also noted that students and parents generally had "little or, at, best, incomplete knowledge" of existing information and how schools used it, and there were no formal procedures for parents to discover and challenge inaccurate information.[15]

The report heavily criticized schools for "few provisions . . . to protect school records from examination by unauthorized school personnel" and for the lack of formal policies for access to records by "law-enforcement officials, the courts, potential employers, colleges, researchers, and others." The report called this state of affairs "a serious threat to individual privacy in the United States," and guidelines for record-keeping were distributed to schools nationwide.[16] Three years later, the Sage Foundation revisited school policies and found that "the vast majority of schools in this country still do not have records policies that adequately protect the privacy of students and their parents," and that even when policies existed, school employees did not clearly understand when those policies applied to them.[17]

In 1973 and 1974, Diane Divoky gained policymakers' attention by publishing multiple articles about student privacy in widely read publications such as *Parade* magazine and *The Washington Post*.[18] She explained that

[hereinafter "Guidelines"] ("Access to pupil records by non-school personnel and representatives of outside agencies is, for the most part, handled on an ad hoc basis. Formal policies governing access by law-enforcement officials, the courts, potential employers, colleges, researchers and other do not exist in most school systems.").

13 Guidelines, *supra* note 12.

14 Guidelines, *supra* note 12.

15 Guidelines, *supra* note 12.

16 Guidelines, *supra* note 12, at 15.

17 Diane Divoky, *Cumulative Records: Assault on Privacy*, *as reprinted in* 120 CONG. REC. 36529 (1974) *and in* H.R. REP. NO. 93-7, at 9634 (1974).

18 In the 1970s, *Parade* magazine was "one of the leading Sunday supplement inserts—used by some 111 newspapers with a combined circulation of more than 19 million." Jack Doyle, *Empire Nehouse: 1920s-2010s*, THE POP HISTORY DIG (September 18, 2012), https://www.pophistorydig.com/topics/tag/parade-magazine-history/. It was extremely influential; among other indications of influence during this time period, *Parade* magazine "published interviews with virtually every major star, political leader and President since 1941," and "is credited with first proposing the idea of a 'Hot Line' between the leadership of the U.S. and the U.S.S.R. in March 20, 1960 . . . President Kennedy wrote the magazine a letter thanking it for the idea." *Facts on Parade*, PARADE, https://parade.com/about-us/. Divoky's influential *Parade* Magazine article, published on March 31, 1974, was titled, "How Secret Records Can Hurt Your Child," and also appeared in the Washington Post the Sunday before April 2, 1974. Divoky authored another influential article, "Cumulative Records:

school record-keeping, "like Frankenstein's monster, . . . now has the potential to destroy those it was created to protect." She described the makeup of this "monster" as "the swift development of modern communications technology and the widening employment of that technology by a social system increasingly bent on snooping" as well as "the emergence of education's ambitious goal of dealing with the 'whole child.'" She noted that "as the records began to contain more detailed and varied information, they took on lives of their own; they became, somehow, more trustworthy and permanent than the quixotic people they represented."

Among other disturbing anecdotes, Diane Divoky highlighted a case before the Supreme Court where the House Committee for the District of Columbia requested and then published "cumulative records of students," including "[c]opies of actual test papers, disciplinary reports and evaluations . . . with the students' names still on them."[19] She also cited cases that she had witnessed while serving on the New York City board of education. She included stories of a junior high school principal telling the secretary at a private tutoring agency who had called to ask about a child's reading level that "the child has a history of bedwetting, his mother is an alcoholic, and a different man sleeps at the home every night;" and a black father whose daughter's record noted that "his own community activities as a 'black militant' are causing his daughter to be 'to [sic] challenging' in class."[20]

Perhaps most troubling in an era of political protests and suspicions of anti-government activities was a project funded by the California Council on Criminal Justice. This project "computerize[d] and centralize[d] all juvenile records," and was a system that, under state law, recorded "children down to the age of six years who have been identified as being 'in danger of becoming delinquent,'" who could be "declared 'pre-delinquent.'"[21] Divoky noted that one of the council's related programs "instructed kindergarten teachers in sophisticated methods of identifying 'target students'—those five-year-olds whose social and academic profiles were similar to those of adolescents who ended up in juvenile courts."[22]

Assault on Privacy," which appears to have originally been published by Learning in September 1973. *See* 120 CONG. REC. 9363 (1974) (containing Rep. Kemp's statements about the article's origin). Divoky's articles were cited by Senator Buckley (NY) when he introduced FERPA, and by Congressmen Koch (NY), Edwards (CA), and McKinney (CT) as appearing in the Washington Post the Sunday before April 2, 1974. *See* S. REP. NO. 93-11, at 14580 (1974); 120 CONG. REC. 36529 (1974); H.R. REP. NO. 93-7, at 71, 84, 90 (1974).

[19] Divoky, *supra* note 17. The case to which Divoky referred is *Doe v. McMillan*, 402 U.S. 306 (1973).

[20] 120 CONG. REC. 36529 (1974).

[21] 120 CONG. REC. 36531 (1974).

[22] 120 CONG. REC. 36531 (1974).

Divoky posited that the most significant problem was living "in a world of technologically recorded, maintained and communicated information."[23] She cited Florida's centralized computer system that used "an IBM 1230 Optical Scanner to enter data for all pupils from the ninth grade on up into a computer."[24] She also described a school record system in Arizona allowing employees to call into a remote recording system and leave comments to create a virtual record.[25] Other employees could then play back the recordings to be transcribed and placed into students' files.[26]

Less than one week after one of Divoky's articles was published in March 1974, Congressman Jack F. Kemp (NY) cited it in a speech on the floor, noting that Congress "must come to grips with the potential abuses which can arise from the disclosure of this information," particularly because those abuses affect "everyone who has even gone to a public or private school—in other words, virtually all of us."[27] Just over a month later, Senator James L. Buckley (NY) introduced FERPA.[28]

B. FERPA's Introduction and Passage

FERPA was introduced on the Senate floor as an amendment to the Elementary and Secondary Education Act of 1974 (ESEA).[29] In his remarks, Senator Buckley said that "[t]he secrecy and denial of parental rights that seem to be a frequent feature of American education is disturbing," and cited examples from Divoky's article.[30] He further explained that, "[s]ome school administrators and educators seem to have forgotten that parents have the

[23] 120 CONG. REC. 36531 (1974).

[24] 120 CONG. REC. 36531 (1974).

[25] 120 CONG. REC. 36531 (1974).

[26] 120 CONG. REC. 36531 (1974).

[27] Rep. McKinney echoed Kemp's comments on the *Parade* article and America's new focus on privacy rights. "The American's concern over privacy stems not just from Watergate revelations—although these have enhanced our citizens' fear of 'Big Brother' Government—but has been compounded over the years for hardly a day goes by that some new outrage is not reported. For example, this past Sunday's Parade magazine carried an article relating to incredible consequences which may befall an adult merely because of records kept on him as a child in elementary school." 120 CONG. REC. 9364 (1974); 120 CONG. REC. 9633 (1974). Kemp offered his own amendment to the ESEA in the House, which sought to allow students to inspect their records and parents to inspect "experimental materials" used in the classroom. Several aspects of Kemp's amendment were made part of Buckley's amendment—which ultimately became FERPA—during the Conference Committee process. *See* 120 CONG. Rec. 26107 (Reps. Kemp and Perkins discussing aspects of Kemp's amendment which were rolled into Buckley's amendment by the Conference Committee).

[28] *See* 120 CONG. REC. 14579 (1974) (containing Buckley's original introduction of FERPA on May 14, 1974).

[29] *See* 120 CONG. REC. 14579 (1974) (containing Senate floor discussion where Buckley introduced FERPA); Pub. L. No. 93-568, 88 Stat. 1855 (1974) (containing the amendments to Elementary and Secondary Education Act including FERPA).

[30] 120 CONG. REC. 14580.

primary legal and moral responsibility for the upbringing of their children and only entrust them to the schools for basic educational purposes."[31] The amendment aimed to ensure that parents could access their children's records, and to prevent "abuse and improper disclosure of such records and personal data on students and their parents."[32] The amendment also required schools to seek parental consent before records were disclosed to third parties and before children were tested or made to participate in "experimental or attitude-affecting programs."[33] Buckley recognized that new requirements would create new administrative burdens, but stated that he was not "concerned about the workload or convenience of the educational bureaucracy but, rather, with the personal rights of America's children and their parents."[34]

Because FERPA was an add-on amendment to another proposed bill, it did not go through hearings or committees, resulting in limited legislative history.[35] This subsequently made it difficult for schools to understand the Act's basic requirements and limitations.[36] In less than one hour, Buckley introduced the amendment, and it was debated and amended multiple times

---

[31] 120 CONG. REC. 14580

[32] 120 CONG. REC. 14581.

[33] 120 CONG. REC. 14581.

[34] 120 CONG. REC. 14581.

[35] The final language of FERPA as enacted initially into law was minorly revised during the ESEA Conference Committee. Most notably, the Conference Committee added a separate "Protection of Pupil Rights," which aimed to address the experimental learning and psychological testing aspects of Buckley's bill that had failed to pass by voice vote on the Senate floor, largely due to the concerns regarding unintended consequences discussed in-text. However, the "Protection of Pupil Rights" was much narrower than Buckley's originally proposed language. The Conference Committee released a report discussing its recommendation, including a few short paragraphs about FERPA. The Conference Report was adopted by the Senate on July 24, 1974, and the House on July 31, 1974, when each house passed the ESEA. *See* 120 CONG. REC. 25472-86 (1974); 120 CONG. REC. 26106-18, 26128 (1974) (House discussing, voting on and adopting FERPA); 120 CONG. REC. 24925-26 (1974) (Senate discussing, voting on and adopting FERPA).

[36] *See Joint Statement in Explanation of the Buckley/Pell Amendment*, 120 CONG. REC. 39853 (1974) [hereinafter "Joint Statement"] ("Since the language was offered as an amendment on the Senate floor, rather than having been the subject of Committee consideration, traditional legislative history materials such as hearings and Committee reports have not been available to serve as a guide to educational institutions, to students, and to the Department of Health, Education, and Welfare in carrying out their various responsibilities under the Act."). *See also* 120 CONG. REC. 41396 (1974) (containing a Washington Post editorial titled "Second Thoughts about School Records"). Rep. Brademas also expressed concern about the lack of legislative history. "I am compelled to say, Mr. Speaker, that I am not entirely convinced that the amendments to the Family Educational Rights and Privacy Act contained in this report are sufficient to remedy all of the anomalies which may arise under that legislation. The original act was added as a floor amendment during Senate consideration of the elementary and secondary education bill earlier this year and, like the amendment contained in this report, has never been the subject of hearings or committee consideration in either body." 120 CONG. REC. 41396 (1974)

on the Senate floor. The Senate ultimately accepted the Act as part of the ESEA bill.[37]

When FERPA was introduced, many senators raised concerns about the Act's potential unintended consequences.[38] Nearly every senator who spoke acknowledged the good intent behind the proposed student privacy legislation but feared that unintended consequences would occur given the lack of formal committee debate and vetting.[39] Senators were also concerned about FERPA's vague language and restrictions on programs, including experimental programs or courses, designed to alter students' behavior and values.[40] The version of FERPA that Senator Buckley originally proposed required parental consent for students "to participate in any project, program, or course, the primary purpose or principal effect of which is to affect or alter the personal behavior or personal values of a student, or to explore and develop teaching techniques or courses primarily intended to affect such behavior and values."[41] Senator Hart asked whether this provision would apply to "the new math, which I still do not understand, but to which my children have been exposed? Could I say 'no' if we were to adopt this amendment?"[42] Senator Buckley immediately replied, "That is not at all the situation. A normal person would agree to experimentation with new math."[43] When a similar question was posed by Senator Mathais, Senator Buckley replied that of course "all education has an effect on attitude . . . I believe there is a tacit rule of commonsense that applies to the interpretation and application of all legislation."[44]

Yet, Senator Cranston argued that the legislation could undermine attendance laws by allowing parents to refuse to have their child attend a class "if, after notification, the parent finds the content of the course or

---

[37] While the bill was introduced in the Senate and added to the ESEA via voice vote in May 1974, it did not pass by both the House and Senate until July 31, 1974, after a conference committee and multiple substantive changes by both the Senate and the House. *Compare* H.R. REP. NO. 93-1211, *reprinted in* H.R. REP. NO. 93-1547 (1974) (the amendment as passed on the Senate floor in May) *with* Education Amendments of 1974, Pub. L. No. 93-380, 88 STAT. 484 (1974) (the final version of the amendment constituting FERPA).

