STRANGER DANGER!: HOW HACKERS BREAK INTO SCHOOL DATABASES TO STEAL STUDENT DATA, AND WHAT LEGISLATURES SHOULD DO ABOUT IT

Rebekah Luna[*]

* J.D. Candidate, Texas Tech School of Law, May 2022.

I. THE GROWING PROBLEM OF INADEQUATE SCHOOL CYBERSECURITY

Schools are common targets for data theft operations, and there is little legislation in place to mitigate the harm these operations cause.[1] Cyber-criminals who wish to steal personal information on Americans often prefer that of children because of its high value on the dark web.[2] Schools are therefore attractive targets for data thieves, who are usually skilled in the art of "hacking."[3] Adding to the attraction, schools generally have minimal protections in place, considering the value of the information they collect and store.[4] In almost every other non-educational sector, entities that maintain confidential information on individuals are held to higher legal standards when it comes to protecting that information.[5] But, because of sovereign immunity, schools are not held legally accountable when cybersecurity breaches of their databases result in the theft of their students' information.[6] To make matters worse, even though these incidents are common, schools also do not have a clearly defined legal duty to take concrete preventative action against these breaches.[7]

To determine the legal duty that schools do have, it is necessary to analyze federal and state laws in place approaching this problem and determine how they work together to guide schools' cybersecurity efforts. One of the main federal laws that touches school cybersecurity, the Federal Educational Rights and Privacy Act (FERPA), forbids the disclosure of certain student information to third parties, but it does not provide

---

1. Nicholas Bogel-Burroughs, *Hackers' Latest Target: School Districts*, N.Y. TIMES (July 28, 2019), https://www.nytimes.com/2019/07/28/us/hacker-school-cybersecurity.html.

2. Emily Wilson, *The Worrying Trend of Children's Data Being Sold on the Dark Web*, THE NEXT WEB (Feb. 23, 2019, 7:30 PM), https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/; Alexandria White, *How to Protect Your Child from Identity Theft*, CNBC, https://www.cnbc.com/select/how-to-protect-child-from-identity-theft/ (last updated Feb. 23, 2021); Al Pascual & Kyle Marchini, *2018 Child Identity Fraud Study*, JAVELIN STRATEGY (Apr. 24, 2018), https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study; *Release: Connolly Amendment to Protect Kids From Online Predators Passes House*, GERRY CONNOLLY (Feb. 4, 2010), https://connolly.house.gov/news/documentsingle.aspx?DocumentID=158; *see Understanding the Basics of the Dark Web*, IRS, https://www.irsvideos.gov/Webinars/UnderstandingBasicsDarkWeb (last visited Sept. 21, 2021) (providing general information on the dark web); *Election Security Spotlight—The Surface Web, Dark Web, and Deep Web*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web/ (last visited Sept. 21, 2021).

3. *Hacking*, TECHOPEDIA (Mar. 27, 2020), https://www.techopedia.com/definition/26361/hacking.

4. Bogel-Burroughs, *supra* note 1.

5. *See infra* notes 150–171 and accompanying text (explaining how non-educational sectors approach cybersecurity).

6. *See infra* Section II.D.1 (explaining how sovereign immunity usually precludes litigation with schools).

7. *K-12 Cybersecurity 2019 Year in Review, Part III: Cybersecurity Incidents: 2019*, K-12 CYBERSECURITY RES. CTR., https://k12cybersecure.com/year-in-review/2019-incidents/ (last visited Sept. 21, 2021).

recompense for student or staff victims when their information is compromised.[8] The other key federal cybersecurity law, the Computer Fraud and Abuse Act (CFAA), criminalizes data theft and unauthorized hacking and provides a civil remedy for victims, but the remedy is only available when the cyber-criminal is caught.[9] State laws are similarly limited.[10] Though every state has passed some form of school cybersecurity legislation, many of them focus only on third-party relationships to schools' databases,[11] and the ones that do require schools to implement cybersecurity measures do not detail exactly what those measures should be, so it is difficult to ascertain when the school has met the legal duty.[12]

Despite the scarce direction in place, federal and state governments have begun to realize the seriousness of cybersecurity concerns in the United States, as evidenced by attempts at legislating a solution in recent years.[13] But in establishing new school laws, legislatures are cautious of overstepping their bounds and asking more of schools than schools are equipped to handle and more of schools than governments are willing to fund.[14] To date, lawmakers have put forth only vague cybersecurity instructions for schools to follow, have implemented no oversight and accountability measures for those instructions, and have provided almost no legal remedy for the student victims.[15]

An analysis of the current state of school cybersecurity legislation in the United States reveals that there is a gap in this area of the law.[16] Because K-12 schools are such attractive targets for data thieves and are, therefore, vulnerable to cyberattacks, Congress should recognize a legal duty of schools to protect student data.[17] It should do so by passing legislation requiring schools to implement secure data collection and cybersecurity practices, and it should provide the necessary funding to make that happen.[18]

This Comment presents a map to one legal solution for the nearly ubiquitous problem of student data theft in America's public schools.[19] Part

---

8. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

9. Computer Fraud and Abuse Act of 1986 (CFAA), 18 U.S.C. § 1030.

10. *See infra* Section II.D (discussing the limitations of state cybersecurity laws).

11. *See, e.g.*, H.B. 2716, Reg. Sess. (Kan. 2020); H.B. 745, 66th Leg. Reg. Sess. (Mont. 2019); H.B. 158, Gen. Sess. (Utah 2020).

12. *See, e.g.*, TEX. CIV. PRAC. & REM. CODE ANN. § 101.021; VA. CODE ANN. § 22.1-20.2 (2015); A.B. 2097, 2016 Reg. Sess. (Cal. 2016), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB2097.

13. *See, e.g.*, Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/2092#:~:text=Prohibits%20an%20operator%20of%20a,behavior%20or%20use%20of%20online.

14. *See* Bogel-Burroughs, *supra* note 1.

15. *Infra* Sections II.B, II.C (discussing the lack of guidance and legal remedy for schools).

16. *See infra* Sections II.B, II.C (analyzing the current state of school cybersecurity legislation).

17. *See infra* Part III (discussing potential federal school cybersecurity legislation).

18. *See infra* Part III (proposing legislation to protect K-12 data).

19. *See infra* Part III (proposing legislation to protect K-12 data).

II details the current state of school cybersecurity, explains why and how K-12 schools are attractive targets for cyber-criminals, and details the dangers of not protecting student data.[20] It also details how the laws in place interact with schools in their cybersecurity efforts and provides a glimpse of how non-education sectors approach cybersecurity.[21] Part III provides model legislation that leaves no questions as to how exactly schools should approach cybersecurity and provides recompense for victims of data theft when cybersecurity measures fail.[22] Part III also shows that the current statutes imposing a legal duty on schools are outdated and draws analogies between the education sector and other modern sectors for which the law recognizes a duty to protect data.[23]

II. THE CURRENT STATE OF K-12 SCHOOL CYBERSECURITY LAWS AND PRACTICES

Several factors contribute to the growing cybersecurity problem in schools.[24] Below, Section A details not only the consequences for individuals of data exposure and theft but also explains that schools often lack the financial resources and expertise effective cybersecurity requires.[25] It also shows that gaps exist in the education of school leaders responsible for dealing with student personal identifying information (PII).[26] Section B discusses how the federal laws that touch school cybersecurity do not provide guidance or assistance for specific cybersecurity practices.[27] Section C discusses federal codified law affecting data security, as well as other federal efforts to secure data.[28] Section D explains the role of sovereign immunity in litigation with schools and discusses how state laws do not provide specific instructions for schools or a remedy for victims of school cybersecurity breaches.[29] Finally, Section E explores how other sectors approach cybersecurity and compares those approaches to that of schools.[30]

20. *Infra* Part II (explaining why and how K-12 schools are attractive targets for cyber-criminals).
21. *Infra* Part II (explaining why and how K-12 schools are attractive targets for cyber-criminals).
22. *See infra* Part III (providing model legislation as to how schools should approach cybersecurity).
23. *See infra* Part III (providing model legislation as to how schools should approach cybersecurity).
24. Bogel-Burroughs, *supra* note 1.
25. *See infra* Section II.A (detailing the consequences for individuals of data exposure and theft).
26. *See infra* Section II.A (showing that gaps exist in the education of school leaders).
27. *See infra* Section II.B (discussing how federal laws that touch school cybersecurity do not provide guidance or assistance for specific cybersecurity practices).
28. *See infra* Section II.C (discussing federal statutes and efforts influencing data security).
29. *See infra* Section II.D (explaining the role of sovereign immunity in litigation).
30. *See infra* Section II.E (exploring how other sectors approach cybersecurity).

