Berkeley Technology Law Journal

Volume 31
Issue 2 *Annual Review 2016*

Article 23

9-25-2016

Edtech and Student Privacy: California Law as a Model

Dylan Peterson

Follow this and additional works at: https://scholarship.law.berkeley.edu/btlj

Recommended Citation
Dylan Peterson, *Edtech and Student Privacy: California Law as a Model*, 31 Berkeley Tech. L.J. 961 (2016).

Link to publisher version (DOI)
https://doi.org/10.15779/Z381G4B

This Article is brought to you for free and open access by the Law Journals and Related Materials at Berkeley Law Scholarship Repository. It has been accepted for inclusion in Berkeley Technology Law Journal by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.

EDTECH AND STUDENT PRIVACY: CALIFORNIA LAW AS A MODEL

Dylan Peterson†

The educational technology ("edtech") industry has grown rapidly over the last decade. Trade groups estimate that the industry centered on software for kindergarten through twelfth grade students has generated $7.9 billion in revenue in a single year.[1] In 2014, edtech startups saw a record of nearly $1.9 billion in venture capital (VC) investment.[2] The boom continued in 2015, as VC funding to edtech startups grew 68% when compared to the previous year.[3] These numbers are staggering, particularly in light of the $400 million in financing edtech companies received in 2009.[4]

Edtech represents a broad category of educational products and services used in schools and by private individuals. The emerging edtech industry includes devices such as tablets and other computers, the applications and software that run on these devices, websites and other Internet-based services (including cloud computing technology and social media), and various other technologies that seek to improve learning and education administration in the home, classroom, school, and school districts. Participants in the edtech industry include both well-established companies like Apple, Microsoft, and Google and smaller, more specialized companies like Schoology and Edmodo. In addition, edtech continues to attract robust startup activity. The industry's growth is poised to continue as K–12

DOI: http://dx.doi.org/10.15779/Z38T840
© 2016 Dylan Peterson.

† J.D. Candidate, 2017, University of California, Berkeley, School of Law.

1. Natasha Singer, *Microsoft and Other Firms Pledge to Protect Student Data*, N.Y. TIMES (Oct. 7, 2014), http://www.nytimes.com/2014/10/07/business/microsoft-and-other-firms-pledge-to-protect-student-data.html [https://perma.cc/C49D-ADAJ] [hereinafter *Firms Pledge to Protect Student Data*].

2. *See* Mark Koba, *Education Technology Funding Soars—But Is It Working in the Classroom?*, FORTUNE (Apr. 28, 2015), http://fortune.com/2015/04/28/education-tech-funding-soars-but-is-it-working-in-the-classroom [https://perma.cc/6K37-V5V4].

3. From quarter three of 2014 through quarter two of 2015. *Funding to VC-Backed Education Technology Startups Grows 503% Over 5 Years*, CB INSIGHTS (July 17, 2015), https://www.cbinsights.com/blog/ed-tech-funding-on-pace-record-year [https://perma.cc/F6A8-58JX].

4. *See* Koba, *supra* note 2.

educators embrace technology and indicate their willingness to integrate a greater level of digital technology in the classroom.[5]

Internet or digital technology has taken a long time to catch on in the education industry.[6] Educators and edtech advocates hope that new technology will provide wide-ranging benefits to students, teachers, and administrators. Although many edtech ideas have proven to be ineffective and have not been profitable, many in the education industry are optimistic that technological innovation will transform student learning in the near future.[7] Edtech, by collecting and storing data on student performance, can help teachers better understand student learning and the effectiveness of different teaching approaches.[8] It may also help teachers customize their teaching to better serve individual students, and improve classroom and school administration.[9]

Growing student use of digital technology has led to increased concerns about access to, and the use of, student data created and gathered by educational websites, applications, and other online services. A series of high profile data breaches in the retail and employment sector has only added to the public push for stricter and more comprehensive student privacy laws.[10] Further, current federal student privacy laws are widely seen as inadequate and outdated. The applicable laws suffer from inadequate enforcement and confusion due to their overlapping and unclear coverage.

The central tension in edtech is between the need to protect student data privacy on the one hand, and edtech companies' ability to innovate on the other, as well as schools' ability to improve efficiency and enhance education. Edtech companies need access to student data to evaluate and

5. Vision K-20, *2015 Results from the Vision K-20 Survey: Executive Summary*, THE SOFTWARE & INFO. INDUSTRY ASS'N 1, 5 (2015), http://www.siia.net/Portals/0/pdf/Education/Visionk20/SIIA%20Vision%20K-20%20Survey%20Executive%20Summary%20V1.pdf [https://perma.cc/BP32-FN3U].