[38] For example, Senator Pell stated, "we are concerned here not with what the Senator from New York intends the language he proposes to accomplish. It is what the language would do. This is what bureaucrats in future years will rely on, what the language in the bill is. They will not look up the debate on the floor at the time of passage of the bill." 120 CONG. REC. 14588 (1974).

[39] *See, e.g.*, 120 CONG. REC. 14582-95 (1974) (containing the statements of Senators Hart, Pell, Mathais, and Stevens).

[40] *See* 120 CONG. REC. 14595 (1974) (statements by Senator Cranston).

[41] 120 CONG. REC. 14579, 14595 (1974).

[42] 120 CONG. REC. 14588 (1974).

[43] 120 CONG. REC. 14588 (1974).

[44] 120 CONG. REC. 14582 (1974).

activity to be objectionable."[45] He characterized the language as "breathtaking in its sweeping generalities," asking:

> How do you determine in advance, and provide notification to the parent, of classroom activities that might bear on the values of a student? A course in American history, for example, that discusses contemporary American ethics in the light of Watergate could be construed as tending to "affect the personal values" of a student. Or, how do you go about discouraging violent or overly aggressive behavior without tending to "alter the personal behavior" of a student? These are serious questions, Mr. President, that we cannot take lightly. Because the penalty for even accidental transgression of these Federal directives is the total loss of Federal funding to any educational institution—public or private, preschool through postsecondary—that is found "out of compliance."[46]

While Senator Buckley further clarified the intent and limits of the provision on the floor, Senator Pell stated, "We are concerned here not with what the Senator from New York intends the language he proposes to accomplish. It is what the language would do. This is what bureaucrats in future years will rely on, what the language in the bill is."[47] Other points of contention involved the bill's strict limitations on sharing personal data, such as requiring a court order prior to sharing student information with law enforcement, and confusion regarding disclosing information to postsecondary institutions for financial aid.[48]

At least two education groups also raised concerns that were discussed in the congressional record. The National School Board Association (NSBA) was concerned that the thirty-day time frame for schools to turn over records was insufficient, and advocated forty five or sixty days, among other concerns.[49] The National Education Association (NEA), in their 1971 Code of Student Rights and Responsibilities, urged strict policies to protect students' and parents' rights to privacy.[50] The NEA thus also opposed the provision requiring parental consent for "experimental programs."[51] The opposition was heard and substantial changes were made to Buckley's

[45] 120 CONG. REC. 14594 (1974).
[46] 120 CONG. REC. 14595 (1974).
[47] 120 CONG. REC. 14588 (1974).
[48] *See, e.g.*, 120 CONG. REC. 14582, 14584, 14589 (1974) (statements of Senators Mathais and Stevens; discussion between Senator Dominick and Senator Buckley).
[49] 120 CONG. REC. 14583 (1974).
[50] 120 CONG. REC. 36529 (1974).
[51] 120 CONG. REC. 14581 (1974).

original language, including cutting the "experimental program" clause through a roll call vote.[52]

Other than brief debates in the Senate (and the House, for its iteration of the bill that was eventually folded into the Senate version) and a few brief paragraphs in the larger ESEA Conference Report,[53] very little legislative history is available from prior to FERPA's enactment that would further clarify the law's scope and intent. Because of this limited history, many relevant stakeholder groups may have known about the law only after it passed.[54]

Thus, the senators discussed several potential unintended consequences that were not addressed in the aforementioned hearings. Senator Dominick worried that the amendment would block post-secondary institutions' ability to obtain information from high schools regarding admissions or to determine whether students were eligible for loans or work-study.[55] This was due to the fact that many students begin college when they are under eighteen years old and parents may not consent to have such information shared. Senator Buckley dismissed this concern, stating, "I find it implausible that parents would not cooperate in helping a child qualify for financial help," but he also pointed out that the bill's language permitted information to be shared for financial aid purposes.[56]

Because of the numerous concerns, Senator Stevens advised further consideration: "Mr. President, I again applaud what the Senator from New York is trying to do, but I think any proposal that has to have so many amendments on the floor to try to perfect the original intent is a measure that should not be passed."[57] Senator Stevens recommended committee hearings to clarify the scope of the section that did not permit data sharing with third parties without their consent.[58]

Once FERPA was passed, and as schools continued to try to implement the law, these unaddressed concerns and others emerged repeatedly, resulting in significant confusion.

52 120 CONG. REC. 14595 (1974).

53 *See* H.R. REP. No. 93-1547 (1974); 120 CONG. REC. 25472-86 (1974).

54 *See* Joint Statement, *supra* note 36, at 39862-63. "Since the language was offered as an amendment on the Senate floor, rather than having been the subject of Committee consideration, traditional legislative history materials such as hearings and Committee reports have not been available to serve as a guide to educational institutions, to students, and to the Department of Health, Education, and Welfare in carrying out their various responsibilities under the Act." 120 CONG. REC. 41396 (1974).

55 120 CONG. REC. 14589 (1974).

56 120 CONG. REC. 14589 (1974).

57 120 CONG. REC. 14593 (1974).

58 120 CONG. REC. 14593-94 (1974).

C. Unintended Consequences in Practice

Almost immediately upon FERPA's passage, stakeholders began to question the law's applicability, its scope, and weighed in on its potential consequences. Much of the confusion regarded whether K-12 schools could continue to share routine information with various individuals and entities. Schools questioned whether they could print students' names in bulletins and read student athletes' information at sporting events, since these activities involved sharing personal information with other students, school personnel, and third parties.[59] Senator Buckley and Senator Pell's *Joint Statement in Explanation of the Buckley/Pell Amendment* echoed the schools' concerns: "A literal interpretation of this language has led school attorneys around the country to advise their clients [to] no longer routinely to print football players' weights in athletic programs and to seek written consent of the cast of the school play that their names may be printed in the program."[60] Schools also questioned whether districts were allowed to transfer students' records when students attended new schools.[61]

The permissible scope of information sharing was also an issue for colleges and graduate programs. One example pertained to student loan information, including the need to inform lenders about dates of attendance for repayment obligations.[62] A member of Congress noted, "[A] student is allowed a nine-month grace period after his last date of attendance before he is required to begin repayment of his obligation. If a school cannot routinely inform the lender of the student's last date of attendance, the lender has no basis for calculating when he may begin to collect the loan."[63] Congress also noted that groups such as the Law School Admissions Council, Educational Testing Service, and the College Entrance Examination Board "need student data in order to perform their function" of developing and validating tests used to help students gain admission to colleges and to predict their success at these institutions.[64] Educational accreditation groups similarly required student data in order to function. A narrow reading of FERPA as originally written could prevent the sharing of this data.[65]

FERPA's sharing restrictions also prompted schools to question whether they could share information with third parties in the event of a

59 120 CONG. REC. 41396 (1974) (quoting *Second Thoughts About School Records*, WASH. POST (Dec. 19, 1974), at A14) [hereinafter Washington Post Editorial]. *See also* Joint Statement, *supra* note 36, at 39863.

60 Joint Statement, *supra* note 36, at 39863.

61 Joint Statement, *supra* note 36, at 39863.

62 Joint Statement, *supra* note 36, at 39863.

63 Joint Statement, *supra* note 36, at 39863.

64 Joint Statement, *supra* note 36, at 39863.

65 Joint Statement, *supra* note 36, at 39863.

health or safety emergency.[66] For example, schools questioned whether, in the event of an epidemic outbreak, they could share information about students tested or affected by the outbreak with appropriate officials such as the Centers for Disease Control.[67] Congress noted, "In the case of the outbreak of an epidemic, it is unrealistic to expect an educational official to seek consent from every parent before a health warning can be issued."[68]

Another significant concern among K-12 and post-secondary institutions was the sharp cutoff and transfer of rights from parents to students when students reached the age of eighteen or enrolled in post-secondary study. Many feared that this requirement would inhibit the sharing of necessary information, such as tuition bills, with parents.[69] Multiple erroneous cross-references and typographical errors within the Act also resulted in confusion, uncertainty, and concern on behalf of educational institutions.[70]

Despite this criticism and confusion, most institutions attempted to comply with the new law.[71] A memo addressed to Senator Buckley stated, "While there is an effort underway to lobby for delay in the implementation of [FERPA], most schools and agencies seem to be able and are in fact preparing to comply with implementation on November 20 [sic], 1974."[72]

Dr. Phil Salmon, Director of the American Association of School Administrators, noted that some schools had "'drop[ped] everything that came along' into the cumulative folder,"[73] and he advised schools "to remove from the folders and destroy such things as unsubstantiated teacher opinions, or language which tends to 'categorize' students.'"[74] Thus, FERPA forced many schools to consider student privacy—perhaps for the first time—and to update their policies and procedures accordingly. Nonetheless, the memorandum also noted that Congress had received numerous calls from schools, districts, colleges, and universities around the country: "nearly all

66 Joint Statement, *supra* note 36, at 39863.
67 Joint Statement, *supra* note 36, at 39863.
68 Joint Statement, *supra* note 36, at 39863.
69 Joint Statement, *supra* note 36, at 39863.
70 Joint Statement, *supra* note 36, at 39863.
71 *See, e.g.*, 120 CONG. REC. 36532 (1974) (*Questions About and Objections to the Buckley Amendment—The Family Educational Rights and Privacy Act of 1974 (Sec. 513 of P.L. 93-380)—and Responses*) [hereinafter "Questions and Objections"]; Carole Marie Mattessich, *The Buckley Amendment: Opening School Files for Student and Parental Review*, 24 CATH. U. L. REV. 588, fn. 60 (1975) [hereinafter "Mattessich Article"].
72 Questions and Objections, *supra* note 71, at 36532. While the Congressional Record does not list an author of the memorandum, Mattessich's law review article suggests that John Kwapisz, an aide to Senator Buckley, drafted the memo and addressed it to Sen. Buckley. *See* Mattessich Article, *supra* note 71, at 588, fn. 38.
73 Questions and Objections, *supra* note 71, at 36532.
74 Questions and Objections, *supra* note 71, at 36532.

the callers have said that their schools are developing a policy and procedures for compliance, but they have a question or two as to what a particular aspect of the bill means or includes, or whether such and such procedure on their part would be appropriate."[75]

Rumors surfaced that, although Senator Buckley was a long-time, active part of the education field, he asked an aide to draft FERPA slightly more than one month before he introduced the bill.[76] This led some stakeholders to question FERPA's conception, especially since the bill never underwent a formal committee process.[77] In response, many called for Congress to delay the Act's date of enactment on November 19.[78] A *Washington Post* article, printed in the congressional record as evidence of the need for the amendment, commented, "Senator James L. Buckley has found out recently that opening up school records is more complicated than it first appeared."[79] On November 14, 1974, a few days before FERPA's initial effective date, Senator Pell's office issued a press release stating that if legislators and institutions could not reach agreement on FERPA's uncertainties and when the law should take effect, he would likely sponsor an amendment to defer the effective date.[80] Shortly thereafter, the process to amend FERPA began.

D. The Buckley/Pell Amendment

FERPA's first amendment, known as the Buckley/Pell Amendment, was offered on the Senate floor on December 13, 1974.[81] During its introduction, Senator Buckley noted that "the educational community has pointed to certain ambiguities . . . contained in the language and provisions—that because there was none of the normal legislative history, it means that [the U.S. Department of Health, Education, and Welfare] HEW does not have an adequate record . . . to develop the necessary regulations."[82] Senators Buckley and Pell offered a joint statement explaining the need for an amendment of FERPA, noting that FERPA's "restrictions are too narrow and, if strictly applied, would seriously interfere in the operation of educational institutions."[83]

---

75 Questions and Objections, *supra* note 71, at 36532.
76 Mattessich Article, *supra* note 71, fn. 38.
77 Mattessich Article, *supra* note 71, at 594.
78 Mattessich Article, *supra* note 71, at 597.
79 Washington Post Editorial, *supra* note 59, at 41396.
80 Washington Post Editorial, *supra* note 59, at 41396.
81 *See* 120 CONG. REC. 39860 (1974).
82 *See* 120 CONG. REC. 39862 (1974).
83 *See* Joint Statement, *supra* note 36, at 39863.