A. The Substantial Risk of Data Exposure in K-12 Schools

Because schools collect so much data from their students and staff, they are attractive targets for hackers who wish to steal data and sell it on the dark web.[31] These types of cybersecurity hacks result in a myriad of problems for all the different stakeholders in schools.[32] The most common problem is that students and staff can have their identities stolen, but cybersecurity breaches can also lead to other harms.[33] The law provides almost no protection for this data, which schools are supposed to safeguard, and no remedy for victims of data theft when the theft is connected to a school.[34] For context, in 2017, schools in the United States reported 122 cybersecurity incidents,[35] many of which "were significant, resulting in the theft of millions of tax payer dollars, stolen identities, tax fraud, and altered school records."[36] This number only includes those incidents which were detected and reported, so the real number of data thefts is likely much higher.[37]

The uptick in cybercrimes stems from the lucrative business of dealing in PII online.[38] The value of data to hackers is that it can be sold on the dark web to people who wish to use it for their own financial gain.[39] While identity theft is the most common crime associated with data breaches, there are several ways to monetize stolen data: blackmail, hacktivism,[40] and

---

31. Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PC MAG. (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web; Wendy Zamora, *What K-12 Schools Need to Shore up Cybersecurity*, MALWAREBYTES LABS (Nov. 21, 2019), https://blog.malwarebytes.com/101/2019/02/k-12-schools-need-shore-cybersecurity/; Bogel-Burroughs, *supra* note 1.

32. "Stakeholders" refers to the people who have an interest in education, including families, students, teachers, administrators, staff, and even the surrounding community. *See* Kaleigh C. Fitzpatrick, *Student Data at Risk: A Multi-Tiered Approach for Massachusetts to Mitigate Privacy Risks While Utilizing Innovative Education Technology in Schools*, 16 J. HIGH TECH. L. 294, 300-01 (2016).

33. *Child Identity Fraud Hit More Than One Million U.S. Victims in 2017 According to New Javelin Strategy & Research Study*, JAVELIN (Apr. 24, 2018), https://www.javelinstrategy.com/node/59561; Steve Zurier, *8 Ways Hackers Monetize Stolen Data*, DARK READING (Apr. 17, 2018), https://www.darkreading.com/attacks-breaches/8-ways-hackers-monetize-stolen-data----------/d/d-id/1331560?image_number=9.

34. *See infra* Sections II.C, II.D (discussing lack of federal and state remedies in comparison to other sector's approaches regarding cybersecurity).

35. Benjamin Herold, *Schools Suffered at Least 122 Cybersecurity Incidents Last Year*, EDUC. WEEK (Feb. 7, 2019), http://blogs.edweek.org/edweek/DigitalEducation/2019/02/schools_cybersecurity_incidents_2018.html.

36. *As Public Schools Embrace Technology, Cybersecurity Incidents Grow Both More Common and More Significant*, K-12 CYBERSECURE (Feb. 7, 2019), https://k12cybersecure.com/2018-year-in-review/2018-press-release/.

37. *Id.*

38. Zurier, *supra* note 33.

39. *Id.*

40. Hacktivism is the use of hacking to affect change or bring awareness to a cause. Patrick Putman, *What is Hacktivism?*, U.S. CYBERSECURITY MAG., https://www.uscybersecurity.net/hacktivist/ (last visited Sept. 21, 2021).

ransomware are just a few examples.[41] Data thieves work by first obtaining PII about a person or group of people.[42] PII includes names, addresses, phone numbers, parents' names, and sometimes other ID numbers like social security numbers or school-issued ID numbers.[43] Criminals use several techniques to gain this data, ranging from complicated phishing schemes to simply grabbing a poorly-disposed-of physical sheet of paper from a trash can.[44] They then sell this information on the dark web.[45] Normally, adult PII is listed in bundles of about 100 persons' information for between $4–$6 a bundle.[46] PII of minors is usually sold individually, for about $100 per minor.[47] Prices vary depending on the amount of PII for sale, the age of the data's owners, their credit score information and quality, and the newness of the information.[48] Once the information is sold, the person who initially stole it usually vanishes,[49] becoming untraceable, and buyers can use it to do whatever they want, which is usually to commit identity theft or open a new line of credit.[50] Because children generally do not have any credit history, it is easy for criminals to use their PII, especially their social security numbers (usually combining such information with fake names), to open lines of credit for months or years without being detected, which is why minors' information is so valuable.[51]

To protect this valuable information, most school districts have installed some form of cybersecurity software into their district networks, but software alone cannot prevent cyberattacks.[52] For a cybersecurity plan to be effective, it must invoke more than one line of defense, and cybersecurity awareness is often key.[53] Teachers and other school staff who deal with data often lack training on common cybersecurity pitfalls, such as: using the same password

41. JAVELIN, *supra* note 33; Zurier, *supra* note 33.

42. *See* Joseph Krebs, *From Jacob to Target: A New Approach Is Needed to Combat Identity Theft*, 18 DUQ. BUS. L.J. 15, 19 (2016).

43. *Id.*

44. *Id.*

45. Miguel Gomez, *Dark Web Price Index 2020*, PRIV. AFFS., https://www.privacyaffairs.com/dark-web-price-index-2020/ (last updated Sept. 5, 2021).

46. *Id.*

47. *Id.*

48. *Id.*

49. *See* Charles Orton-Jones, *Catching Hackers is Not Getting Easier*, RACONTEUR (Mar. 8, 2016), https://www.raconteur.net/technology/cybersecurity/catching-hackers-is-not-getting-easier/; *see also* Nadav Avital & Gilad Yehudai, *The Trickster Hackers—Backdoor Obfuscation and Evasion Techniques*, IMPERVA (July 11, 2018), https://www.imperva.com/blog/the-trickster-hackers-backdoor-obfuscation-and-evasion-techniques/ (explaining why hackers can so easily become untraceable).

50. Krebs, *supra* note 42, at 27.

51. CONNOLLY, *supra* note 2; Pascual & Marchini, *supra* note 2.

52. Bogel-Burroughs, *supra* note 1.

53. Remesh Ramachandran, *The Importance of Training: Cybersecurity Awareness like a Human Firewall*, ENTREPRENEUR (Oct. 15, 2019), https://www.entrepreneur.com/article/340838; *The Importance of Training: Cybersecurity Awareness As a Firewall*, FORBES (Aug. 27, 2019), https://www.forbes.com/sites/insights-fortinet/2019/08/27/the-importance-of-training-cybersecurity-awareness-as-a-firewall/?sh=2b1ce8c68b4b.

for multiple accounts; electing to stay logged in instead of typing a password every time they access information; or sharing confidential information in an unencrypted format via email or text—especially on personal electronic devices not connected to (or protected by) school networks.[54] Schools often lack funding to install software on every device that touches student information, especially because so many school employees use personal devices for school business.[55] Funding constraints also mean that the devices that are protected by software often do not feature the most cutting edge technologies that contain all the features necessary to protect against experienced hackers.[56] Sometimes districts do have funding but fail to understand the importance of using high-quality cybersecurity programs and opt for a less expensive and less effective one.[57] The inefficacy of school cybersecurity practices is traceable to the dealings of federal and state governments with the issue—specifically, their failure to require that schools utilize the most modern and effective defenses.[58]

B. Common Cybersecurity Practices

Though most schools lack the cybersecurity infrastructures necessary to protect student data, effective technology does exist.[59] Among the most effective software programs are threat detection and response systems, which identify and mitigate threats before IT professionals are even aware of them.[60] Encryption, another cybersecurity tool, is a way of scrambling data that is stored or sent within school cyberinfrastructure so that only those with permission can view it.[61] Virtual Private Networks (VPNs) protect a computer's privacy while it is connected to the internet by encrypting online traffic, even when the computer's user accesses public Wi-Fi networks.[62] They work as a digital mask, hiding private information about a computer and its user.[63] Firewalls secure computers by blocking access to unsecured

54. Mike Oswalt, *6 Practical Safeguards to Protect Student Data*, ILLUMINATE EDUC. (Aug. 3, 2017), https://www.illuminateed.com/blog/2017/08/6-practical-safeguards-protect-student-data/.

55. Bogel-Burroughs, *supra* note 1.

56. *Id.*

57. Ramachandran, *supra* note 53.

58. *See* Oswalt, *supra* note 54 (explaining practical safeguards to protect data).

59. *See infra* notes 60–68 and accompanying text (discussing common effective cybersecurity tools).

60. Nate Lord, *What is Threat Detection and Response? Solutions, Benefits, and More*, DIGIT. GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/what-threat-detection-and-response-solutions-benefits-and-more#:~:text=Threat%20detection%20and%20response%20is,may%20be%20required%20in%20response.

61. *What is Encryption?*, CLOUDFARE, https://www.cloudflare.com/learning/ssl/what-is-encryption/ (last visited Sept. 21, 2021).

62. Tim Mocan, *VPN vs. Firewall vs. Antivirus—What's the Difference?*, CACTUS VPN (July 19, 2018), https://www.cactusvpn.com/vpn/vpn-vs-firewall-vs-antivirus/.