6. *See Firms Pledge to Protect Student Data*, *supra* note 1.

7. *See* Natasha Singer, *Silicon Valley Turns Its Eye to Education,* N.Y. TIMES (Jan. 11, 2015), http://www.nytimes.com/2015/01/12/technology/silicon-valley-turns-its-eye-to-education.html [https://perma.cc/R5NL-XG2Z] [hereinafter *Silicon Valley*].

8. *See* Susan Dynarski, *When Guarding Student Data Endangers Valuable Research,* N.Y TIMES (June 13, 2015), http://www.nytimes.com/2015/06/14/upshot/when-guarding-student-data-endangers-valuable-research.html [https://perma.cc/D2Y2-73U3]. As a side note, it is important to recognize that many edtech companies do not collect student data at all and should not be grouped with many of the companies that do collect, store, and use student data.

9. *See* Jules Polonetsky & Omar Tene, *Who is Reading Whom Now: Privacy in Education from Books to MOOCs*, 17 VAND. J. ENT. & TECH. L. 927, 931, 940 (2015).

10. *See* Keith R. Krueger & Bob Moore, *New Technology "Clouds" Student Data Privacy*, KAPPAN MAGAZINE 19, 19 (Feb. 2015).

improve education programs.[11] And while the general public appears unified behind the effort for greater student privacy protections at both the state and federal level, some involved in education technology are worried that the passage of stricter privacy laws without careful evaluation could greatly reduce the benefits of technology in the classroom.[12] Many policymakers and parents believe that companies that handle children's data must act with extra care in order to ensure their privacy.[13] This view favors more expansive regulation of student privacy and the modernization of student privacy law.[14]

This Note will both evaluate current federal student privacy law and analyze the effectiveness of the California legislature's efforts to enhance student privacy protections. Specifically, Part I of this Note will discuss the scope of the edtech industry and address the nature of student privacy. Part II will evaluate current federal student privacy law and introduce the California legislature's efforts to enhance student privacy protections. Part III will discuss the adequacies and shortcomings of California's Student Online Personal Information Protection Act (SOPIPA), examine the law's effect on the incentives of edtech companies subject to its regulation, and assess whether it appropriately addresses the concerns of parents and educators. Furthermore, Parts III and IV will evaluate whether SOPIPA succeeds in striking an appropriate balance between innovation and the consensus policy goal of strong student data privacy protection, and whether SOPIPA is an adequate solution to the inadequate scheme of federal student privacy law. This Note concludes that while SOPIPA effectively responds to many of the gaps in federal law and successfully updates an outdated body of law, it largely functions as a Band-Aid measure, and federal reform is needed. Additionally, while SOPIPA is a definite improvement on existing student privacy laws, it has some substantive shortcomings, and creates some new problems for the edtech industry.

---

11. *See* Dynarski, *supra* note 8.

12. *See, e.g.*, *id.*

13. *See* Mike Orcutt, *Educational Technology Faces a Pivotal Privacy Moment*, MIT TECH. REV. (July 27, 2015), http://www.technologyreview.com/news/539101/educational-technology-faces-a-pivotal-privacy-moment [https://perma.cc/ED3Q-UNJQ]; *see, e.g.*, Dynarski, *supra* note 8; *see* Polonetsky & Tene, *supra* note 9, at 949–54.

14. It is interesting, however, that in many contexts the government does very little to protect children's privacy. This is perhaps most apparent in the context of the children's retail market. Many companies in this market target children through club or loyalty program memberships. There is little regulation in this area, which can allow companies to collect information such as a child's home address and birthday in order to better market their products to children. *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (forthcoming 2016).

I. BACKGROUND: AN OVERVIEW OF EDTECH

While edtech is a very important industry, it remains difficult both to define the edtech market and determine whether edtech products offer any benefits to teachers, students, and schools. This Part will first discuss the current scope of the edtech market, including its growth and the types of extant edtech companies and their monetization strategies, as well as criticisms about technology use and effectiveness in the classroom. It will then discuss privacy issues generally and provide a synopsis of the issues specifically raised by student privacy.