The Buckley/Pell Amendment also addressed many problems resulting from FERPA's initial language. The amendment defined key terms, including "education records" and "educational institutions,"[84] and created the "directory information" exception, which addressed concerns about the necessary or routine sharing of student information.[85] As the name suggests, the directory information exception allows schools to share names, addresses, birth dates, heights and weights of student athletes, and students' most recently attended educational institutions, among other information. The amendment described this as information "that would not generally be considered harmful or an invasion of privacy if disclosed."[86] Since recipients of this information could redisclose it, FERPA requires that schools notify parents and students about which categories of information the school chooses to designate as directory information, and offer an opportunity to opt out of this sharing.[87]

The amendment also clarified that schools could share, without obtaining consent, de-identified data with federal authorities and bodies for auditing and accreditation purposes, state authorities pursuant to state law, and organizations such as the Law School Admissions Council and the College Entrance Exam Board.[88] Sharing this information would allow these organizations to predict applicants' potential success in post-graduate programs.[89] Post-secondary institutions were also concerned about sharing students' personal data with third parties for financial aid applications.[90] The Buckley/Pell Amendment clarified that schools could use and share social security numbers, with consent, for financial aid applications.[91] The amendment also noted that parents' financial information would not be shared with students as part of the latter's right to access their records.[92]

The Buckley/Pell Amendment also allowed students to waive their rights to access and confidentiality, a noteworthy addition since it seemed to be at odds with FERPA's original aims regarding student record

[84] Pub. L. 93-568, 88 Stat. 1855, 1859 (1974).

[85] Pub. L. 93-568, 88 Stat. 1855, 1859 (1974).

[86] U.S. Department of Education, About ED Frequently Asked Questions, https://www2.ed.gov/policy/gen/guid/fpco/faq.html#q4 (last visited Mar. 9, 2020).

[87] Pub. L. 93-568, 88 Stat. 1860 (1974).

[88] *See* Joint Statement, *supra* note 36, at 39863.

[89] *See* Joint Statement, *supra* note 36, at 39863.

[90] Joint Statement, *supra* note 36, at 39863.

[91] Joint Statement, *supra* note 36, at 39863.; *see also* 120 CONG. REC. 36535 (1974) (Part of the "Conference Report Explanation of Action on Buckley Amendment to H.R. 69 reads, "An exception under the conference substitute occurs in connection with a student's application for, or receipt of, financial aid. The conferees intend that this exception should allow the use of social security numbers in connection with a student's application for, or receipt of, financial aid.").

[92] Pub. L. 93-568, 88 Stat. 1860 (1974).

accessibility. A 1975 law review article reflected that, since this provision might cause students to "waive their future rights of access to certain confidential information," it ironically would "effectively close up many of the files which the original [FERPA] intended to open."[93] Several members of Congress carefully drafted this provision so that schools could not condition attendance or matriculation on a waiver of these rights.[94] The House of Representatives, when it adopted the Buckley/Pell Amendment, added this language protecting these waiver rights.[95] In addition to exempting directory information, parents' financial records, psychiatric and physician records, certain confidential letters of recommendation, and medical information in the case of an emergency, the Buckley/Pell Amendment also created an exception for "personal notes of education staff."[96] This exception included records written by and ancillary to education personnel, solely in the possession of the education staff member, that are not available or revealed to anyone other than a substitute teacher.[97]

Although the Buckley/Pell Amendment seemed to relax some of FERPA's sharing restrictions, it also clarified who had access to student data and the third parties with which schools shared it. The amendment required schools to maintain a list of all these parties and to make this list available to parents and students when appropriate, for review.[98]

The new language also gave parents substantive rights that were not present in the original FERPA. For example, while FERPA originally allowed educators' personal comments and impressions to become part of a student's record—and gave parents no way to prevent this from occurring––the Buckley/Pell Amendment allowed parents to insert an explanatory statement into their children's education record.[99] While the original FERPA cut off parents' rights after a student turned eighteen or enrolled in college, the amendment also allowed parents who claimed a student as a dependent on their tax returns to retain access to that student's records and grade information after the student turned eighteen.[100] The Buckley/Pell Amendment was passed on December 31, 1974 as P.L. 93-568, effective retroactively to FERPA's initial effective date of November 19, 1974.[101]

93 Mattessich Article, *supra* note 71, at 589.
94 *See* 120 CONG. REC. 39864 (1974) (discussion between Sens. Mondale and Pell).
95 *See* 120 CONG. REC. 41392 (1974) (statement by Sen. Perkins).
96 120 CONG. REC. 41392 (1974) (statement by Sen. Perkins).
97 Pub. L. 93-568, 88 Stat. 1860 (1974).
98 Pub. L. 93-568, 88 Stat. 1862 (1974); 120 CONG. REC. 41392 (1974) (statement by Sen. Perkins).
99 120 CONG. REC. 41392 (1974); Pub. L. 93-568, 88 Stat. 1855 (1974).
100 Pub. L. 93-568, 88 Stat. at 1861 (1974).
101 *See generally* Pub. L. 93-568, 88 Stat. 1855 (1974).

Despite the initial backlash from schools following the enactment of FERPA and the Buckley/Pell Amendment, some critics continued to question FERPA's impact on students and educational institutions. Two years after FERPA was passed, Katherine Cudlipp, Assistant Counsel to the Public Works Committee of the Senate, suggested that the law raised awareness more than it spurred requests for information:

> Approximately twenty-one months have passed since the effective date of the Act. Although institutions have modified certain practices, some of the worst fears about red tape have not been realized. There has been no great surge in requests by parents or students for access to files, but public awareness of the provisions of the Amendment—measured by reports in the press and inquiries to HEW—appears to be substantial . . . . It is suggested that the real value of the Amendment may be first that it has caused educational institutions to consider their policies and practices with respect to student records—many perhaps for the first time.[102]

Cudlipp also noted that because of the Act's enforcement mechanisms, much of the law's effect depends on whether students and parents are aware of their rights under FERPA.[103] Many stakeholders also feared that the FERPA and the Buckley/Pell Amendment would be costly for schools to implement. These fears proved largely unfounded because FERPA's regulations did not impose affirmative obligations on schools to submit procedures, conduct audits, or produce policies in order to receive federal funding.[104] National Association of Elementary School Principals President Edward Keller noted in March of 1976, "[t]he Amendment, in fact, requires little more than what many schools were already doing."[105]

III. STUDENT PRIVACY IN THE MODERN ERA

Forty years after FERPA was passed, more than 1,000 bills on student privacy have been introduced in all fifty states since 2013,[106] and more than 130 have passed in forty states and Washington, D.C. Like FERPA, most of the laws emerged in response to growing concerns over the increased amount

102 Katherine Cudlipp, *The Family Educational Rights and Privacy Act Two Years Later*, 11 U. OF RICHMOND L. REV. 33, 48 (1976)

103 *Id.* at 38–39.

104 *Id.* at 40.

105 *Id.*

106 Data Quality Campaign, *Education Data Legislation Review 2017 State Activity* (2017), available at https://2pido73em67o3eytaq1cp8au-wpengine.netdna-ssl.com/wp-content/uploads/2017/09/DQC-Legislative-summary-0926017.pdf.

of student data collected but also how stakeholders use, report, and protect this data. Well-publicized data breaches in the private sector (such as at Target and Home Depot) lack trust in the government's protection of privacy following the Edward Snowden leaks, and activists' claims about FERPA's insufficiency in the modern era fueled these worries and mobilized state legislatures to act. The result was a patchwork of legislative regimes across the country.

When legislators have passed these student privacy bills quickly and with little stakeholder input, they have brought unintended consequences to the students they sought to protect. For example, as detailed further below, the Louisiana state legislature passed a highly restrictive student privacy law that resulted in extreme such consequences.[107] The law prohibited the state education agency (SEA) from collecting any student information; required parental consent for nearly all information sharing; and imposed fines and jail time on teachers and principals for all disclosure violations, even accidental cases. These stipulations prevented schools and the SEA from performing basic, necessary functions and prevented some students from accessing crucial benefits such as the state's scholarship fund. In many ways, these consequences mirrored those that led to FERPA's first amendment. In this section, we provide an overview of the current student privacy landscape and discuss four case studies demonstrating unintended consequences that resulted from new student privacy laws.

A. The State Student Privacy Landscape: 2014-2020

Since the 1800s, schools have collected data to monitor students' progress, which has helped educators understand how to best serve their students. However, the increasing presence and sophistication of digital technology in schools since FERPA was passed have yielded significantly greater data collection. The passage of the No Child Left Behind Act (NCLB) in 2002 also began a new era of data collection.[108] Suddenly, this well-meaning attempt to close the achievement gap required local and state education agencies (LEAs and SEAs, respectively) to report students' progress and to track how schools were serving different student subgroups.[109] Analysis of that data has resulted in substantial, useful findings. For example, a study released in 2016 revealed disproportionate suspension rates of minority students and that these students are routinely not referred to advanced placement classes.[110]

---

[107] *See infra* Section III B.
[108] *See* Pub. L. 107-110, 115 Stat. 1425 (2002) (codified at 20 U.S.C. § 7971 et seq.).
[109] Pub. L. 107-110, 115 Stat. 1425 (2002) (codified at 20 U.S.C. § 7971 et seq.).
[110] Monica Bulger et al., *The Legacy of InBloom*, DATA & SOCIETY 4 (2017), https://datasociety.net/wp-content/uploads/2017/02/InBloom_feb_2017.pdf.

Education technology, or edtech, is now ubiquitous in the modern school system.[111] In most schools, teachers use a learning management system to track attendance, lesson plans, and homework, and a student information system to access student records. Many middle and high schools issue laptops to all students and allow them to take the devices home. Students often use their own devices to work on assignments collaboratively inside and outside the classroom.[112]

In 2013, an edtech initiative called inBloom launched in order to improve data entry and storage in educational settings.[113] With inBloom, teachers could better understand the data collected about their students and would no longer have to enter multiple usernames and passwords for each edtech tool used; student information did not have to be entered multiple times in every database; and parents could access their children's records in one place.[114] InBloom's website advertised the company's "world-class" security protections.[115] States across the country raced to adopt the initiative because of inBloom's potential value for teachers, students, and parents.

However, the publicity regarding inBloom drew public attention to how schools collected and used students' data. Parents were shocked to learn that "schools [were collecting] hundreds of data elements, and [using] those to evaluate students unbeknownst to them."[116] Schools were also handing over that student data to third-party companies. In a case study of inBloom published in 2017, researchers noted that the tool "served as an unfortunate test case for emerging concerns about data privacy coupled with entrenched suspicion of education data and reform."[117] Stakeholders linked debates about increased standardized testing associated with Common Core curricula and teacher evaluations to data privacy issues, creating an incendiary environment that culminated in intense focus on inBloom and, ultimately, pressure on lawmakers to act.

Privacy activists who opposed the increase in sharing students' data emphasized the risks of data use and technology, while ignoring benefits

---

[111] Natasha Singer, *How Google Took Over the Classroom*, N.Y. TIMES (May 13, 2017) https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html; *see also* Cambridge Assessment International Education, *Global Education Assessment*, 12 (2018) https://www.cambridgeinternational.org/Images/514611-global-education-census-survey-report.pdf.

[112] *See* Cambridge Assessment International Education, *supra* note 111 (finding that 42% of students globally use a smartphone in the classroom).

[113] Bulger, *supra* note 110.

[114] Bulger, *supra* note 110.

[115] Bulger, *supra* note 110.

[116] Colorado State Board of Education, *Study Session Regarding inBoom, Inc.*, (2013) (statement of Khaliah Barnes, Administrative Law Counsel, Electronic Privacy Information Center), https://epic.org/privacy/student/EPIC-Stmnt-CO-Study-5-13.pdf.