63. *Id.*

websites and can prevent certain computer programs from connecting to the internet.[64] Finally, two-factor authentication (sometimes called two-step verification) is used by almost every major technology company, including Google and Amazon, and requires one additional element of proof of a user's identity beyond a username and password.[65] Commonly, after entering a password and username, a unique code is sent to another device, like a cell phone or tablet, to confirm that the person attempting to access the protected information has permission.[66]

Together, these components comprise standard data security frameworks used by high-stakes businesses and other entities with computer networks.[67] While no cybersecurity framework is impenetrable, these security tools provide the best defense against catastrophic data breaches and are well regarded in the cybersecurity community.[68] Furthermore, these types of safeguards are generally held as necessary for any effective cybersecurity endeavor, but are missing from all school cybersecurity legislation.[69]

C. Federal Codified Law Affecting Data Security & Efforts to Secure Data

The Constitution of the United States leaves the burden of providing public education to the states, but because of the compelling national interest the federal government has in ensuring effective public schools, the federal government, "through the legislative process, provides assistance" to states in their efforts to educate their citizens.[70] There is no federal law that specifically deals with school cybersecurity, but a few federal laws are currently in play that tangentially affect schools' cybersecurity efforts.[71] FERPA requires schools to keep certain student information confidential, and it is generally the federal law that school officials consider when they make decisions regarding student data privacy—inside the cybersphere and out.[72] The Student Privacy Policy Office sits within the Department of Education and manages how the federal government deals with student data it receives from individual schools and states.[73] The CFAA criminalizes cyber data theft,

64. *Id.*

65. Eric Griffith, *Two-Factor Authentication: Who Has It and How to Set It Up*, PC MAG. (Aug. 4, 2020), https://www.pcmag.com/how-to/two-factor-authentication-who-has-it-and-how-to-set-it-up.

66. *Id.*

67. Mocan, *supra* note 62.

68. *Id.*

69. *See infra* Sections II.C.1, II.C.2 (discussing the gap in state legislation when federal statutes do not provide effective remedies).

70. *10 Facts About K-12 Education Funding*, U.S. DEP'T OF EDUC., https://www2.ed.gov/about/overview/fed/10facts/index.html (last visited Sept. 21, 2021).

71. *See infra* Sections II.C.1, II.C.2 (explaining the effect of FERPA and CFAA on school cybersecurity).

72. *See infra* Section II.C.1 (explaining the effect of FERPA on school cybersecurity).

73. *See infra* Section II.C.1 (explaining the role of the Student Privacy Policy Office).

so people who steal data from schools could be prosecuted under the act.[74] Finally, the proposed Student Digital Privacy and Parental Rights Act of 2015, had it been passed, might have filled the existing gap in federal school cybersecurity law, and it serves as a jumping-off point for discussion of not only the state of federal school cybersecurity law but what provisions a new bill might contain.[75]

1. The Federal Educational Rights and Privacy Act and the Student Privacy Policy Office

Last amended in 2001, FERPA is the primary federal statute dealing with the protection of student data and privacy.[76] It establishes that students (and parents of minor students) have a right to know about the purpose, content, and location of PII that their institution keeps as part of their educational records.[77] Additionally, FERPA provides a waivable expectation of confidentiality for educational records.[78] The law also provides that a certain category of PII, directory information, such as name, address, telephone listings, and dates of attendance, may be disclosed to third parties without consent unless the eligible student has notified the school in writing that they do not want this information to be disclosed.[79]

Though FERPA is the primary legal guide for schools, as they deal with student data, it neglects to cover cybersecurity specifically.[80] This distinction is critical: FERPA addresses knowing, voluntary disclosures of PII, while cybersecurity policies address unknowing, involuntary disclosures of PII.[81] Schools are, therefore, left thinking that compliance with FERPA wholly satisfies their duty of care.[82] In fact, in most jurisdictions, they are correct in this thinking.[83]

---

74. *See infra* Section II.C.2 (explaining the effect of CFAA).

75. Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015).

76. FERPA, 20 U.S.C. § 1232g.

77. *Id.*; *DART Toolkit II: Legal Issues—FERPA Overview*, AM. PSYCH. ASS'N, https://www.apa.org/pi/disability/dart/legal/ferpa (last visited Sept. 21, 2021).

78. FERPA, 20 U.S.C. § 1232g; AM. PSYCH. ASS'N, *supra* note 77.

79. FERPA, 20 U.S.C. § 1232g; AM. PSYCH. ASS'N, *supra* note 77.

80. *See* FERPA, 20 U.S.C. § 1232g.

81. *See infra* Sections II.C.1, II.C.2 (explaining the effect of FERPA and CFAA on school cybersecurity).

82. FERPA, 20 U.S.C. § 1232g; AM. PSYCH. ASS'N, *supra* note 77.

83. FERPA, 20 U.S.C. § 1232g; AM. PSYCH. ASS'N, *supra* note 77; *see also* Lynn M. Daggett, *FERPA in the Twenty-First Century: Failure to Effectively Regulate Privacy for All Students*, 58 CATH. U. L. REV. 59, 67–69 (2009) (comparing schools' expectations of duties depending on jurisdictional interpretation of FERPA).

Similarly situated within the United States Department of Education is the Student Privacy Policy Office.[84] It "leads . . . efforts to protect privacy" by ensuring compliance with the several federal statutes intended to protect student information.[85] Generally, this office ensures the protection of student information within the Department of Education.[86] It is also the office responsible for investigating allegations of FERPA violations.[87]

2. The Computer Fraud and Abuse Act

Enacted in 1986, the Computer Fraud and Abuse Act (CFAA) is the federal law that criminalizes computer fraud, data theft, and provides relief to victims.[88] While FERPA focuses on the duty of schools in dealing with information, CFAA focuses on the bad actors—those who would steal data—and provides some relief to victims.[89] It was enacted to "deter and punish [a] new dimension of criminal activity" after Congress noticed a trend of criminals breaking into public and private computer systems.[90] It details the appropriate criminal penalty for various levels of cybercrime.[91] Importantly, it also attempts to provide a legal remedy for people whose data has been stolen under this act.[92] However, its pitfall is that it only provides that victims may "maintain a civil action against the violator" for damages.[93] As this Comment has already mentioned, this sort of remedy has not been effective for victims of data theft because the cyber-criminals that steal PII usually sell the information anonymously, and quickly, before vanishing.[94] It is very difficult to track them down, and the CFAA only provides a remedy against those hidden violators.[95] While the language of the statute seems to provide a remedy for victims, in reality, it does little to soften the blow of data theft.[96]

---

84. *US Department of Education Principal Office Functional Statements, Student Privacy Policy Office*, U.S. DEP'T OF EDUC., https://www2.ed.gov/about/offices/list/om/fs_po/opepd/intro.html#8 (last updated Nov. 8, 2019).

85. *Id.*

86. *Id.*

87. *Id.*

88. CFAA, 18 U.S.C. § 1030.

89. FERPA, 20 U.S.C. § 1239g; CFAA, 18 U.S.C. § 1030.

90. H.R. REP. NO. 98-894, at 10 (1984).

91. *See id.*

92. CFAA, 18 U.S.C. § 1030(g).

93. *Id.*

94. *See* K-12 CYBERSECURITY RES. CTR., *supra* note 7 (noting the effect of cyberthieves disappearing after stealing data).

95. CFAA, 18 U.S.C. § 1030(g).

96. *See* K-12 CYBERSECURITY RES. CTR., *supra* note 7.

3. The Proposed Student Digital Privacy and Parental Rights Act of 2015

The Obama Administration acknowledged part of this problem and sought to pass a bill—the Student Digital Privacy and Parental Right Act of 2015—that would begin to curtail it.[97] The fact that this was even discussed, however briefly, is evidence that there is a growing school cybersecurity problem and some government motivation and momentum to solve it.[98] This effort, in particular, was intended to "prevent companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school."[99] While its focus was on educational third parties and the responsibilities and parameters surrounding their encounters with student data, the bill would have also affected how schools handle student data.[100] Among other provisions, the bill required schools to develop and implement data security procedures and processes for responding to data breaches and notify en masse every stakeholder, including the Federal Trade "Commission . . . students, parents, educational agencies or institutions, or officials of such agencies or institutions (including teachers)" of data security breaches.[101] It also would have required schools to delete certain student information that is not required by law to be maintained by the school within forty-five days after a request from an educational agency, institution, or student's parent.[102] It also provided a requirement that school operators disclose publicly the types of PII they collect or generate and the third parties they disclose that information to.[103] The Obama Administration introduced the bill on April 29, 2015, but it did not receive a vote.[104]

D. The Role of Sovereign Immunity & States' Attempts to Mitigate the School Cybersecurity Problem

Despite the federal government's minimal school cybersecurity laws in place, since 2013, all fifty states have passed at least one student privacy

---

97. Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015) (as introduced to House of Representatives, Apr. 29, 2015).

98. *See id.*; Fitzpatrick, *supra* note 32.

99. Press Release, White House, Office of the Press Secretary, Fact Sheet: Safeguarding American Consumers & Families (Jan. 12, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families (announcing a newly proposed student data protection entitled Student Digital Privacy Act).

100. *Id.*

101. H.R. 2092(b)(2).

102. *Id.*

103. *Id.*

104. *H.R. 2092 (114th): Student Digital Privacy and Parental Rights Act of 2015*, GOVTRACK, https://www.govtrack.us/congress/bills/114/hr2092 (last visited Sept. 21, 2021).

law.[105] Most of these laws are narrowly tailored and limited in scope, so they necessarily only provide limited protection and relief for students.[106] This limitation of relief is generally due to the role of sovereign immunity when it comes to states (acting through schools) being sued.[107] Nevertheless, a few states have actually begun to outline the duty of schools regarding their stewardship of student data.[108] Key states that have taken substantive steps to protect student data are Texas, California, and Virginia.[109]

The scope of this Comment is limited to public K-12 schools, but because private schools would be affected by this proposed legislation as well, they are briefly mentioned.[110] The statute this Comment proposes only covers public schools, but because school attendance is compulsory in every state in the United States, all K-12 students are affected by cybersecurity breaches, so all families have an interest in the cyber-safety of their families.[111] If legislation like that modeled below passes, and public schools increase their cybersecurity and cyber-education efforts, private schools will likely at least rise to meet those same standards—if not exceed them.[112] Nevertheless, while cybersecurity in schools is a nationwide concern, public schools are functions of state governments, so a discussion of the laws surrounding them must include what currently exists at the state level.[113] This discussion will begin with a brief consideration of sovereign immunity. Below, sub-section 1 discusses how sovereign immunity affects school liability, and sub-sections 2, 3, and 4 discuss cybersecurity law in Texas, Virginia, and California, respectively.[114]

---

105. For a comprehensive list and summary of all recent state student privacy laws, see *State Student Privacy Laws*, STUDENT PRIV. COMPASS, https://studentprivacycompass.org/state-laws/ (last visited Sept. 21, 2021).