A. WHAT IS EDUCATION TECHNOLOGY?

Education technology can be difficult to define because of its breadth. And a discussion of technology often exclusively contemplates modern technology. However, education has long incorporated technology. For example, a blackboard, an overhead projector, a television, and a book are all pieces of education technology. The transition from manual and physical print technology to today's digital and Internet-based technology is the primary source of the present privacy problem.[15] Before the late twentieth century, student data was almost exclusively stored in paper form.[16] Not long ago, computers were considered a luxury in schools. But now digital devices are largely considered a necessity (or are quickly becoming one) to provide students with a quality education. The influx of digital technology (devices, websites, software, and apps that utilize the Internet and cloud-based technology) into the education system presents the law with new student privacy challenges. New technology has increased the ease of collecting and storing data on individual students, raising new concerns about the security of this personal information once it has been collected.[17] The current scope and rapidly evolving nature of edtech makes it a particularly difficult area for privacy law to address.

1. Types of Edtech Companies and Monetization Strategies

Different types of edtech companies use different business models and monetize their products in unique ways.[18] Many edtech startups offer their

15. *See generally* Sonja Trainor, *Student Data Privacy is Cloudy Today, Clearer Tomorrow*, KAPPAN MAG., Feb. 2015, at 13.

16. *Id.* at 14.

17. Joanna Tudor, *Legal Implications of Using Digital Technology in Public Schools: Effects on Privacy*, 44 J. L. & EDUC. 287, 288 (2015).

18. Edtech companies can generally be placed into one of three categories. First, there are companies like Apple, Microsoft, and Google. These are technology companies that do not exclusively have an education focus, but many of their products and services are

products to schools on a free or freemium[19] basis in order to bypass schools' limited budgets and slow, bureaucratic technology adoption process.[20] However, the lack of a clear and certain monetization route may be holding down VC investment in the industry.[21] There is debate over whether startups that do not have a clear strategy to monetize their user-base will be sustainable.[22] Investors are generally more confident in edtech companies that charge their customers consistent fees.[23] Many software companies charge for their service directly either for a one-time fee or on a subscription basis.[24] Other companies, particularly platform companies like Apple, Google, and Microsoft, offer products at a low cost or offer ad-free versions

widely used in schools. These are platform-based companies that want consumers to adopt their entire ecosystem of products and services. *See* Matt Buchanan, *Apple vs. Google: Did Apple Learn Anything From its War With Microsoft,* WIRED (Nov. 1, 2013), http://www.wired.com/2013/11/is-the-mobile-dogfight-between-apple-and-google-just-like-the-one-with-microsoft [https://perma.cc/AQC3-M3N9]. For example, Google's platform encompasses its Chromebook computers, Apps for Education, e-mail platform (g-mail), search engine, and many other products and services. *See Google for Education*, GOOGLE, https://www.google.com/edu [https://perma.cc/4FZR-PMFU]. These platforms hope to benefit from network effects: their assumption is that wider distribution will exponentially attract more customers and encourage current customers to stay with the company. *See* Buchanan, *supra* note 18. Second, there are well-established education-centric companies. This category includes companies like Houghton Mifflin Harcourt, Walsworth, and Pearson, which are traditional education companies. These types of companies provide services such as education publishing and school assessment, but are also generally expanding into digital content and services. This category also includes companies like Edmodo, Canvas, and Blackboard. These companies exclusively provide digital education services, platforms, and content. Third, there are edtech companies that can be classified as startups. These companies have limited distribution, funding, and may be made up of just a single entrepreneur or partners. For the most part, these companies have not signed the Student Privacy Pledge that will be discussed later in the Note.

19. Investopedia defines "freemium" as:

> a combination of the words 'free' and 'premium' used to describe a business model that offers both free and premium services. The freemium business model works by offering simple and basic services for free for the user to try and more advanced or additional features at a premium. This is a common practice with many software companies, who offer basic software free to try but with limited capabilities.

Freemium Definition, INVESTOPEDIA, http://www.investopedia.com/terms/f/freemium.asp [https://perma.cc/4Y3X-TBXT].

20. *Silicon Valley*, *supra* note 7.
21. *See id.*
22. *See id.*
23. *See id.*
24. *See id.*

of their services to students[25] in order to attract a user base that will later yield a powerful network of users.

For the purposes of this Note, the division between edtech startups and more established edtech companies (both platform-based companies and education centric companies) will play a significant role in the evaluation of SOPIPA, particularly due to their differing resources and revenue streams.