[117] Bulger, *supra* note 110.

such as personalized learning. A parent advocacy group called Class Size Matters described inBloom as a company built to "collect, format, and share personally identifiable student data with for-profit vendors" to "help [these vendors] develop their 'learning products.'"[118] The Electronic Privacy Information Center, another advocacy group, raised concerns that inBloom could help create "principal watch lists," allowing school administrators to surveil, label, and punish students with little procedural transparency.[119] InBloom's messaging did little to assuage the fears raised by parents and privacy organizations. The company's website contained lists of data elements that districts could collect about students, and the security policy stated that the company could not "guarantee the security of the information stored" or that the information would not be "intercepted" when transmitted.[120] This was a frightening admission to the many parents who were unaware that this language was standard in edtech companies' privacy policies.[121]

Parents protested in states like Louisiana and Georgia, causing state leadership to cancel partnerships with inBloom, while other states publicly announced that they would evaluate the tool before moving forward.[122] In seven months, inBloom's nine state partners became three.[123] By fall 2013, New York was the only state publicly moving forward with inBloom.[124] However, in early 2014, the New York state legislature included a clause in its budget "making it illegal for the state to share personally identifiable student data with any shared learning infrastructure service provider via a private, cloud-based, or state operated student datastore," banning schools from using services such as inBloom. InBloom shut down in May 2014.[125]

However, inBloom's demise did not eradicate the public's fears about student privacy, in part because school districts and edtech companies overall were unprepared to respond to activists' privacy concerns. Mostly for the first time, schools were asked to justify the data they had been collecting and to explain their processes for protecting that data. Almost no state or district knew how to answer these questions. In this vacuum of silence and confusion, activists presented frightening what-if privacy

---

118 Bulger, *supra* note 110.

119 Colorado State Board of Education, *supra* note 116.

120 Katie Ash, *inBloom Aims to Increase Data Flow Despite Controversy*, EDUCATION WEEK (April 16, 2013), http://blogs.edweek.org/edweek/DigitalEducation/2013/04/inbloom_aims_to_increase_data_.html.

121 *Id*. at 19.

122 *Id*. at 20.

123 *Id*.

124 *Id*. at 20–21.

125 Bulger, *supra* note 110.

scenarios to motivate parents to push for new legal privacy regimes, and the media continued reporting these issues through 2014 and 2015. Some articles claimed that "[t]he NSA has nothing on the ed tech startup known as Knewton," using alarming imagery such as "data mining your children" and "monitoring every mouse click."[126] A *New York Times* opinion piece headline declared that "Student Data Collection Is Out Of Control."[127] An NPR Marketplace report described, "A day in the life of a data-mined kid," in which students carry identification cards installed with radio frequency identification chips that track their every movement.[128] Parents quoted in these articles worried that the data collected would affect their children's future college choices and job prospects.

In this context, parents' fears regarding the collection and use of their children's educational data are understandable, and some stakeholders mobilized these fears to persuade legislators. One expert made a widely reported statement at a congressional hearing, stating that only seven percent of school contracts banned outside vendors from selling student information, without noting that the seven percent cited was made up of a subgroup of less than ten districts.[129]

Legislators responded quickly to stakeholders' concerns, introducing 110 student privacy bills in thirty-nine states in 2014 and 180 student privacy bills in forty-nine states in 2015.[130] By the end of 2019, states had passed more than 130 student privacy laws in forty states and Washington D.C.[131] These states have reacted to irresponsible student data practices and their constituents' outrage by passing laws intended to protect students' privacy. However, some state legislatures did not fully appreciate how these laws

---

[126] Stephanie Simon, *The Big Biz of Spying on Little Kids*, POLITICO (May 15, 2014), https://www.politico.com/story/2014/05/data-mining-your-children-106676.

[127] Khaliah Barnes, *Student Data Collection Is Out of Control*, N.Y. TIMES (December 19, 2014), https://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/student-data-collection-is-out-of-control.

[128] Adriene Hill, *A Day in the Life of a Data Mined Kid*, MARKETPLACE (Sept. 15, 2014), https://www.marketplace.org/2014/09/15/day-life-data-mined-kid/.

[129] The study conducted in this case included information from only twenty-three (out of the 14,000 total) U.S. school districts, and the seven percent cited covered a subgroup of less than ten districts. Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, FORDHAM UNIVERSITY (2013), https://www.fordham.edu/info/23830/research/5917/.

[130] *See State Student Data Privacy Legislation: What Happened in 2014, and What Is Next?*, DATA QUALITY CAMPAIGN (Sept. 22, 2014), https://dataqualitycampaign.org/resource/state-student-data-privacy-legislation-happened-2014-next; *see also Student Data Privacy Legislation: What Happened in 2014, and What Is Next?*, DATA QUALITY CAMPAIGN (Sept. 24, 2015), https://dataqualitycampaign.org/resource/student-data-privacy-legislation-happened-2015-next/.

[131] *See generally State Student Privacy Laws*, FERPASHERPA (last updated 2019), https://ferpasherpa.org/state-laws/ (tracking state student privacy legislation passed since 2013).

would impact day-to-day instruction in the digital classroom.

Unintended consequences have often resulted from laws written with vague or sweeping language, harsh penalties, and no consultation with the stakeholders who implement the laws. For example, if a policymaker asked constituents whether they would ban the sale of all student data, the likely response would be overwhelmingly positive. Yet, as described further in the case studies below, an outright ban with no exceptions would prohibit schools from offering yearbooks, class photos, and PTA directories. Most policymakers seek to carefully balance crucial protections for students with allowances for responsible data use, to avoid banning useful practices. Yet, the overheated privacy debate resulting in unbalanced legislation has fueled deep distrust among education stakeholders, with far-reaching effects. Parents have struggled to understand how schools use and protect their children's information; edtech providers have struggled to develop their products and services and, in some cases, even operate; administrators, educators, and researchers have struggled to gather students' information needed to improve schools and students' achievement. To achieve promising educational innovations such as personalized learning, student privacy laws must improve, along with public perception and privacy practices on the ground. The following four cases illustrate unintended consequences resulting from hastily passed, reactive legislation intended to protect students. The cases can also help policymakers craft laws that make privacy a part of stakeholders' use of student data, rather than an impediment to that use.

B. Louisiana

Louisiana's student privacy law, one of the strictest in the nation, took effect in 2015.[132] The bill intended to ease parents' concerns by ensuring protection of students' data and providing transparency to parents about data sharing practices with school vendors.[133] However, the original law's opt-in consent requirement for sharing student information, vague wording, and strict interpretation led to several unintended consequences. The law required parents to return a consent form to share any student data, including data used for consideration for the state scholarship fund.[134] This meant that

---

[132] Corinne Lestch, *Are Student Privacy Laws Hurting Students?*, ED SCOOP (Mar. 2, 2015), https://edscoop.com/are-student-privacy-laws-hurting-students.

[133] Kim Nesmith, SXSWedu: Accidental Consequences of Student Privacy Laws Panel (March 2018) https://schedule.sxswedu.com/2018/events/PP78336; *Louisiana House Education Committee Meeting: Testimony for Amendments to HB 718* (May 2015) (statement of Rep. John Schroeder), http://house.louisiana.gov/H_Video/VideoArchivePlayer.aspx?v=house/2015/may/0512_15_ED [hereinafter "Louisiana House Education Committee Meeting"].

[134] Louisiana House Education Committee Meeting, *supra* note 133 (containing

if parents did not return the form, which was often the case, schools could not submit students' information to be considered for scholarships.[135] "If a parent doesn't send that letter back, or doesn't give us permission, then their child could lose out on opportunities for financial aid," West Baton Rouge Parish Schools Superintendent Wes Watts said. "Just the thought of that makes me cringe."[136]

Some of the law's other unintended consequences emerged when St. Tammany Parish School District implemented the law in full before the legislation's original effective date.[137] State Representative Schroeder, whose district included St. Tammany Parish School District and who later introduced legislation to amend the original law, noted that "some of the unintended consequences are you can't hang art on a wall in the schoolhouse without taking the name out, you can't do a newsletter and have kids names on it, so we were running across problems with just ID cards and cafeteria cards."[138] In the *Franklin Banner-Tribune*, a school board legal advisor said that the Louisiana law meant that "[w]ithout that [written parental] approval we would potentially be in violation of the law by publishing names and photographs in yearbooks, in football programs, students of the month, the honor rolls, etcetera."[139]

Another consequence resulted from the provision to increase transparency regarding data sharing. The provision required schools to publish on their websites their vendor contracts and the third parties with which schools shared data.[140] As a result, the provision made students' data potentially less safe. Louisiana School Boards Association attorney Danny Garrett explained, "What we had inadvertently done is we had created a roadmap for people who were going to try to access that data, because they could go on the school system's website, see what vendor had what types of data, and then they could go and attack that vendor."[141]

testimony from Rep. Schroeder and discussion by AmeliaVance regarding opt-in consent found in original act).

135 Lestch, *supra* note 132.

136 Lestch, *supra* note 132.

137 Louisiana House Education Committee Meeting, *supra* note 133; *SXSWedu: Accidental Consequences of Student Privacy Laws Panel*, *supra* note 133 (statement of Vance); Act 837, H.R. 1076, Reg. Sess. (2014), *available at* http://www.legis.la.gov/legis/ViewDocument.aspx?d=916157.

138 The problems with the law were discussed in the testimony for amendments to HB718. Louisiana House Education Committee Meeting, *supra* note 133.

139 *School Board Wrestles With State Privacy Laws*, FRANKLIN-BANNER TRIBUNE (July 10, 2015), https://archive.stmarynow.com/local/school-board-wrestles-state-privacy-laws.

140 Act 837, H.R. 1076, Reg. Sess. (2014), *available at* http://www.legis.la.gov/legis/ViewDocument.aspx?d=916157.

141 *Louisiana Legislature Education Committee Hearing* (2015) (statement of Danny Garrett) http://house.louisiana.gov/H_Video/VideoArchivePlayer.aspx?v=house/2015/may/0512_15

Louisiana passed HB 718 on June 23, 2015, to address some of these unintended consequences and clarify the legislative intent.[142] The amendment allowed any district to pass a policy with less-stringent privacy requirements.[143] This resulted in multiple different versions of student privacy laws varying by district, which still exist today.[144] However, the amendment retained several of the original legislation's extreme requirements. Both versions of the Act do not allow the state Department of Education to receive personally identifiable information, instead requiring the department to create a unique identifier for each student.[145] The law's strict penalties, a $10,000 fine and up to six months in jail per violation, also remain.[146]

C. New Hampshire

In 2015, New Hampshire passed a student privacy law that prohibited schools from recording in classrooms "for any purpose without school board approval after a public hearing and without written consent of the teacher and the parent or legal guardian of each affected student."[147] This meant that New Hampshire school officials needed to hold a public hearing, obtain school approval, and receive written consent from all affected teachers and parents before recording could take place in classrooms.[148] The law complicated the teacher certification process, which often requires recording teachers in order to evaluate them.[149] The law also conflicted with the federal law mandating accommodations for students with disabilities, the Individuals with Disabilities Education Act (IDEA).[150] In response to confusion over how districts should proceed under the state law, Heather Gage, of the N.H. Department of Education, stated in November 2015, "You need to continue to provide services for special education, as mandated by

_ED.

142 H.B. 718, 2015 Reg. Sess. (La. 2015).

143 H.B. 718, § 1H, 2015 Reg. Sess. (La. 2015).

144 Emily Tate, *What It's Like Navigating the Strictest Student Privacy Law in the Country*, EDSURGE (Jun. 18, 2019), https://www.edsurge.com/news/2019-06-18-what-it-s-like-navigating-the-strictest-student-privacy-law-in-the-country.

145 H.B. 718, 2015 Reg. Sess. (La. 2015), Original.

146 H.B. 718, 2015 Reg. Sess. (La. 2015), Original.

147 H.B. 507, 2015 Sess. (N.H. 2015).

148 H.B. 507, 2015 Sess. (N.H. 2015).

149 Priscilla Morrill, *Law on Recording in Classroom Questioned*, MONADNOCK LEDGER-TRANSCRIPT (Nov. 5, 2015), https://www.ledgertranscript.com/Archives/2015/11/p1Schools-ml-110315; *Privacy and Classroom Video Recordings for Teacher Preparation*, AMERICAN ASSOCIATION OF COLLEGES FOR TEACHER EDUCATION https://secure.aacte.org/apps/rl/res_get.php?fid=2529&ref=res.