106. *Id.*

107. *Infra* Section II.C.1 (explaining the role that sovereign immunity plays in precluding litigation with schools).

108. *See, e.g.*, TEX. CIV. PRAC. & REM. CODE ANN. § 101.021; VA. CODE ANN. § 22.1–20.2 (2015); A.B. 2097, 2016 Reg. Sess. (Cal. 2016), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB2097.

109. *See infra* Sections II.C.2–3 (comparing current cybersecurity protection in different states).

110. *See infra* Sections II.D.1–3 (discussing how these laws affect private school security standards).

111. Table 5.1, *Compulsory School Attendance Laws*, NAT'L CTR. FOR EDUC. STAT., https://nces.ed.gov/programs/statereform/tab5_1.asp (last visited Sept. 21, 2021).

112. Private schools usually meet or exceed public school security standards. *See* Jude Schwalbach, *Students' Safety is No Small Consideration in Parents' Private School Choice*, HERITAGE (Dec. 3, 2018), https://www.heritage.org/education/commentary/students-safety-no-small-consideration-parents-private-school-choice#:~:text=Private%20school%20choice%20gives%20children,were%20previously%20out%20of%20reach.&text=Moreover%2C%20DeAngelis%20and%20Shakeel%20found,theft%20than%20at%20public%20schools (discussing private school safety standards).

113. U.S. DEP'T OF EDUC., *supra* note 70.

114. *See infra* Section II.D.1–4 (discussing the role of sovereign immunity and states' attempts to mitigate the school cybersecurity problem).

1. How Sovereign Immunity Protects Schools from Legal Accountability

Sovereign Immunity is the doctrine which holds that the government can only be sued if it has given consent.[115] It exists because the government (via schools) cannot do its job if it is constantly being taken to court for legal matters, regardless of their merit.[116] Additionally, the state purse would drain quickly if the government was sued every time a state employee behaved negligently.[117] School districts, in particular, have limited funds that must be spread widely to serve all the needs they are expected to meet.[118]

When these principles were used to write current school negligence law (like that in Texas), cybersecurity was not a prominent issue, so it was not considered.[119] Legislatures could have had no idea of the momentous challenges the internet would bring to concepts like safety and privacy, so legislatures did not consider it when they drafted sovereign immunity rules and their exceptions.[120]

Most state governments have given consent for suits against schools in a few narrow scenarios.[121] For example, through the Texas Torts Claims Act, Texas has recognized a few circumstances where a school (as the state) has a legal duty to act reasonably. In those circumstances, a school can be successfully sued when in violation of the Act.[122] For instance, a person in Texas can sue the state for property damage, personal injury, and death resulting from a state employee's negligence.[123] But, the catch is that injured parties can only bring suit if the injury arises from the employee's operation of a motor vehicle and if the employee would also be liable under Texas law.[124]

---

115. *Sovereign Immunity*, LEGAL INFO. INST. [hereinafter *Sovereign Immunity*], https://www.law.cornell.edu/wex/sovereign_immunity (last visited Sept. 21, 2021); *State Sovereign Immunity*, LEGAL INFO. INST. [hereinafter *State Sovereignty Immunity*], https://www.law.cornell.edu/constitution-conan/amendment-11/state-sovereign-immunity (last visited Sept. 21, 2021).

116. *Sovereign Immunity*, *supra* note 115; *State Sovereign Immunity*, *supra* note 115.

117. *Sovereign Immunity*, *supra* note 115; *State Sovereign Immunity*, *supra* note 115.

118. Linda Darling-Hammond, *America's School Funding Struggle: How We're Robbing Our Future by Under-Investing in Our Children*, FORBES (Aug. 5, 2019), https://www.forbes.com/sites/lindadarlinghammond/2019/08/05/americas-school-funding-struggle-how-were-robbing-our-future-by-under-investing-in-our-children/?sh=2507dbbc5eaf.

119. Caleb Townsend, *A Brief and Incomplete History of Cybersecurity*, U.S. CYBERSECURITY MAG., https://www.uscybersecurity.net/history/ (last visited Sept. 21, 2021); George Mutune, *The Quick and Dirty History of Cybersecurity*, CYBER EXPERTS, https://cyberexperts.com/history-of-cybersecurity/#:~:text=The%20history%20of%20cybersecurity%20starts,a%20priority%20for%20every%20organization (last visited Sept. 21, 2021).

120. Townsend, *supra* note 119; Mutune, *supra* note 119.

121. *Sovereign Immunity*, *supra* note 115; *State Sovereign Immunity*, *supra* note 115.

122. TEX. CIV. PRAC. & REM. CODE ANN. § 101.021.

123. *Id.*

124. *Id.*

2. Texas's Attempts to Safeguard Student Data: A Step in the Right Direction

Despite the limitations of sovereign immunity, Texas has taken steps to protect student data.[125] The primary Texas statute for student data security includes in most relevant part: "Each school district shall adopt a cybersecurity policy to[:] (1) secure district cyberinfrastructure against cyber attacks and other cybersecurity incidents; and (2) determine cybersecurity risk and implement mitigation planning."[126] Texas has recognized a need to require that schools do something in terms of cybersecurity, but the language of this statute is limited to the identification of the need.[127] Questions remain regarding what it looks like to "secure district cyberinfrastructure" and how schools should "determine cybersecurity risk and implement mitigation planning."[128] The Texas Legislature meant to protect student data, but it only required in practice that schools make a showing of some effort in that direction, so they did not achieve their goal.[129]

Texas's statutory instruction for school districts to assess cybersecurity risks establishes a foundation for cybersecurity risk management because it is impossible to mitigate risks unless the risks are known and documented.[130] However, the statutory instruction places the additional burden of risk assessment onto each individual school instead of leaving that task to state officials.[131] Though this instruction is for each independent school district to complete, the cybersecurity risks facing schools are not necessarily unique from one to another.[132]

Texas also requires that schools notify students and their families of cybersecurity breaches within a reasonable time.[133] What remedy is available to families in those situations is unclear.[134] If there is a breach and the school does notify the student in a timely manner, state laws provide no relief for the victims.[135]

---

125. TEX. EDUC. CODE ANN. § 11.175.

126. *Id.*

127. *Id.*

128. *Id.*

129. Naveen Goud, *Texas School District Experiences DDoS Cyber Attack*, CYBERSECURITY INSIDERS, https://www.cybersecurity-insiders.com/texas-school-district-experiences-ddos-cyber-attack/ (last visited Sept. 21, 2021).

130. TEX. EDUC. CODE ANN. § 11.175(b)(2).

131. *Id.* § 11.175(b) (the statute contains instructions for "[e]ach school district.").

132. *See* Doug Levin, *How Should We Address the Cybersecurity Threats Facing K-12 Schools?*, THE K-12 CYBERSECURITY RES. CTR. (Mar. 14, 2017), https://k12cybersecure.com/blog/how-should-we-address-the-cybersecurity-threats-facing-k-12-schools/. See also Rob McDonald, *5 Information Security Challenges All Universities Face*, VIRTRU, https://www.virtru.com/blog/security-challenges/ (last visited Sept. 21, 2021), for an analysis of the cybersecurity challenges faced by universities; they are similar in scope and form to those faced by K-12 Schools.