150 20 U.S.C. § 1232(g); Morrill, *supra* note 149.

federal law."[151] For example, video recording is often used as an accommodation for students with ADHD; one website discussing video recordings' many uses in the classroom provides that "[i]ncorporating videos into lessons offers a viable method for students with special needs, such as ADD/ADHD or conditions requiring home-bound stints, to retain and remember information. The medium makes for one more way to ensure all learners enjoy access to educational materials that meet their specific requirements."[152]

These contradictions brought swift feedback to Rep. Glenn Cordelli, the law's initial sponsor, regarding the issues with teacher certification and students with individualized education programs (IEPs).[153] "This is certainly not intended to prevent things like that," Cordelli stated regarding video recording for students with IEPs. "It got interpreted a lot more broadly than originally intended."[154] He said that the initial goal of the legislation was to protect teachers from having their classrooms recorded without their consent, and to protect students' privacy in classrooms where recordings take place.[155] However, legislators received complaints about the act's consequences from both parents and teachers. A Drummond Woodsum report published on the New Hampshire School Administrators Association website notes, "Schools were frustrated with these changes as it limited their ability to measure student performance and to implement best practices for certain students, particularly those with disabilities. Parents were frustrated with the new law because they wanted more information on their child's educational program and progress and felt recordings were an effective way to get this information."[156]

The N.H. School Boards Association and the N.H. Department of Education issued a technical advisory regarding the law's requirements in October 2015.[157] This feedback led to an amendment in the next legislative

---

[151] Morrill, *supra* note 149.

[152] *11 Reasons Every Educator Needs a Video Strategy*, ONLINE UNIVERSITIES (Sep. 23, 2012), https://www.onlineuniversities.com/blog/2012/09/11-reasons-every-educator-needs-video-strategy [hereinafter "11 Reasons"].

[153] Morrill, *supra* note 149.

[154] Morrill, *supra* note 149.

[155] Morrill, *supra* note 149.; N.H. House Record 38 House Journal 23, 19 (Mar. 9, 2016), http://www.gencourt.state.nh.us/house/caljourns/journals/2016/HJ_23.pdf; Ganley, *supra* note 160.

[156] Gerald M. Zelin et al., *Development in New Hampshire Education Law: State Statutes*, DRUMMOND WOODSUM (Oct. 5, 2016), https://www.nhsaa.org/site/handlers/filedownload.ashx?moduleinstanceid=167&dataid=249&FileName=Developments%20in%20New%20Hampshire%20Education%20Law%20-%20Gerald%20Zelin%20Erin%20Feltes%20and%20Meghan%20Glynn.PDF.

[157] *Id.* (the advisory has since been removed, and in place is the general data collection and records page https://www.education.nh.gov/data/index.htm).

session, which narrowed the statute's language and clarified its intent.[158] The 2016 amendments, HB 1372, clarified that nothing in the act prohibits recording or requires public process and written consent for students with disabilities and for instructional purposes.[159] These amendments also allowed recording for teacher evaluations but retained the original requirements, including a public hearing, school board approval, and opt-in consent of each affected teacher and each student's parent.[160]

This restriction on video recording for teacher certification is particularly onerous for teachers and administrators if they cannot obtain all parents' opt-in consent, because certain certification organizations require video recordings as part of the certification process.[161] An information privacy principles report published by the American Association of Colleges for Teacher Education (AACTE) states, "[c]lassroom video is an essential part of performance assessment because it captures teacher candidates as they deliver instruction and interact with students."[162]

Moreover, for decades, the National Board for Professional Teaching Standards® "certification of accomplished teaching" has emphasized teachers' ability to describe, analyze, and reflect upon videos for their own teaching practices.[163] Researchers have also found that video recordings used for teacher evaluations often require less time and resources, compared to in-person observations, and are perceived to be less biased.[164] A study commissioned by the Center for Education Policy Research at Harvard University found that, "[r]esearch about video observations provides a very clear message—teachers perceive the process as more fair, useful, and satisfactory compared to in-person observations."[165] Despite this widespread

---

158 H.B. 1372, 2016 Leg. Session (N.H. 2016) (permitting a child with a disability to use audio or video recording devices in the classroom).

159 H.B. 1372, 2016 Leg. Session (N.H. 2016).

160 H.B. 1372, 2016 Leg. Session (N.H. 2016).

161 *Securing Personal Information in Performance Assessment of Teacher Candidates*, THE AMERICAN ASSOCIATION OF COLLEGES FOR TEACHER EDUCATION https://secure.aacte.org/apps/rl/res_get.php?fid=2538&ref=rl; *ePortfolio Submission,* NAT'L BD. FOR PROF'L TEACHING STANDARDS, GUIDE TO NATIONAL BOARD CERTIFICATION 1 (2019), https://www.nbpts.org/national-board-certification/candidate-center/eportfolio-submission [hereinafter "Securing Personal Information"].

162 Privacy and Classroom Video Recordings for Teacher Preparation, AMERICAN ASSOCIATION OF COLLEGES FOR TEACHER EDUCATION, https://secure.aacte.org/apps/rl/res_get.php?fid=2532&ref=res.

163 *See, e.g.*, *General Portfolio Instructions: Components 2, 3 and 4*, NAT'L BOARD FOR PROF. TEACHING STANDARDS (2019), https://www.nbpts.org/wp-content/uploads/NB_general_portfolio_instructions.pdf; *see generally* National Board Certification Overview, NAT'L BOARD FOR PROF. TEACHING STANDARDS https://www.nbpts.org/national-board-certification/overview.

164 *See* Securing Personal Information, *supra* note 161.

165 Thomas J. Kane et al., *The Best Foot Forward Project: Substituting Teacher-*

professional support for classroom recordings to evaluate and improve teaching, the stringent requirements for video recordings were still in place in 2020.

D. Connecticut

Connecticut passed the Student Data Privacy Act in 2016[166] and amended it in both 2017[167] and 2018[168] to address unintended consequences. Stakeholders believed that the 2016 Act required a contract between local boards of education and anyone with whom the district shared student data.[169] This meant that if only two students in an entire district used a certain software for an IEP or class project, the district had to complete a contractual agreement with the vendor, binding it to Connecticut's privacy law.[170] This resulted in excessive time, money, and resources expended to effect these contracts.[171] Connecticut Association of Schools Executive Director Karissa Niehoff stated in written testimony to the Joint Education Committee on March 14, 2018, "One district technology director calculated that PowerSchool (the most common data platform in schools) has over 160 individually negotiated contracts with exactly the same language. If a district has [thirty] (low estimate) apps and software packages that use student data, this suggests that there are nearly 5,000 individual contracts that need to be negotiated across the state."[172] Doug Casey, Executive Director of the Connecticut Commission for Educational Technology, wrote in an article about the Act that, "Having 169 districts and thousands of technology companies separately interpret and act on our state's student data privacy law. . . has proven hugely time-intensive, duplicative and inefficient."[173] To

Collected Video for In-Person Classroom Observations First Year Implementation Report, CTR. FOR POL'Y RESEARCH-HARVARD U., http://cepr.harvard.edu/files/cepr/files/l4a_best_foot_forward_research_brief1.pdf?m=1443808234; *Letter to Teachers: Benefits of Video Observations and Common Questions about Privacy and Video*, THE BEST FOOT FORWARD PROJECT (2015), http://cepr.harvard.edu/files/cepr/files/c1a_benefits_of_using_video_letter.pdf.

166 Act of June 9, 2016, Pub. L. No. 16-189, Stat. 5469 (2016) (concerning student data privacy).

167 2017 Legis. Bill Hist. CT H.B. 7207 (Conn. 2017).

168 2018 Legis. Bill Hist. CT H.B. 5444 (Conn. 2017).

169 Amelia Vance, Director of Education Policy at the Future of Privacy Forum, Speaking on the Accidental Consequences of Student Privacy Laws at SXSW EDU (Mar. 6, 2018).

170 Vance, *supra* note 169.

171 David Desroches, *School Districts Struggle to Comply with New Student Data Privacy Law*, WNPR NEWS (June 4, 2018), http://www.wnpr.org/post/school-districts-struggle-comply-new-student-data-privacy-law.

172 Testimony from Karissa L. Niehoff, ED.D, Conn. Ass'n of Sch.'s, on SB 452, 453, 455, 459, HB 5444, 54445 (Mar. 14, 2018).

173 Doug Casey, *State Action to Streamline Compliance: The Connecticut Story*, FERPASHERPA (Jan. 16, 2018), https://ferpasherpa.org/casey1.

address the time and resource burdens placed on districts, the 2018 amendments allowed state-level negotiations of contracts with vendors through a uniform student privacy terms-of-service addendum.[174]

In some instances, districts were unable to reach an agreement with a vendor, which meant foregoing beneficial software.[175] For example, Monroe Schools Assistant Superintendent Jack Zamary said, "When you get into sophisticated applications at the high school level, for Advanced Placement courses, the software that's used at that level is very professional."[176] While companies, such as Google, have changed their terms of service to comply with the Connecticut law, Zamary said that some companies are not willing to change their terms because the Connecticut school market is too small,[177] and "it really puts us in a very awkward place . . . [b]ecause our kids love the course, they love doing the work, but we're having a real challenge getting compliant software to offer that kind of course."[178]

The 2016 law also imposed a strict notification time frame, requiring personal notice to all students and parents within five days of any contractual agreement with a vendor that handles student data.[179] This notice required communicating the substance of the contract and which student data would be collected or used pursuant to the contract.[180] The original statute also required notification to students and parents within forty-eight hours of a data breach, regardless of whether the breach was patched or the school district had determined which students' data was affected.[181]

The Act was amended in 2017 to give districts and vendors more time to comply with the law, by moving its effective date to July 2018.[182] Joseph Cirasoulo, Executive Director of the Connecticut Association of Public School Superintendents, said at the Joint Standing Committee hearing on March 6, 2017, "I also don't think that any of us fully understood the implications of the Act once it got down especially to the classroom level

174 2018 Legis. Bill Hist. CT H.B. 5444 § 1.

175 Desroches, *supra* note 171.

176 Desroches, *supra* note 171.

177 Desroches, *supra* note 171; Corinne Lestch, *Google Adds New Terms to Comply with Connecticut Student Data Privacy Laws*, EDSCOOP (May 11, 2018), https://edscoop.com/google-adds-new-terms-that-comply-with-connecticut-student-data-privacy-laws.

178 Desroches, *supra* note 171.

179 Act Concerning Student Data Privacy, Pub. Act No. 16-189, § 2 (g) (effective October 1, 2016).

180 Act Concerning Student Data Privacy, Pub. Act No. 16-189, § 2 (g) (effective October 1, 2016).

181 Vance, *supra* note 169; Zachary Schurin, *Changes to Student Data Privacy Act Enacted: Is Your District Ready For July 1, 2018?*, JDSUPRA (Jun. 12, 2018), https://www.jdsupra.com/legalnews/changes-to-student-data-privacy-act-85242.

182 Schurin, *supra* note 181.

and that's why we're back asking for a postponement, relooking at it, revising it, so we can protect the data and the privacy of the date (sic) and also allow for things to go on in the classroom that should go on."[183]

The Act was amended in 2018 to further address consequences that the 2017 postponement and amendments had not fully resolved.[184] These amendments partially addressed the contract negotiation burdens by allowing the Connecticut Commission for Educational Technology to create "The Hub," an online database that allows educators and school administrators to quickly search and identify companies that have signed Connecticut's Student Data Privacy Pledge and have agreed to comply with Connecticut's Act.[185] Most significant, the 2018 amendments also created an exception to the requirement for written contracts for each vendor, for vendors used for IEPs that are "unable to comply with the provisions of this section."[186] Doug Casey stated in his 2018 written testimony to the Joint Education Committee, "The Student Data Privacy Act was never intended to deprive a special education student from being able to access a particular resource needed to fulfill his or her individualized education plan."[187] While a prior version of the amendment limited the special education exception only to vendors providing services or products used by two or fewer children per district, some school officials, such as Amity Regional School District No. 5 Superintendent Charles S. Dumais, felt that this did not go far enough and called for a complete exception regardless of the number of students.[188] The 2018 amendment states that if a vendor meets the student IEP exception, the vendor still must have attempted to create a contractual agreement with the school board, the school board must have researched and failed to find alternatives that would comply with the Act, the parent must give written consent, and the vendor must still comply with the Act's use restrictions.[189]

[183] The committee hearing was for PA 17-200. Transcripts from the Joint Standing Committee Public Hearing(s) and/or Senate and House of Representatives Proceedings, Pub. Act No. 16-189, H.B. 7207, Connecticut State Library (2018).