133. TEX. EDUC. CODE ANN. § 11.175(f).

134. *Id.*

135. *Id.*

3. Virginia's Statute as a Model for Key Portions of School Cybersecurity Legislation

Virginia's 2015 school cybersecurity bill is similar in substance to that of Texas but goes beyond, requiring that school districts actually implement a plan and details part of what the plan should include.[136] The statute also centralizes data security planning within the state government by having the Virginia Information Technology Agency create a model data security plan each year, upon which school districts can base their own data security plans.[137] While Virginia does not create the districts' plans for them, the state does take an active role in risk mitigation and planning.[138]

Virginia's law also required the Department of Education to "designate a chief data security officer" and fund the position, which it did.[139] The officer's job is to assist school districts with developing their security plans should they request such assistance.[140]

4. California's Research-Backed First Step

After a finding by the U.S. Department of Education that social security numbers are the most misused piece of personal student information, California passed a law in 2016 that requires superintendents to assign a student identification number to each student "with exceptional needs."[141] The California statute also removed existing language that had allowed superintendents to use social security numbers to identify students or their school records, and provided that "[a] school district shall not collect or solicit social security numbers or the last four digits of social security numbers from pupils or their parents or guardians unless otherwise required to do so by state or federal law."[142]

While it is true that social security numbers are generally the most dangerous information in the hands of cyber-criminals, it is not true that it is the only dangerous or misused information.[143] When criminals gather enough PII on a particular student, which is easy to do if, say, a list of names and

---

136. VA. CODE ANN. § 22.1-20.2 (2015).

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

141. A.B. 2097, 2016 Reg. Sess. (Cal. 2016), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB2097.

142. *Id.*

143. Social security numbers are more dangerous than other types of PII in the hands of criminals because they can be used without other PII from the same owners accompanying them. IDENTITY THEFT AND YOUR SOCIAL SECURITY NUMBER, SOC. SEC. ADMIN. 1 (June 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

addresses and family information—a list that almost every school has—is exposed, the results can be just as catastrophic for victims as they would be if the criminal had access to only social security numbers.[144] All PII is valuable and can be misused if a criminal has enough time and expertise.[145]

Nonetheless, the assignation of school-specific ID numbers for students is not a new concept and is a way for schools to avoid using a student's own PII to identify them in their educational records.[146] If data is exposed and the only data available is a name and student ID number, that information likely will not be useful to a cyber-criminal because the student ID number is not linkable to the student's valuable PII on its own.[147] However, a big caveat exists here: if the ID number can be used on its own as a key to access other academic or personal information, then it is effectively useless in terms of cybersecurity because if a criminal has the key (the student ID number), then they can access the rest of the valuable PII without even hacking into any system.[148] As is the case with most cybersecurity law, the language provided by California is but a step toward holistic cybersecurity legislation.[149]

E. Other Sectors' Approaches to Cybersecurity

Just as every state has passed some sort of school cybersecurity legislation, there are advances in other forms of cybersecurity law happening all over the country.[150] This idea of a heightened standard for reasonable cybersecurity measures extends beyond schools.[151] There are other similarly situated sectors and industries in which cybersecurity is also an important issue, and courts and lawmakers have addressed the legal duty of officials in these areas to varying degrees of effectiveness.[152]

For example, courts are trending toward recognizing a legal duty of employers to protect their employees' data.[153] The court in *Dittman v. UPMC* reasoned that because an employer required its employees to disclose their PII to it, it owed a duty to the employees to protect their data, and employees

144. Meridith Levinson, *Are You at Risk? What Cybercriminals Do with Your Personal Data*, CIO (Jan. 26, 2012), https://www.cio.com/article/2400064/are-you-at-risk--what-cybercriminals-do-with-your-personal-data.html.

145. *Id.*

146. Oswalt, *supra* note 54.

147. *Id.*

148. *Id.*

149. A.B. 2097, 2016 Reg. Sess. (Cal. 2016), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB2097.

150. *See generally Cybersecurity Legislation 2019*, NAT'L CONF. OF STATE LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx (last visited Sept. 21, 2021).

151. *Id.*

152. *Id.*

153. *See* Dittman v. UPMC, 196 A.3d 1036, 1056 (Pa. 2018).

were able to recover damages when that duty was not met.[154] While schools are not businesses and generally should not be run as such,[155] the same reasoning the court used in *Dittman* applies here.[156] Because school districts require students and families to disclose their PII to the school, schools should be required to take special measures to protect that data and provide recompense when that duty of care is not met.[157]

Police departments are also attractive targets for cyber-criminals, though often for different reasons.[158] Like schools, police departments are governmental arms that hold tons of PII on private citizens, not only those currently involved in the criminal justice system but even those who have been involved with it in the past.[159] Courts have interpreted 42 U.S.C. § 1983 to create civil liability for violations of constitutional rights.[160] Several circuits have recognized data breaches in governmental entities that hold PII of private citizens as a violation of the right to due process and have outlined roadmaps for recovering damages against the government accordingly.[161]

Institutions of higher education face similar cybersecurity concerns as do K–12 schools, though their data is arguably not as valuable because many university students already have lines of credit connected to their PII and are older in general than K–12 students.[162] Nevertheless, there has been greater scrutiny by federal departments in regulating universities' use of data than there has been for K–12 schools.[163] The laws and regulations focus mostly on frontloading cybersecurity work to prevent data breaches and do not explicitly provide remedies for university-connected people whose data is exposed or stolen but even still do more to protect data than those applied to K–12 schools.[164] Many cases arising under these laws are settled when

---

154. *See id.*

155. Valerie Strauss, *Why Schools Aren't Businesses: The Blueberry Story*, WASH. POST (July 9. 2013), https://www.washingtonpost.com/news/answer-sheet/wp/2013/07/09/why-schools-arent-businesses-the-blueberry-story/.

156. *See Dittman*, 196 A.3d at 1038.

157. Oswalt, *supra* note 54.

158. *See* CYBER INTRUSION AND DATA BREACHES (2017), NAT'L WHITE COLLAR CRIME CTR., 11, https://www.marc.org/Government/Cybersecurity/assets/cyber-intrusion-and-data-breaches.aspx (last visited Sept. 21, 2021).

159. Police departments maintain data on many groups of people, including criminals, suspects, officers, and witnesses. *Id*.; *see Protecting Law Enforcement Information*, INT'L ASS'N OF CHIEFS OF POLICE, https://www.iacpcybercenter.org/topics/it-security/ (last visited Sept. 21, 2021).

160. *See* 42 U.S.C. § 1983.

161. NAT'L WHITE COLLAR CRIME CTR., *supra* note 158; Kallstram v. City of Columbus, 136 F.3d 1055, 1069–70 (6th Cir. 1998).

162. Samantha Mello, Data Breaches in Higher Education Institutions, at 22 (Spring 2018) (Honors Theses and Capstone, University of New Hampshire, Durham), https://scholars.unh.edu/cgi/viewcontent.cgi?article=1407&context=honors; McDonald, *supra* note 132.

163. *See generally Federal Data Protection Laws*, EDUCASE, https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/hot-topics/federal-data-protection-laws (last visited Sept. 21, 2021).

164. *Id.*

pursued.[165] University data does not just include that of faculty and students but also the millions of subjects of university research.[166] People choose to pursue higher education and generally opt to participate in research too,[167] but the data they elect to share is legally more protected than the data K–12 students are required to disclose in order to pursue their compulsory educations in public schools.[168]

Finally, hotels generally collect a significant amount of information on their guests through credit cards and drivers' licenses.[169] *In re Marriott International Inc., Customer Data Security Breach Litigation*, a class action suit against a hotel chain for negligently caring for guest information, the court found that allegations by hotel guests, that the data they provided to a hotel chain was the target of a cybersecurity attack, did establish injury in fact for most victims.[170] The class members and jurisdictions involved in the case were widespread, but the court found that the victims did state a claim under laws in Florida, Georgia, New York, Maryland, and California.[171]

1. The E-Government Act of 2002 and FISMA

Finally, the E-Government Act of 2002 and the Federal Information Security Management Act of 2002 (FISMA) apply to the federal government, so they deal with a variety of data, ranging from PII of citizens to matters of national security.[172] Because public schools are not agents of the federal government, these laws do not touch public schools.[173] However, they do provide a framework for federal cybersecurity legislation that will certainly be taken into account next time cybersecurity legislation is taken up by Congress, so they are valuable to this discussion.[174]

The E-Government Act of 2002 requires federal agencies to review and assess how sensitive information, including PII, within federal agency IT systems is "collected, stored, protected, shared and managed."[175] Under this law, before an agency collects PII it must conduct a privacy impact assessment which specifies what data it will collect, the method of collection,

---

165. *See* Jessica Davis, *Washington State University Settles $4.7M Data Breach Lawsuit*, HEALTH IT SEC. (Apr. 23, 2019), https://healthitsecurity.com/news/washington-state-university-settles-4.7m-data-breach-lawsuit.

166. *Id.*

167. *See* Mello, *supra* note 162, at 17.

168. *See generally* EDUCASE, *supra* note 163.

169. *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 454 (D. Md. 2020).

170. *Id.* at 453–92.

171. *Id.* at 486–93.

172. 44 U.S.C. § 3511.

173. *See id.*

174. *See id.* § 3514.

175. *E-Government Act of 2002*, U.S. DEP'T OF JUST., https://www.justice.gov/opcl/e-government-act-2002 (last updated Feb. 13, 2019).

how it will use or share the data, how it will secure the data, and whether individuals may consent to specific uses of the data.[176]

FISMA applies "to federal agencies and to contractors and affiliates of those agencies" (an example of a contractor or affiliate of a federal agency would be an institution of higher education that receives federal grants).[177] FISMA requires federal agencies to keep inventory of all the IT systems they use and assess, categorize risk levels for each IT system, create and maintain system security plans, and review their security systems annually for compliance.[178] The data security principles underlying this statute also come into play when considering school cybersecurity.[179]

III. CONGRESS SHOULD ADOPT MODEL LEGISLATION TO PROTECT K–12 DATA

Because K–12 schools house largely unprotected data belonging to minors, and are, therefore, such attractive targets for data thieves, they are naturally vulnerable to cyberattacks.[180] Congress should legislatively impose a legal duty upon schools requiring them to protect students and their data by implementing more secure data collection and cybersecurity practices, and it should provide the necessary funding to ensure compliance with the mandate. There is currently no such federal or state statute though some states have proposed or enacted laws that include portions of what this Comment proposes.[181]

A. Proposed Model Legislation on School Cybersecurity

Most of the laws in the United States, including state laws, that deal with the ability to recover damages against schools when schools are negligent were first enacted in the 1960s, 1970s, or 1980s—or earlier, in some cases—and maintain the prioritization of the era.[182] Therefore, they were not architected with modern problems like cybersecurity in mind.[183] For example, the statute in Texas that allows individuals to sue the state

176. EDUCASE, *supra* note 163.

177. 44 U.S.C. § 3506; *see* EDUCASE, *supra* note 163.

178. 44 U.S.C. § 3506; Nate Lord, *What is FISMA Compliance? 2019 FISMA Definition, Requirements, Penalties, and More*, DIGIT. GUARDIAN (Dec. 1, 2020), https://digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more.

179. EDUCASE, *supra* note 163.

180. Herold, *supra* note 35.

181. *See, e.g.*, TEX. EDUC. CODE ANN. § 11.175; *see also* Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015).

182. *See, e.g.*, TEX. CIV. PRAC. & REM. CODE ANN. § 101.021; ALA. CONST. art. I, § 14; FLA. STAT. § 768.28(1).

183. *See* TEX. CIV. PRAC. & REM. CODE ANN. § 101.021; ALA. CONST. art. I, § 14; FLA. STAT. § 768.28(1).

government, including public schools, for negligence only provides a legal remedy if the individual's injury arises from a motor vehicle incident or if the negligent state employee would also be personally liable for the injury.[184] The statute was first enacted in 1969.[185] But the dangers of data vulnerability are now as obviously precarious as physical harm, and this realization has exposed a gap in the list of exceptions to sovereign immunity.[186] Though it makes sense to limit government liability to a certain extent, this sensibility is not extended to those situations where the government itself has put people at risk for the injuries they have sustained.[187] As the government, through the arm of public schools, requires its people to take risks by trusting it with their valuable information, it must mitigate that risk by imposing upon itself a duty to protect that information, and it must be willing to incur the costs associated with doing so.[188] If the government cannot meet this standard, it must reconsider its need for students to disclose their information to their schools in the first place.[189]

The language proposed below draws on Texas Senate Bill 820 and the Student Digital Privacy Act, combining and expanding their frameworks and policy motives to produce a comprehensive piece of legislation.[190] While Senate Bill 820 laid a foundation for Texas legislation on education cybersecurity, it did not provide specific parameters for meeting the standard it attempted to lay out, so it is difficult to ascertain when the standard has been met.[191] Other statutes that states have enacted or entertained present similar challenges and have done little to mitigate the harm students have faced when their data has been exposed by or stolen from school databases.[192]

The Student Digital Privacy Act was never enacted into law, but if it had been, it would have been a foundation-laying rule, focusing on the dealings of educational third parties with student information instead of acting as a cure for the student data security woes facing the nation's schools.[193] Parts of the language of the Student Digital Privacy Act, therefore, serve as a foundation for what needs to happen moving forward, but parts of it could prove to be harmful if it stands as is.[194] For example, it is important that the Federal Trade Commission (FTC) is notified of data breaches in schools, and

184. TEX. CIV. PRAC. & REM. CODE ANN. § 101.021.

185. *Id.*; Dick Evans et al., *Texas Torts Claims Act Basics*, TEX. MUN. LEAGUE https://www.tml.org/DocumentCenter/View/329/Texas-Tort-Claims-Act-PDFPDF (last visited Sept. 21, 2021).

186. *See, e.g.*, TEX. CIV. PRAC. & REM. CODE ANN. § 101.021.

187. *See supra* Section II.D.1 (discussing sovereign immunity).

188. *See supra* Section II.D.1 (discussing sovereign immunity).

189. *See supra* Section II.D.1 (discussing sovereign immunity).

190. TEX. EDUC. CODE ANN. § 11.175; Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015).

191. *See generally* TEX. EDUC. CODE ANN. § 11.175.

192. *See supra* Section II.D.2–4 (discussing state codified law dealing with cybersecurity in schools).

193. Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015).

194. *Id.*

it is imperative that security procedures are put into place.[195] However, publicly disclosing the types of information in a school's possession is effectively an advertisement for hackers looking to break into databases.[196] This provision would be catastrophic unless qualified so that the type of information is not disclosed to the public but instead to those whose data is involved and coupled with clear instructions for how exactly data should be protected and oversight intended to see that those protections are put into place and maintained.[197] The model language seeks to achieve this effect. Example language is italicized:

SCHOOL DISTRICT CYBERSECURITY

(a) In this section:

(1) "Covered information" means personally identifiable information, and information that is linked or linkable to personally identifiable information that[198]

(i) is collected or generated through a school service; and

(a) the operator of the school service knows or should know relates to a student; or

(b) is collected, generated, or maintained at the direction of an educational agency or institution serving the student or officials of such an agency or institution, including teachers.

(2) "Cyberattack" means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system for the purpose of accessing covered information or for any other purpose.

(3) "Cyberinfrastructure" means the systems that school districts use to house school data, including all covered information, that they maintain on students and staff.

(4) "Cybersecurity" means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access, and to protect all data, including covered information, from theft or exposure to the public.[199]

---

195. This notification is important because it ensures accountability and disclosure of the state of school cybersecurity. *Id.*

196. For an ethical discussion of disclosing cybersecurity vulnerabilities, see Jonathan Trull, *Responsible Disclosure: Cybersecurity Ethics*, CSO (Feb. 26, 2015, 5:27 AM), https://www.csoonline.com/article/2889357/responsible-disclosure-cyber-security-ethics.html.

197. *Id.*

198. This and other framing portions of this statutory language are based on language from the Student Digital Privacy and Parental Rights Act of 2015. *See* Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015).

199. This and other parts of the framing of this statutory language are based on language from the Texas Education Code § 11.175. *See* TEX. EDUC. CODE ANN. § 11.175.

> *(5) "Staff" means all adult employees of a school, including teachers, administrators, and support staff.*
> *(6) "Victim" means a student or staff member whose information has been exposed or stolen, or the family member of a student whose information has been stolen who is financially responsible for the student.*[200]

Section (a), above, provides clear definitions for important terminology. Much niche vocabulary exists in the world of internet academia, and sometimes there are several words that non-experts use interchangeably.[201] The above section serves to establish official vocabulary so that all schools and other stakeholders have mutual understanding when discussing cybersecurity issues. It also serves to clarify the language that follows in the remainder of the example statute.

(b) Each school district shall develop and maintain a cybersecurity framework for:

> *(1) the securing of district cyberinfrastructure and all covered information against cyberattacks and other cybersecurity incidents by:*
>
> > *(i) the purchase and installation of software in all district devices and networks that includes, at minimum, a threat detection and response system,*[202] *encryption*[203] *of all student and staff covered information, and firewall and VPN security;*[204] *and*

Section (b)(1), above, sets out the new cybersecurity standard in two parts. Part one explains the types of software that schools must adopt, and part two sets out standards for personnel dealing with data and for routines and practices schools should begin. This section is the primary instruction in the proposed language, and it includes an expensive but effective standard, requiring that all schools not only have some type of cybersecurity software but also specifying features the software must include to pass muster.

---

200. *Id.*
201. *See generally id.*; Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015).
202. Lord, *supra* note 60.
203. CLOUDFARE, *supra* note 61.
204. Mocan, *supra* note 62.

> *(ii) requiring two factor authentication*[205] *for staff members who log in to school networks, and instituting policies against the sharing of confidential student and staff information through unprotected channels such as text messages and personal email addresses; and*[206]

While section (b)(1)(i) sets out standards for school cyberinfrastructure, section (b)(1)(ii), above, details the standard of care that school personnel should take when dealing with PII of other personnel or students. School staff members who need to discuss or share a student's or other staff member's information must be educated on proper handling of PII, and the standard preventing casual sharing of this information must be met with consistency for other portions of the cyberinfrastructure to withstand cyberattacks.[207] Because no cyberinfrastructure system is 100% secure from hackers, this second portion is key to protect students and staff PII.[208]

> *(2) regular cybersecurity risk assessment by performing an audit of its intake of all covered information relating to students, and its storage processes and data handling practices each year, and evaluating security software performance routinely.*[209]

Section (b)(2), above, maintains a standard that many state statutes have already set out: school districts should regularly audit their cybersecurity systems for weaknesses.[210] Additionally, schools must audit not only their processes for collecting student data, but also the actual types of data they collect to ensure that they are only going to be responsible for information that they actually needed in the first place.[211] Several state school-cybersecurity statutes already include provisions for routine risk assessment and data auditing similar to this one.[212]

---

205. Griffith, *supra* note 65.

206. *See generally* Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015).

207. Ramachandran, *supra* note 53; FORBES, *supra* note 53.

208. Ramachandran, *supra* note 53; FORBES, *supra* note 53.

209. *See* TEX. EDUC. CODE ANN. § 11.175(b).

210. Some state statutes that already require regular audits of cybersecurity systems include the Virginia Code § 22.1-20.2, Colorado Revised Statutes § 22-16-104, and Louisiana H.B. 1076. *See* VA. CODE ANN. § 22.1-20.2 (2015); COLO. REV. STAT. § 22-16-104 (2019); H.B. 1076, 40th Leg., Reg. Sess. (La. 2014).