[184] *See generally* An Act Making Revisions to the Student Data Privacy Act of 2016, Pub. Act No. 17-200 (approved July 10, 2017).

[185] Act Making Revisions to the Student Data Privacy Act, Pub. Act No. 18-125 (effective July 1, 2018).

[186] Act Making Revisions to the Student Data Privacy Act, Pub. Act No. 18-125 (effective July 1, 2018).

[187] Letter from Douglas Casey, Exec. Dir., CT Comm. For Educ. Tech., to CT. Educ. Comm., (March 14, 2018) (available at https://www.cga.ct.gov/2018/EDdata/Tmy/2018HB-05444-R000314-Casey,%20Douglas,%20Executive%20Director-CET-TMY.PDF).

[188] Letter by Charles Dumais, Superintendent, Amity Regional School District No. 5 to the Connecticut Joint Education Committee (Mar. 13, 2018) (available at https://www.cga.ct.gov/2018/EDdata/Tmy/2018HB-05444-R000314-Dumais,%20Charles,%20Superintendent-Amity%20Regional%20School%20District%20No.%205-TMY.PDF).

[189] Act Concerning Revisions to the Student Data Privacy Act 2018 Conn. Acts,

The Act's amendments also relax some of the notification procedures.[190] Instead of requiring individual notice of each vendor contract, schools instead must post on a website notices of the contracts within five days of having reached the agreement.[191] Schools must provide to parents, before September 1, each year, the website address where the notices are posted.[192] The amended Act also extends the breach notification time frame to two business days instead of forty-eight hours, but still does not address breaches that have not been patched or cases in which the affected students are unknown.[193] The Joint Education Committee report for the 2018 amendments demonstrated continued overwhelming support for the Student Data Privacy Act, but many of the public comments asked for the legislature to not delay the Act's implementation any longer.[194] The 2018 amendments were passed on June 7, 2018, with most of the provisions becoming effective as scheduled on July 1, 2018.[195]

E. Virginia

Virginia provides another cautionary tale in which lawmakers enacted student privacy legislation as a swift reaction to isolated incidents. In 2018, Virginia passed a law to limit the sharing of student directory information, especially student emails, phone numbers, and addresses, and the law was subsequently amended in 2019 to eliminate unintended consequences.[196] The original bill emerged in reaction to the actions of a progressive political group, NextGen, during Virginia's 2017 State Elections.[197]

Substitute House Bill No. 5444 (2018); Schurin, *supra* note 181.

[190] Act Concerning Revisions to the Student Data Privacy Act 2018 Conn. Acts, Substitute House Bill No. 5444 (2018).

[191] Act Concerning Revisions to the Student Data Privacy Act 2018 Conn. Acts, Substitute House Bill No. 5444 (2018).

[192] Act Concerning Revisions to the Student Data Privacy Act 2018 Conn. Acts, Substitute House Bill No. 5444 (2018).

[193] Act Concerning Revisions to the Student Data Privacy Act 2018 Conn. Acts, Substitute House Bill No. 5444 (2018).

[194] *See generally* Connecticut Joint Education Committee, Joint Favorable Report, H.B. 5444 (2018).

[195] *See* Ch. 170, Sec. 10-234 and accompanying subsections https://www.cga.ct.gov/current/pub/chap_170.htm#sec_10-234aa; *see also* Substitute House Bill No. 5444 (2018) https://www.cga.ct.gov/2018/ACT/pa/2018PA-00125-R00HB-05444-PA.htm (containing the act's passage date).

[196] *Compare* H.B. 1, 2018 Leg. Session (Va. 2018) *and* S.B. 512, 2018 Leg. Sess. (Va. 2018) (both encompassing the original act) *with* H.B. 2449, 2019 Leg. Sess. (Va. 2019) (containing the amendment).

[197] Carmen Forman, *Progressive Political Group Obtains Cellphone Numbers from Virginia Tech, Radford Students For Electoral Campaigns*, THE ROANOKE TIMES (Oct. 3, 2017), https://www.roanoke.com/news/politics/montgomery_county/progressive-political-group-obtains-cell-phone-numbers-from-virginia-tech/article_43921646-7977-5040-b92b-2db4fa1b7350.html.

NextGen obtained college students' cell phone numbers through a Virginia Freedom of Information Act (FOIA) request served on various universities, and then texted students to encourage them to register to vote and to vote and volunteer for progressive candidates.[198] After NextGen's actions gained the attention of collegiate and local news media, Virginia House Delegates Tony Wilt and Joseph Yost discussed introducing legislation in the subsequent term to prevent this sort of data sharing in the future.[199] Both Dels. Wilt and Yost faced Democratic challengers who received campaign contributions from NextGen, and Wilt's challenger, Brent Finnegan, was one of the candidates that NextGen had encouraged students to support in the organization's text messages.[200] Del. Yost was ultimately defeated by his challenger, but Del. Wilt was re-elected, and prefiled HB 1.[201]

HB 1 sought to modify the directory information section of the Code of Virginia, by requiring schools to obtain opt-in consent from students, or parents of students under age eighteen, in order to ever disclose directory information to others, including disclosure through a FOIA request.[202] In addition to HB 1, Del. Chris Hurst, who defeated Joseph Yost for the Delegate seat in the 2017 election, also introduced a bill in light of NextGen's use of student directory information. Hurst's HB 147 sought to add one sentence to Virginia's FOIA Scholastic Records exemption, to exclude students' cell phone numbers and email addresses from FOIA's mandatory disclosure.[203]

In the Senate, Sen. Suetterlein introduced a bill, SB 512, requiring educational institutions to obtain written opt-in consent before sharing students' addresses, phone numbers, and emails pursuant to FOIA requests.[204] Hurst's bill was passed by a House subcommittee, but was left in the general House without further consideration.[205] Wilt's HB 1 passed the House, but the Senate voted to substitute HB 1 for Suetterlein's bill, SB 512.[206] The House rejected this substitution, and a conference committee

198 Madisson Haynes, *JMU Students Receive Mass Texts From Brent Finnegan Campaign*, THE BREEZE (Sept. 27, 2017), https://www.breezejmu.org/news/jmu-students-receive-mass-texts-from-brent-finnegan-campaign/article_e4dfd698-a38f-11e7-b096-cfda707daac8.html; Forman, *supra* note 197.

199 Forman, *supra* note 197.

200 Haynes, *supra* note 198.

201 H.B. 1, 2018 Leg. Sess. (Va. 2018).

202 H.B. 1, 2018 Leg. Sess. (Va. 2018).

203 H.B. 147, 2018 Leg. Sess. (Va. 2018).

204 S.B. 512, 2018 Leg. Sess. (Va. 2018).

205 H.B. 147, 2018 Leg. Sess. (Va. 2018).

206 *See* H.B. 1, 2018 Leg. Sess. (Va. 2018), S.B. 512, 2018 Leg. Sess. (Va. 2018) and accompanying legislative history.

was convened, which ultimately resulted in the passage of HB 1 and SB 512 in both houses.[207] Gov. Ralph Northam signed both into law, and they became effective July 1, 2018.[208]

Together, the laws required schools to obtain opt-in consent from students not only when sharing students' email addresses and phone numbers pursuant to FOIA, but for all sharing of directory information.[209] The bills' passage made Virginia the first state to adopt an opt-in regime for sharing directory information, as other states and FERPA mandate an opt-out regime whereby schools notify students and parents of what constitutes directory information and give them the opportunity to opt out of the schools' sharing of this information.[210]

From the outset, even prior to the law's passage, some stakeholders were skeptical of HB 1's broad scope, calling it a "sledgehammer" when compared to HB 147, which was perceived to be a "scalpel."[211] Some interest groups, such as the Virginia Coalition for Open Government, also opposed the bill.[212] When the 2018 school year began a few months after the July 1 effective date, stakeholders immediately noticed the law's unintended consequences. Since the initial legislation was prompted by FOIA requests gone wrong and only public institutions are subject to FOIA requests, some private universities assumed that the law only applied to public institutions.[213] For example, the general counsel of University of Richmond, a private institution, tracked the bill from its introduction through passage but did not express opposition because she did not think the bill would apply to the University of Richmond.[214]

---

207 *See* H.B. 1, 2018 Leg. Sess. (Va. 2018), S.B. 512, 2018 Leg. Sess. (Va. 2018) and accompanying legislative history.

208 *See* H.B. 1, 2018 Leg. Sess. (Va. 2018), S.B. 512, 2018 Leg. Sess. (Va. 2018) and accompanying legislative history.

209 *See* H.B. 1, 2018 Leg. Sess. (Va. 2018), S.B. 512, 2018 Leg. Sess. (Va. 2018) and accompanying legislative history.

210 Carmen Forman, *Del. Tony Wilt Files Legislation to Restrict Student Data in Wake of NextGen Virginia's Tactics*, THE ROANOKE TIMES (Nov. 20, 2017), https://www.roanoke.com/news/politics/general_assembly/del-tony-wilt-files-legislation-to-restrict-student-data-in/article_865be8d2-ab15-56fb-8c58-8a3a0f04aadb.html.

211 Paul Fletcher, *Editorial: A sledgehammer or a scalpel?*, VIRGINIA LAWYERS WEEKLY (Dec. 21, 2017), https://valawyersweekly.com/welcome-ad/?retUrl=/2017/12/21/editorial-a-sledgehammer-or-a-scalpel/.

212 Letter from Megan Rhyme, Executive Director, Virginia Coalition for Open Government, to Ralph Northam, Governor of Virginia (Mar. 21, 2018) (available at https://www.opengovva.org/sites/default/files/images/stories/files/HB1SB512toGovernor.pdf).

213 Ashlee Korlach, *Recent Virginia Law Prevents Release of Student Email Addresses, Necessitated Removal of Student Directory*, THE COLLEGIAN (Oct. 2, 2018), https://www.thecollegianur.com/article/2018/10/recent-virginia-law-prevents-release-of-student-email-addresses-necessitated-removal-of-student-directory.

214 *Id.*

After stakeholders realized the scope of the legislation, universities pulled their student directories from both their public and internal websites so that third parties and other students could no longer locate other students' email addresses.[215] A statement by the VCU Office of the Provost read, "Students will no longer be able to find contact information for another student through phonebook.vcu.edu or the people search on the VCU website."[216] The same office also stated, "University online applications—such as Blackboard, email, room reservation systems and Service Desk—will no longer enable non-employees to search for student eID and email addresses, including the auto-complete feature of email addresses currently used in many systems."[217]

Students and educators also found it more difficult to work on group projects and to collaborate with classmates because institutions interpreted the bill as prohibiting professors from sharing students' email addresses with other students.[218] University of Richmond Registrar Susan Breeden said, "I think the hallmark of a Richmond education is the collaboration, and it just makes it harder."[219] Some professors anticipated these issues and required students to opt in to data sharing early on in the semester. "In one of my first classes this semester, my teacher made it clear for us to go into myVCU and give the university permission to share contact information in order to make class communications easier," a VCU student stated.[220] Student journalists were also concerned about the "dangerous precedent" that HB 1 could set for obtaining student information from FOIA requests.[221] Student Press Law Center Senior Legal Counsel Mike Hiestand stated, "This is really the nuclear option for public records."[222] When stakeholders began to feel the law's unintended effects, reports surfaced that certain university registrars sought amendment of the statute when the legislature reconvened.[223]

As a result, Del. Wilt introduced HB 2449 to amend his original bill.[224] Wilt explained, "My intent from the very beginning was not to place a

---

[215] Nia Tariq, *Virginia Law Does Away With University Directories for Student Privacy*, COMMONWEALTH TIMES (Sept. 28, 2018), https://commonwealthtimes.org/2018/09/28/virginia-law-does-away-with-university-directories-for-student-privacy.

[216] *Id.*

[217] *Id.*

[218] Korlach, *supra* note 213, at 23.

[219] Korlach, *supra* note 213, at 23.

[220] Tariq, *supra*, note 215, at 23. The VCU student quoted is Jordan Glisan.

[221] Gabriel Greschler, *Virginia Governor Signs Two Bills Which Limit Access to Student Records*, STUDENT PRESS LAW CENTER (Feb. 8, 2018), https://splc.org/2018/02/virginia-directories-foia-exemption-bill/.