211. Editors Desk, *Why Cybersecurity Audit Should be a Priority for You*, CYBERSECURITY MAG. (Nov. 22, 2020), https://cybersecurity-magazine.com/why-cyber-security-audit-should-be-a-priority-for-you/.

212. *See* VA. CODE ANN. § 22.1-20.2 (2015); COLO. REV. STAT. § 22-16-104 (2019); H.B. 1076, 40th Leg., Reg. Sess. (La. 2014).

(c) Each school district will be responsible for holding a cybersecurity professional development session at least once each year to educate school employees on the importance of cybersecurity and best practices for preventing cybersecurity breaches.

Section (c), above, is important because cybersecurity only works if every person who operates within a district's cyberinfrastructure is on guard against cyberattacks and does their part to keep confidential information truly confidential.[213] School employees will only be willing and able to do so if they understand the purpose behind cybersecurity and how cyber-criminals are able to steal information.[214]

(d) The superintendent of each school district shall designate a cybersecurity coordinator from among the superintendent's staff to serve as a liaison between the district and the Department of Education's Student Privacy Policy Office in cybersecurity matters.[215]

(e) Each district's cybersecurity coordinator shall report to the Department of Education any cyberattack, attempted cyberattack, or other cybersecurity incident against the district cyberinfrastructure as soon as practicable after the discovery of the attack or incident.[216]

Section (d), above, requires each school district to establish a liaison between the district and the U.S. Department of Education, and section (e), above, establishes a line of communication between the two. This provision ensures a layer of oversight and accountability for schools facing cybersecurity threats, but more importantly, the Department of Education can also provide assistance in mitigating any potential harm done.

(f) The Department of Education shall form a mitigation plan that includes setting up a fund out of which to pay damages or partial damages to student and staff victims of school security breaches when their covered information has been exposed or misused or when this statute has otherwise been shown to have been violated by the school district from which the individual's data was stolen.[217]

> *(1) Damages shall be paid according to the extent of the injury suffered by each victim. The extent of the injury will be assessed according to the following factors:*

---

213. Ramachandran, *supra* note 53; FORBES, *supra* note 53.

214. Ramachandran, *supra* note 53; FORBES, *supra* note 53.

215. *See* TEX. EDUC. CODE ANN. § 11.175(d).

216. *See id.* § 11.175(e).

217. *See* Student Digital Privacy and Parental Rights Act, H.R. 2092, 114th Cong. (2015); TEX. EDUC. CODE ANN. § 11.175(b).

> *(i) The time between the security breach and when the victim or victims were informed.*
> *(ii) Whether the victim's covered information was stolen or just exposed.*
> *(iii) The age of the victim.*
> *(iv) The amount of covered information stolen or exposed.*
> *(v) What was done with the stolen information.*
> *(vi) The costs incurred by the victim associated with credit repair or identity recovery, or any other costs associated with repairing the injury.*[218]

Section (f), above, establishes a financial mitigation plan out of which victims can be compensated for their injuries.[219] The Department of Education's budget is largely directed toward supporting schools and providing assistance to schools as they implement various types of new programming, so it would make sense for this department's funding to also include provisions for damages when necessary.[220] This section, however, provides that the Department will be responsible for damages or partial damages and is within the realm of reasonability for individual districts to pay part of the damages and the Department of Education to pay the other part.[221] The primary purpose of this provision is to ensure that families of students or staff members whose data is compromised are compensated.[222] This provision is extremely important, as funding for damages is one of the most obviously lacking elements in the global mitigation efforts.[223] While the funding could come from anywhere, the Department of Education seems like a logical choice.[224]

(g) As new cybersecurity and cyberattack technology becomes available, section (b) of this statute will be amended accordingly. The purpose of this statute is to ensure that schools are employing the most effective cybersecurity technology currently available.[225]

---

218. *See supra* Section II.E (discussing how schools should be required to take special measures to protect student data and should compensate victims when that duty is not met).

219. *See* TEX. EDUC. CODE ANN. § 11.175(b)(2); *supra* Section II.E (discussing school liability for injuries from cybersecurity).

220. *Budget Factsheet*, U.S. DEPT. OF EDUC. https://www2.ed.gov/about/overview/budget/budget16/budget-factsheet.pdf (last visited Sept. 21, 2021).

221. *See supra* Section II.E (discussing school liability for injuries from cybersecurity).

222. *See supra* Section II.E (discussing how other sectors compensate their victims).

223. *See* sources cited *supra* note 49 (explaining that hackers vanish making it almost impossible to receive civil damages).

224. *See* U.S. DEP'T OF EDUC., *supra* note 70.

225. *See How to Keep up with Constantly Changing Cybersecurity Threats*, MARYVILLE UNIV. https://online.maryville.edu/blog/how-to-keep-up-with-constantly-changing-cybersecurity-threats/ (last visited Sept. 21, 2021).

Finally, because cybersecurity is rooted in computer and internet technology, it is always changing and evolving.[226] Section (g), above, provides a clause that ensures that as these evolutions and changes happen, school cybersecurity also evolves. The most dangerous cyber-criminals use the most up-to-date tools available to them, so it is important that schools do the same.[227] This provision is one of the most important elements of the example language because it goes beyond addressing cybersecurity challenges that schools currently face and is flexible enough to address future unknown cybersecurity challenges.[228]

While the focus of this Comment is the effect of school data breaches on students, the language provided above also includes protections for staff members whose data has been compromised. The harm done to minors when their data is stolen is arguably greater and more difficult to detect than that done to adults in the same types of situations, but harm is still harm and can be costly regardless of age.[229] Adults might be able to recover smaller amounts under the statute (according to the extent of their damages), but it would be an oversight to leave them out completely, especially considering the cost of their remedies could be less than that of students and, therefore, more affordable.[230]

B. The Challenges of Implementing the Proposed Model Legislation

The two main challenges to overcome in enacting education legislation are the maintenance of local school autonomy and the funding of new endeavors.[231] However, while these may seem like obstacles on the surface, in reality they pose little threat to passing legislation patterned on that above.

1. School District Autonomy

Like it is important for teachers to make decisions pertaining to the goings on of their classrooms, it is also important for school boards and superintendents to make decisions for their local school districts.[232] School

---

226. *Id.*; Ben DiPietro, *Speed of Tech Change a Threat to Cybersecurity*, WALL ST. J. (Apr. 20, 2018), https://www.wsj.com/articles/speed-of-tech-change-a-threat-to-cybersecurity-1524249888.

227. *Top Ten Tools for Cybersecurity Pros*, CYBERSECURITY EDUC. GUIDES, https://www.cybersecurityeducationguides.org/2017/11/top-ten-tools-for-cybersecurity-pros-and-black-hat-hackers/ (last visited Sept. 21, 2021).

228. *See* MARYVILLE UNIV., *supra* note 225; DiPietro, *supra* note 226.

228. *See* DiPietro, *supra* note 226.

229. Shalina Chatlani, *Cost of Education Data Breaches Averages $245 Per Record*, K-12 DIVE (July 18, 2017), https://www.k12dive.com/news/cost-of-education-data-breaches-averages-245-per-record/447376/.

230. *See id.*

231. *See supra* Section II.B.1–2 (discussing the implications of school autonomy and funding).

232. *School Autonomy*, CTR. ON REINVENTING PUB. EDUC., https://www.crpe.org/sites/default/files/

districts can—and should—control their own budgeting and personnel decisions, write and amend codes of conduct, and enact school-specific governing rules as these elements must be formatted to meet the needs of each unique school district and community.[233] However, the elements that school leaders must consider and make choices about must also operate within the realm of state and federal law.[234] For example, most states impose standardized testing that school districts cannot choose to forego without facing significant financial repercussions that cripple school operations.[235] Most states also have laws mandating an exact number of minutes that students must spend receiving classroom instruction each day.[236] Moreover, these standards are generally aligned to and derived from federal guidelines upon which the individual school district's receipt of federal funds is contingent.[237]

In a similar vein, while the daily operations and demographics of each school district are unique, the cybersecurity needs of each school district are not unique, so the example language this Comment proposes will not affect districts differently.[238] The biggest variant among districts that affect their cybersecurity systems is size.[239] But, size does not change whether a school district needs the precautions and standards outlined above—only the extent and the cost of their installation and maintenance matters.[240] Additionally, cybersecurity is not a local concern.[241] Cyber-criminals can attack any school's cyberinfrastructure from anywhere and all schools must address this threat.[242] Therefore, uniformity in cybersecurity requirements is not only logical, but is the least burdensome solution for schools and students.[243]

Portfolio_components_2.pdf (last visited Sept. 21, 2021); Stephen Goldsmith, *The Autonomy a School Needs for Success*, GOVERNING (Sept. 19, 2017), https://www.governing.com/archive/bfc/col-autonomy-school-success-indianapolis.html.

233. *See* CTR. ON REINVENTING PUB. EDUC., *supra* note 232; Goldsmith, *supra* note 232.

234. *See supra* Sections II.B.1, II.B.2 (explaining federal regulations on cybersecurity).

235. *See* Catherine Gerwertz, *What Tests Does Each State Require?*, EDUC. WEEK, https://www.edweek.org/teaching-learning/what-tests-does-each-state-require (last visited Sept. 21, 2021).

236. *Instructional Time Requirements*, CAL. DEPT. OF EDUC., https://www.cde.ca.gov/fg/aa/pa/instructionaltimetable.asp (last visited Sept. 21, 2021).

237. *See 50 State Comparison: K-12 Funding*, EDUC. COMM'N OF THE STATES, https://www.ecs.org/50-state-comparison-k-12-funding/ (last visited Sept. 21, 2021).

238. *See Why Cybersecurity Needs to Be a Priority for the Education Sector*, SWIVEL SECURE, https://swivelsecure.com/solutions/education/why-cybersecurity-needs-to-be-a-priority-for-the-education-sector/ (last visited Sept. 21, 2021); Cisco, *Securing Schools: The 5 Key Components of a Comprehensive Approach to Cybersecurity in Education*, GOV'T TECH. (Apr. 27, 2020), https://www.govtech.com/education/news/Securing-Schools-The-5-Key-Components-of-a-Comprehensive-Approach-to-Cybersecurity-in-Education.html.

239. *See* SWIVEL SECURE, *supra* note 238; GOV'T TECH., *supra* note 238.

240. *See* SWIVEL SECURE, *supra* note 238; GOV'T TECH., *supra* note 238.

241. *See generally* Michael Figueroa, *Cyber Security Is a National Concern*, COMMPRO, https://www.commpro.biz/cyber-security-is-a-national-concern/ (last visited Sept. 21, 2021).

242. *See id.*

243. *See id.*

While some might argue that the federal government's reach into (what are presumed to be) otherwise autonomous school communities is a huge government overstep, the reality is that if there is an overstep, it has already happened.[244] Since the early 1900s, school attendance has become compulsory in every state, the government (federal and state) has imposed mandatory academic standards on schools, and teacher qualifications are generally uniform across the country.[245] There are laws governing the types of food that school cafeterias can serve and the types of schedules schools must follow.[246] In 2020, the government has not only required that students attend school but has dictated almost exactly the manner in which schools must operate.[247] In order to meet many of these requirements, schools are constantly collecting data on their students—often informally and unknowingly.[248] They know attendance rates, academic performance levels, contact and other directory information, and details about students' families. This data collection allows schools to meet the standards set out by the government in order to have funding.[249]

So, like *Dittman*, which required employers to protect mandated employee information, now that the government has set up schools in a way that require families to share information, the government must act to protect that information and—by extension—the people it serves.[250] There is little big-picture individual school decision-making power left, and because the government has mandated that schools operate in such a way, it must require students and families to trust them with their personal information.[251] The only ethical way forward is ensuring that the information is—at least—as safe with the school as it would be had the school never entered it into its databases.[252]

---

244. *See* Bogel-Burroughs, *supra* note 1.

245. *See* NAT'L CTR. FOR EDUC. STAT., *supra* note 111; Gerwertz, *supra* note 235; *Educational Programs Licensure Requirements by State* (June 2019), https://www.sru.edu/documents/academics/online-learning/Education%20State%20by%20State%20Requirements%20reviewed%20COE%20-%202019.pdf.

246. *See generally Federal Legislation & Regulations*, SCH. NUTRITION ASS'N, https://schoolnutrition.org/legislationpolicy/federallegislationregulations/ (last visited Sept. 21, 2021); CAL. DEP'T OF EDUC., *supra* note 236.

247. *See, e.g.*, Kaia Hubbard, *Those States Have COVID-19 Mask Mandates*, U.S. NEWS (Sept. 13, 2021, 10:29 AM), https://www.usnews.com/news/best-states/articles/these-are-the-states-with-mask-man (listing multiple states that imposed mask mandates in schools).

248. *See* Nicole Dobo, *Schools Collect More Data, But How is it Used?*, HECHINGER REP. (July 19, 2017), https://hechingerreport.org/schools-collect-data-used/.

249. *See id.*

250. *See* Dittman v. UPMC, 196 A.3d 1036, 1056 (2018).

251. *See supra* Section II.C (examining federal codified law affecting data security and efforts to secure data).

252. *See supra* Section III.A (proposing model legislation on school cybersecurity).

2. Reframing the Expense of Cybersecurity

Though cybersecurity programs are very costly, identity theft and rectifying wrongs done by cyber-criminals are even more expensive.[253] Moreover, when there is no law in place that provides effective protection for those whose data is stolen, the ones who end up paying for it are the students and families who had no power over the data breach incident in the first place.[254] Because most families have no choice but to share their data with their schools, they should not be penalized with credit repair and identity recovery fees when that data is used in ways that harm them.

A common political theme in the United States and almost every individual state today is the issue of school funding.[255] Most schools lack the resources they need, so, it can seem counterintuitive to direct the limited funds that are available toward a problem that many people are unaware of and that several people have not personally encountered.[256] However, if the categorization of cybersecurity expenses is shifted from simply adding them to technology budgets as an afterthought and when space is available for them, to thinking of them as any other form of security, the precautions seem less frivolous.[257] With the rise of school shootings and other violence in schools, it is easy for any taxpayer to conceptualize the need for security guards, automatically-locking doors, security cameras, metal detectors, and identity badges for staff and students; so, it is not difficult to convey to them the importance of spending precious dollars on these types of physical security efforts.[258] Accordingly, legislatures already recognize the importance of physical safety and have directed funds appropriately.[259] They should do the same with cyber safety, and this transition will be easier when there is sufficient education about the danger of ineffective cybersecurity and the harms it imposes on the most vulnerable Americans.[260] Unfortunately, without statutory language similar to what this Comment proposes, people will be educated in cyber-dangers the hard way: by having their data exposed or stolen and working to repair the damage on their own.[261]

---

253. Chatlani, *supra* note 229.

254. *See id.*; Dobo, *supra* note 248.

255. *2020 Presidential Candidates on Education*, BALLOTPEDIA, https://ballotpedia.org/2020_presidential_candidates_on_education (last visited Sept. 21, 2021).

256. *See supra* notes 52–55 and accompanying text (discussing the lack of funding in schools).

257. *See* John Woodrow Cox & Steven Rich, *Armored School Doors, Bullet Proof Whiteboards and Secret Snipers*, WASH. POST (Nov. 13, 2018), https://www.washingtonpost.com/graphics/2018/local/school-shootings-and-campus-safety-industry/.

258. *See id.*

259. *Id.*

260. *See* Zamora, *supra* note 31.

261. K-12 CYBERSECURITY RES. CTR., *supra* note 7.

In the same vein, the cybersecurity measures should be paid for from each independent district's security budget, not from its technology budget, which is often the case.[262] This shift in budget labeling might seem like a minor change in phrasing that affects nothing but appearances, but its value is in what it does to how leaders think about cybersecurity.[263] It is not a luxury to be added on top of the credentials of already thriving schools but a baseline necessity for protecting the vulnerable from great harm.[264]

C. Practical Considerations for Implementing School Cybersecurity Law

While cybersecurity software and systems are the foundation of an effective cybersecurity practice, arguably the second most important element is education.[265] School staff must be made aware of the dangers of poor cybersecurity, and only then will they be on board.[266] The effectiveness of the systems depends on the use of the systems, so teachers, other school staff, and families must understand the importance of working within the cybersecurity systems of their schools.[267]

For example, if a school uses Microsoft as its main operating system, and the main operating system of the school is protected by advanced software, but a certain teacher prefers Google Classroom for daily classroom operations, and regularly asks students to submit their opinions, facts about themselves, essays, parent information, or anything else via Gmail or other Google services, then the teacher might be operating outside of the protected cyberinfrastructure of their school and might be putting student data at risk. However, because the teacher's Google account is password protected and students submit information using a classroom nickname, the teacher thinks the operating procedures are safe. This is the kind of operation that might poke a hole in an otherwise airtight cyberinfrastructure, and it is the type of problem that can only be solved by an awareness campaign undertaken by every school district in the country.[268] When everyone is aware of the dangers of ineffective cybersecurity, everyone will work together to support the systems that keep student information safe.[269]

---

262. *See* Zamora, *supra* note 31.
263. *See id.*; Cox & Rich, *supra* note 257.
264. *See* Zamora, *supra* note 31, at 12.
265. *See* Ramachandran, *supra* note 53; FORBES, *supra* note 53.
266. *See* Ramachandran, *supra* note 53.
267. *See id.*; FORBES, *supra* note 53.
268. *See supra* notes 52–53 and accompanying text (discussing how awareness is key to cybersecurity and how teachers with a lack of training can be susceptible to common cybersecurity pitfalls).
269. *See* Zamora, *supra* note 31.

IV. CONCLUSION

Student data collected and held by public schools in the United States is at risk of exposure and theft.[270] Because minors are attractive targets for data thieves and because schools have small cybersecurity budgets and limited cybersecurity expertise, this student data is particularly vulnerable.[271] To make matters worse, neither the federal government nor state governments have passed legislation that adequately addresses this crisis.[272]

This Comment provides example language for a new federal statute intended to provide the support that schools need to protect the student data they care for.[273] With language like that above, schools will be able to do their job of educating America's students without the concern that important student data might be exposed at any moment. It also removes the financial burden from the shoulders of students and families whose data has been compromised and places it on the government—where it belongs.

---

270. K-12 CYBERSECURITY RES. CTR., *supra* note 7.

271. *See supra* Section II.A (discussing the risk students and families take by attending public schools and sharing data with them).

272. *See supra* Section II.B (discussing current state and federal cybersecurity legislation).

273. *See supra* Section III (modeling potential legislative language).