[222] *Id.*

[223] Korlach, *supra* note 213, at 23.

[224] H.B. 2449, 2019 Leg. Sess. (Va. 2019).

hardship on the schools. The real goal was to prevent outside people, whoever they may be—political groups—completely unrelated to the school, being able to access students' most intimate information for their own purposes."[225] HB 2449 created an exception to the opt-in requirement for directory information when information is shared internally with other students or with school board employees.[226] These changes alleviated concerns among university professors regarding sharing students' contact information with other students, and among university contractors and vendors.[227] Governor Northam signed HB 2449 into law on March 5, 2019.[228]

IV. LESSONS LEARNED AND KEY PRINCIPLES FOR STUDENT PRIVACY LEGISLATION

The unintended effects discussed above are emblematic of the challenges that privacy legislation has posed in the last decade, echoing many issues that arose when the U.S. Congress passed FERPA in 1974. For legislators, this history offers more than a cautionary tale; it suggests specific lessons and principles that policymakers can use to change the trajectory of future privacy legislation. For example, some of the student privacy laws were passed hastily in response to public fears or specific incidents, with little input from stakeholders.[229] Other laws neglected to clearly define their scope and requirements, resulting in confusion and anxiety.[230] These patterns indicate four principles that are essential for crafting clear, balanced, and fair education privacy laws: trust, transparency and inclusion, context, and clarity. As discussed further below, each of these principles is multifaceted in terms of student privacy. Trust is not simply a value to assume among education stakeholders; it requires understanding dominant perceptions about data privacy, particularly fear. Transparency means not just communicating with stakeholders, but also understanding how transparency works in the laws themselves. This section describes how these principles can function as a roadmap for producing better education privacy laws and for helping lawmakers use carefully crafted laws to encourage a culture of privacy in schools and districts.

225 Amy Friedenberger, *Northam Signs Legislation Amending Student Privacy Law*, THE ROANOKE TIMES (Mar. 15, 2019), https://www.roanoke.com/news/northam-signs-legislation-amending-student-privacy-law/article_def67d88-3679-5ec7-8ea2-7b86d042896f.html (last accessed Apr. 14, 2019).

226 H.B. 2449, 2019 Leg. Sess. (Va. 2019).

227 Friedenberger, *supra* note 225.

228 H.B. 2449, 2019 Leg. Sess. (Va. 2019).

229 *See, e.g.*, Forman *supra* note 197.

230 *See, e.g.*, 11 Reasons, *supra* note 152.

A. Trust: Understand the Role of Trust and Fear in Student Privacy Legislation

Privacy is an amorphous concept rooted in trust.[231] As a society, we want to trust that when institutions use our personal information to make decisions that affect our lives, they will use it fairly and protect it. FERPA and subsequent student privacy laws emerged in part from contexts in which the public had lost trust in institutions. FERPA arose in the aftermath of revelations about the Vietnam War and Watergate.[232] The wave of student privacy laws in 2014 followed the Edward Snowden leaks and major data breaches from trusted, everyday entities such as the retailer Target.[233] Virginia passed its restrictive data sharing law after legislators lost trust in the information sharing process, because one bad actor exploited the process and gained access to students' contact information.[234]

A profound sense of fear replaced this broken trust, both in the days of FERPA and in the past decade, informing public perceptions and driving privacy legislation. The fear of harm resulting from lack of privacy protections in part spurred FERPA, as people worried that schools were creating permanent student records to which parents had no access but that would follow students throughout their lives, potentially predetermining their opportunities and perpetuating discrimination.[235] Forty years later, several state student privacy laws, including those passed after the demise of inBloom, sought to address the fears that "personalized learning" would do the same—create a record that tracks students and predetermines their opportunities.[236]

Effectively addressing privacy harms means avoiding the instinctive response to do *something* in reaction to public fear, and, instead, approaching policymaking with intent to address the harms. First, reactive, hastily passed laws often do not address the actual harms. Although widespread fears about data breaches contributed to the 2014 deluge of student privacy laws, very

[231] Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559 (2015).

[232] Mary Margaret Penrose, *In the Name of Watergate: Returning FERPA to its Original Design*, 14 N.Y.U. J. LEGIS. & PUB. POL'Y 75, 94 (2011).

[233] Sonja Trainor, *Student data privacy is cloudy today, clearer tomorrow*, KAPPAN (Feb. 2015), at 13–14. https://iu.instructure.com/files/56302724/download?download_frd=1.

[234] *See* s*upra* Section III E.

[235] *See supra* Section II A.

[236] Ariel Bogle, *What the Failure of inBloom Means for the Student-Data Industry*, SLATE (Apr. 24, 2014, 3:45 PM), https://slate.com/technology/2014/04/what-the-failure-of-inbloom-means-for-the-student-data-industry.html. ("It's clear that legislators on both the federal and state level need to consider how to strengthen student privacy protections . . . [w]hile people seem willing to give up vast amounts of their own information to the cloud, there is a strict line when it comes to fears of a child's learning difficulties haunting her into middle age.").

few of those laws include data breach provisions.[237] Likewise, transparency measures that require stakeholders to navigate to a school district website to read contractual clauses is unlikely to quell fear of the unknown, such as "the cloud," complex technology, and technical jargon. Moreover, very few state student privacy laws require training for staff, making operationalizing data privacy practices a monumental task.[238]

Second, because rushed legislation often does not appropriately address the actual harms, most of the original fears catalyzing the laws remain, including fears of a permanent record, security breaches, the lack of transparency regarding data collection, improper sharing of student data, and general fear of the technological unknown.[239] Thus, it is not surprising that recent statistics still reflect low public trust overall in tech companies and significant fear of data breaches. The Pew Research Center reported in 2018 that only twenty-eight percent of Americans trust tech companies to do the right thing always or most of the time.[240] Another 2018 survey shows that eighty-three percent of respondents support tougher regulations and penalties for data privacy breaches.[241]

Policymakers should strive to understand the fears underlying privacy concerns, so they can address those fears effectively and, in doing so, gain the trust of education stakeholders. Sometimes, the response need not involve new legislation. Guidance explaining how current laws and frameworks apply to emerging issues can help stakeholders implementing laws to approach privacy compliance in flexible ways.[242] For example, the Department of Education periodically updates its FERPA "Frequently Asked Questions" guidance, to help schools and districts to better understand how

---

[237] *State Student Data Privacy Legislation: What Happened in 2014, And What's Next?*, DATA QUALITY CAMPAIGN (Aug. 2014), https://dataqualitycampaign.org/wp-content/uploads/2016/03/DQC-Data-Privacy-whats-next-Sept22.pdf.

[238] "Although more than 300 bills have been introduced over the past two years on student data privacy, few mention training." *See* Amelia Vance, *Policymaking on Education Data Privacy: Lessons Learned*, 2 EDUCATION LEADERS REPORT 2, 13 (Apr. 2016), www.nasbe.org/wp-content/uploads/Vance_Lessons-Learned-Final.pdf [hereinafter "Lessons Learned"].

[239] *See, e.g.*, *supra* Sections III B, C, D, E (discussing Louisiana, New Hampshire, Connecticut and Virginia's student privacy laws which required subsequent amendments due to unintended consequences).

[240] Aaron Smith, *Public Attitudes Toward Technology Companies*, PEW RESEARCH CENTER (June 28, 2018) http://www.pewinternet.org/2018/06/28/public-attitudes-toward-technology-companies.

[241] HarrisX, *Inaugural Tech Media Telecom Pulse Survey 2018*, available at http://harrisx.com/wp-content/uploads/2018/04/Inaugural-TMT-Pulse-Survey_-16Apr18_Library_V3.pdf.

[242] *Guidance Documents from Federal Agencies*, Government Accountability Office (May 18, 2015) https://www.gao.gov/assets/670/669721.pdf.

to comply with the law in a constantly changing educational environment.[243]

B. Transparency and Inclusion: No Legislation Without Representation

Transparency and inclusion are integral to building trust in privacy legislation.[244] Transparency in student privacy laws is essential both as part of the laws' content and for the process of creating effective laws.[245] Similarly, inclusion is essential for obtaining stakeholders' expertise to ensure the laws work as intended and also to encourage stakeholders to buy in to carefully considered efforts to protect students' data.

Policymakers can build trust by communicating with stakeholders about why student privacy laws are necessary. Many laws protect data but do not explain why the data is needed in the first place.[246] Better data can lead to more effective teaching and learning,[247] but if parents and other stakeholders do not understand how data can help students, they will not understand how or why the state needs to protect the privacy and security of the data.[248] They may demand that schools not collect data at all. Thus, a key part of transparency involves communicating the value of data, but also why education agencies partner with companies to store, analyze, and protect data.

It is equally important for policymakers to understand how transparency works in the laws themselves and to practice transparency in the process of creating the laws. Legislators are not always aware of how transparency should function in strong privacy legislation—for example, in the Connecticut law, legislators decided that transparency meant notification to parents within five days of every school contract with edtech vendors.[249]

[243] U.S. Dept. of Educ., *Frequently Asked Questions*, https://studentprivacy.ed.gov/frequently-asked-questions (last visited Mar. 6, 2020).

[244] *See generally* Neil Richards and Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016).

[245] Lessons Learned, *supra* note 238.

[246] Richards & Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. at 433 (2016) ("So much of modern networked life is mediated by information relationships, in which professionals, private institutions, or the government hold information about us as part of providing a service. Such relationships are everywhere we look.").

[247] "Data is one of the most powerful tools to inform, engage, and create opportunities for students along their education journey—and it's much more than test scores. Data helps us make connections that lead to insights and improvements." *Why Education Data?*, DATA QUALITY CAMPAIGN, https://dataqualitycampaign.org/why-education-data/ (last visited Apr. 14, 2020).

[248] *Empowering Parents and Communities through Quality Public Reporting*, DATA QUALITY CAMPAIGN (April 20, 2015), https://dataqualitycampaign.org/resource/empowering-parents-communities-quality-public-reporting/

[249] *See* Act Concerning Student Data Privacy, Pub. Act No. 16-189, § 2 (g) (effective October 1, 2016); Vance, *supra* note 169.

This resulted in excessive notices that did not help parents understand how their children's privacy was protected.[250]

To understand how transparency should work in student privacy laws, lawmakers need to practice inclusion in two ways: they need to include all stakeholders who will implement and be affected by the law, which will encourage these parties to buy into legislators' efforts; they also need to get the right input from experts to understand key concepts, which will facilitate effective bills. Inclusion is essential because, for example, if the disability rights community is left out of the consultation process, they may rightly believe that student privacy laws create further barriers for students with special needs. Such lack of transparency can severely undermine even well-intentioned laws.

To obtain input from experts, policymakers should with consult those who implement the law, are regulated by it, affected by it, and those with additional expertise.[251] These stakeholders include educators, district officials, state leaders, lawyers, and technology experts and vendors, all of whom bring immeasurable value and perspective to the conversation.[252] Many legislators were students long before tablet computers and edtech apps were a standard part of curricula.[253] Modern data protections or new technologies that seem reasonable to laypeople may strike experts as impossible or unwise. One of the most common problems that occurred as student privacy legislation was introduced in states in 2013 and 2014 centered around school memorabilia like photos and yearbooks. In addition to the problems in Louisiana described above, some bills proposed banning the use of "portable media devices" to store or transmit student personally identifiable information (PII). However, since photos were considered student PII in most proposed bills, these bills would have banned cameras.[254]

For these reasons, seeking guidance from the right stakeholders regarding the twenty-first century classroom is essential. The National Association of State Boards of Education (NASBE) recommends "[a]sking those who have to implement laws how they would affect their districts or schools" as a best practice to help decrease unintended consequences.[255]

Not only does consulting with stakeholders help avoid such consequences, it also ensures that policies and laws are practical and can be

250 Vance, *supra* note 169.

251 Future of Privacy Forum, *The Policymakers Guide to Student Data Privacy*, FERPASherpa (April 4, 2019) https://ferpasherpa.org/policymakersguide.

252 *Id.* at 10.

253 Online learning environments first started to appear in 1995, and only became routine starting in 2008. *See* A.W. (Tony) Bates, *Teaching in a Digital Age*, at 6, 2 (October 10, 2019) https://opentextbc.ca/teachinginadigitalage/.

254 Lessons Learned, *supra* note 238, at 11.

255 Lessons Learned, *supra* note 238, at 11.

implemented. If Congress had held hearings and called for public comments before enacting FERPA, the uncertainties regarding student loans and letters of recommendation might have been addressed before the law went into effect. If New Hampshire's legislature had consulted with teachers before banning video recordings, lawmakers likely would have learned that recordings are required as part of some students' IEPs.

Policymakers can incorporate stakeholders' input at many points during the legislative process. The West Virginia State Board of Education, for example, held statewide public forums to help communities understand how the state gathered and protected students' data.[256] Another Connecticut student privacy law, the Act Concerning Students' Right to Privacy in Their Mobile Electronic Devices, required the state to establish a diverse working group of representatives from the Commission on Women, Children, and Seniors; the Association of Public School Superintendents; the Center for Children's Advocacy; and the ACLU.[257] The working group was tasked with providing recommendations for a statewide policy on student mobile phone searches and seizures.[258] By mandating the convening of diverse perspectives on student privacy, the Act laid the foundation for sustained conversations and collaborative relationships.[259] Other states, such as Maryland and New York, have laws that mandated working groups to review current student privacy laws or provide input on regulations.[260] These types of official working groups can be invaluable by providing a designated space for diverse stakeholders to learn about and weigh in on student privacy issues.

C. Context: Foresight from the Field

Inclusion and transparency allow legislators to understand the context in which education stakeholders use student data and implement privacy safeguards. This process allows policymakers to, in the words of Louisiana privacy expert Kim Nesmith, be aware of "what they don't know. It doesn't matter who you are, but the reality is we sometimes don't recognize there are

---

[256] Amelia Vance, *West Virginia's Steady Course on Student Data Privacy*, NASBE (February 2016), http://www.nasbe.org/state-innovation/west-virginias-steady-course-on-student-data-privacy/.

[257] H.B. 5170, 2018 Leg. Sess. (Conn. 2018).

[258] H.B. 5170, 2018 Leg. Sess. (Conn. 2018).

[259] H.B. 5170, 2018 Leg. Sess. (Conn. 2018).

[260] *See* Ann. Code of Maryland, Education. Art. 1, § 7-2001-2005. (Md. 2018); McKinney's Education Law § 2-d(4)(b) and § 2-d(5), 2 (N.Y. 2019); New York State Education Department, *Proposed Addition of Part 121 to the Regulations of the Commissioner Relating to Student Privacy* (Jan. 3, 2019) at 21, https://www.regents.nysed.gov/common/regents/files/119p12d1.pdf.

things we don't know, and we don't know what that is."[261] The more that stakeholders participate in the legislative process of crafting student data privacy laws, the more deeply legislators will understand the nuances and implications of privacy regulations in education.

Context is particularly important at the state level, where policymakers need to understand not only current federal requirements, but also what is happening on the ground in classrooms throughout their state. For example, most of the 130 student privacy laws passed since 2013 have not provided funding or training for implementation.[262] As privacy experts have noted,"[c]ompared to large businesses, schools have far less funding and technical expertise. Even large school districts are hard pressed to keep up with the continual security alerts, patches, and updates needed to maintain secure systems of their own."[263] In this context, sweeping legislation with strict penalties coupled with lack of funding for training and implementation, as occurred in Louisiana, can cause panic and paralysis in schools.[264] Without people on the ground who know how to protect student privacy and have the resources to do so, schools will struggle to comply with privacy laws.[265] For this reason, context in this realm also means analyzing the effects of laws in other states, which may reflect consequences to avoid or useful models to consider.

Similarly, it is unwise to limit how schools use third parties without first understanding how and why schools partner with them in the first place. Most schools use private companies to assist with digital technology and student data because districts simply do not have the human or technical resources to build and manage the required systems.[266] Consequently, banning third parties may seriously disrupt school systems, particularly in small and under-resourced districts, which cannot build in-house capital and attract in-house expertise.

D. Clarity

Deep understanding of the context of student data and privacy laws

---

[261] *SXSWedu: Accidental Consequences of Student Privacy Laws Panel*, *supra* note 133.

[262] Lessons Learned, *supra* note 238, at 11.

[263] Joseph Jerome and Jules Polonetsky, *Student Data: Trust, Transparency and the Role of Consent*, Future of Privacy Forum (Oct. 2014), https://fpf.org/wp-content/uploads/FPF_Education_Consent_StudentData_Oct2014.pdf.

[264] *See, e.g.*, *supra* Section III B.

[265] *See* Emily Tate, *What It's Like Navigating the Strictest Student Privacy Law in the Country*, ED SURGE (Jun. 18, 2019) https://www.edsurge.com/news/2019-06-18-what-it-s-like-navigating-the-strictest-student-privacy-law-in-the-country (interview with Kim Nesmith discussing the importance of training or assisting districts with navigating new student privacy laws and Louisiana's approach through its Data Governance and Privacy Guidebook).

[266] Lessons Learned, *supra* note 238, at 5.

allows policymakers to draft clear, balanced legislation. Here, clarity means defining actual threats and how laws intend to address them, ensuring that legislative language is targeted and specific, and defining key terms. First, laws should clearly explain how privacy provisions will mitigate actual privacy threats, and these provisions should be evidence-based and vetted by privacy experts. In the above-mentioned Connecticut law, it was unclear how increased parental notification actually helped to protect students' data.[267]

Second, the case studies also demonstrate how vague, sweeping language can create serious problems when stakeholders try to implement privacy laws. The sponsor of New Hampshire's law intended to prevent teachers from having their classrooms recorded without their consent and to protect students' privacy in classrooms where recording occurred.[268] Yet, the law's sweeping language ("No school shall record in any way a school classroom for any purpose without school board approval after a public hearing, and without written consent of the teacher and the parent or legal guardian of each affected student") seemed to allow no exceptions for IEPs and other necessary cases.[269] The law's vagueness also left school districts wondering how many public hearings and consent forms were required for each recording.[270] Such vague language results in misinterpretations and misapplications of the same law. Those implementing the law may construct their own standards to meet their particular needs, which may contradict the law's original intent.

Third, creating precise legislative language means defining key terms. Debating FERPA's original language, Senator Buckley responded as follows to criticisms of the ambiguous language regarding parental consent for research and experimental programs: "In general, the premise is that parents are generally responsible adults, having prime responsibility for their children. I have no doubt that they would act responsibly."[271] Here, Buckley assumed that parents, as rational actors, would allow their children to participate in indisputably beneficial experimental programs, such as "new math." Yet, in doing so, he apparently believed that all parents would understand the term "experimental" in the same way.

More recent examples of this issue include a 2013 executive order signed into Georgia law. The executive order prohibited education agencies

267 *See* H.B. 5170, 2018 Leg. Sess. (Conn. 2018).

268 Zelin, *supra* note 156.

269 Morrill*, supra* note 149.

270 Morrill*, supra* note 149.

271 120 CONG. REC. 14588 (1974) (containing the Senate Floor debate where Buckley posited that parents are ultimately responsible for their children—and their children's data—not educational institutions).

from tracking, housing, reporting or sharing "psychometric data" with the federal government without defining the term.[272] The common definition of "psychometric" is information that is designed to show someone's personality, mental ability, or opinions, i.e., "any measurement of learning."[273] Left undefined, this prohibition could be understood to ban Georgia schools from tracking, housing, reporting or sharing student homework assignments or testing outcomes because they evaluate student learning. Legislators should therefore define key terms precisely and consider potential misinterpretations, particularly by seeking feedback from stakeholders.

E. Create a Culture of Privacy

Unintended consequences notwithstanding, student privacy legislation, from FERPA to state laws in the twenty-first century, have encouraged public awareness of students' right to privacy.[274] Many states and school districts now have data governance plans, and third parties are more accountable for their responsibilities regarding student data.[275] Practitioners and stakeholder organizations have developed hundreds of new resources to better protect students' privacy.[276]

Nonetheless, significant hurdles and threats remain. School administrators have many extremely important responsibilities, and privacy may feel unimportant compared to ensuring students have enough food or raising graduation rates. The initial attention brought by a federal law such as FERPA or a state law such as Louisiana's does not foster ongoing student privacy awareness; once public interest in the new requirements subsides, there is no incentive for continued privacy discussions or initiatives. Moreover, state and federal legislators continue to introduce poorly crafted

---

[272] *Deal executive order protects students, local control*, GEORGIAGOV (May 15, 2013), https://web.archive.org/web/20140109013246/https://gov.georgia.gov/press-releases/2013-05-15/deal-executive-order-protects-students-local-control.

[273] *See Psychometric*, CAMBRIDGE ADVANCED LEARNER'S DICTIONARY & THESAURUS (last visited Apr. 15, 2020) https://dictionary.cambridge.org/us/dictionary/english/psychometric; *see also* Amelia Vance, *Regulating Student Data Privacy: Don't Throw the Baby Out with the Bathwater*, NASBE (April 2015), http://www.nasbe.org/policy-update/regulating-student-data-privacy-dont-throw-the-baby-out-with-the-bathwater.

[274] *See, e.g.*, *supra* Section III A (discussing inBloom and the reaction from parents and other stakeholders which ultimately led to its downfall).

[275] Benjamin Herold, *Are State Student-Data-Privacy Laws Changing Companies' Behavior?*, EDUCATION WEEK MARKET BRIEF (Jan. 2, 2019), https://marketbrief.edweek.org/market-trends/state-student-data-privacy-laws-changing-companies-behavior.

[276] Resources, FERPASHERPA (last visited Apr. 15, 2020) https://ferpasherpa.org/resources.

student privacy bills.[277] General consumer privacy bills have also emerged that may present unintended consequences for schools.[278] Some student privacy laws require training but do not provide the resources to conduct it.[279] Without such resources, districts and states may shut down innovation in the face of privacy concerns or requirements, rather than adopt appropriate safeguards.[280] Education stakeholders at all levels still struggle to understand the effects of the dramatic changes in the student privacy landscape.[281]

For this reason, legislators should address the lack of incentives for engagement about student data privacy. They can do so by legislating to help schools and districts create a culture of privacy. The principles discussed above provide a roadmap for creating legislation that supports such a culture. Several states, such as Utah, have begun to lead the way–for example, Utah's student privacy law not only mandates student privacy protections; it also requires an annual student privacy course for educator relicensure.[282] In this way, it underscores the importance of continuing privacy education by creating a recurring obligation to keep privacy concerns at the forefront of educators' minds.

V. CONCLUSION

Student data can be used to improve education outcomes, close achievement gaps, and inform fair distribution of resources. By reacting to privacy concerns without fully understanding their context or the landscape in which privacy laws will function, however, legislators risk greater harm to students in the form of unintended consequences. Policymakers should therefore solicit input from stakeholders and communicate with the public, prior to the passage of laws, to identify such consequences. Lawmakers must seek to protect students' privacy with fair, balanced laws that ensure that

---

[277] *See, e.g.*, *supra* Sections III B, C, D & E (discussing Louisiana, New Hampshire, Connecticut, and Virginia's poorly drafted student privacy laws that failed to account for unintended consequences when initially passed); S.B. 1341 § 6(d), 114th Cong. (2015-16) (Senator Vitter's bill)

[278] *See, e.g.*, Anisha Reddy, Tyler Park and Amelia Vance, *Child Privacy Protections Compared: California Consumer Privacy Act v. Proposed Washington Privacy Act*, FUTURE OF PRIVACY FORUM (Jan. 27, 2020), https://fpf.org/2020/01/27/child-privacy-protections-compared-california-consumer-privacy-act-v-proposed-washington-privacy-act.

[279] Lessons Learned, *supra* note 238, at 11.

[280] *See, e.g.*, *School Districts Struggle To Comply With New Student Data Privacy Law*, Connecticut Public Radio (June 4, 2018) (accessed Apr. 14, 2020) https://www.wnpr.org/post/school-districts-struggle-comply-new-student-data-privacy-law (discussing forgoing the use of a game design app used in Advanced Placement classes for privacy concerns).

[281] *See supra* Sections II & III (highlighting examples of unintended consequences resulting from both federal and state-level student privacy legislation and the dramatic changes that resulted).

[282] Utah Code § 53E-9-204 (2019).

schools can safely use data and technology to support equitable learning and opportunities for all students.