2. Benefits and Criticisms of Edtech

While edtech has grown tremendously over the last few years, some leaders in the education industry question whether the benefits of new technology are truly being realized and whether access to technology is broad across schools with varying economic resources and can be sustained over the long-term.[26] Access to technology is still limited in lower income neighborhoods, and many edtech services are not cheap.[27] Furthermore, in order to keep up with rapidly evolving technology in the face of ever-dwindling budgets, many school districts have chosen to issue bonds in order to bridge the funding gap.[28] Schools not only find that devices quickly become obsolete as technology evolves,[29] but also must build funding into their budgets for the applications and other services that run on these devices.[30]

Aside from problems with the cost of and access to educational technology, many teachers are concerned that digital technology supplants their ability to teach and reach students.[31] Some teachers see the integration of digital devices into classroom teaching as a distraction that has far less educational value than edtech companies credit it with.[32] A recent study found that, although students that use computers "moderately" at school generally perform better than those that use them infrequently, the performance of students that use computers very frequently suffers.[33] This may mean that teachers need to be more involved in the design and

25. *See* Tudor, *supra* note 17, at 321.
26. *See* Koba, *supra* note 2.
27. *See id.*
28. *Id.*
29. *See id.*
30. *See id.*
31. *See id.*
32. *See id.*
33. *New Approach Needed to Deliver on Technology's Potential in Schools*, ORGANISATION FOR ECON. CO-OPERATION & DEV. (Sept. 15, 2015), http://www.oecd.org/education/new-approach-needed-to-deliver-on-technologys-potential-in-schools.htm [https://perma.cc/86GP-2H85].

implementation of edtech products.[34] But it is at least clear that educators and edtech companies still have a lot to figure out in order to unlock the true potential of digital technology integration in the classroom. However, and notwithstanding these criticisms, researchers expect school expenditures on new technology to continue to grow for the foreseeable future.[35]

Proponents of technology in the classroom maintain that students and teachers can benefit from it in many ways. For example, the use of data-collecting digital technology can provide students with a more personalized education than would otherwise be available to them.[36] A piece of software may be able to recognize certain reoccurring problems that a student struggles with, or determine a student's optimal learning style in a way that a teacher may be unable to uncover.[37] More generally, collection of large amounts of data "promises big advantages" to education including "the ability to track and document the needs, progress, and success of individuals and groups."[38] The technology itself may also increase opportunities for collaboration among students and can lead to greater engagement in learning.[39]

B. DEVELOPMENT OF PRIVACY LAW & STUDENT PRIVACY

High profile privacy threats have recently taken center stage in the national discourse, leading to increased public concern about the potential privacy implications of the collection of personal information and data by companies, organizations, and government agencies.[40] Further, Edward Snowden's disclosures relating to the National Security Agency's collection of the personal phone records of millions of Americans has increased the push for stronger privacy protections.[41]

Information privacy, or data protection, law is a relatively new area of law that is largely still taking shape.[42] Much of the development in this area has occurred since the year 2000 as new technologies have forced lawmakers to reevaluate privacy protections and determine the nature of public

34. *See id.*
35. Koba, *supra* note 2.
36. *See* Polonetsky & Tene, *supra* note 9, at 939.
37. *See* Orcutt, *supra* note 13.
38. Trainor, *supra* note 15, at 13.
39. *See* Polonetsky & Tene, *supra* note 9, at 931.
40. *See* Dynarski, *supra* note 8.
41. *See id.*
42. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 39 (3d ed. 2015).

expectations of privacy in the digital technology space.[43] For example, the first data breach notification statute was not passed in the United States until 2003.[44]

As noted by Daniel Solove and Paul Schwartz, "privacy problems occur in particular contexts, and different types of problems involve different trade-offs and concerns."[45] In other words, the best solution to the student data problem may differ greatly from the solution to various other privacy problems that arise in other contexts (such as adult data privacy or even child privacy in Internet use outside of the education context). This Section will discuss the current state of student privacy law and the central issues facing policy makers.

1. Current Issues Surrounding Student Privacy

Like privacy generally, student privacy remains a developing and constantly changing area of the law. But student privacy is not a new concern. Federal statutes have regulated student privacy in some form for over forty years. The Family Educational Rights and Privacy Act of 1974 (FERPA), the first federal statute to regulate student privacy, was described as being "on the frontier of federal privacy regulation" at the time of its enactment.[46] However, FERPA's effectiveness has come into question as the edtech market has exploded in the last few years.[47] While in the past, student privacy was largely regulated by federal statutes, legislative activity in this area has shifted to the states. Twenty-eight states enacted student privacy laws in 2014.[48] In comparison, state legislatures only enacted a single student privacy bill in 2013.[49] Since 2013, nearly all states have passed or considered bills to enhance student data privacy protections.[50] Many of

43. *See id.*
44. *Id.*
45. *Id.*
46. Daniel Solove & Paul Schwartz, *The Battle for Leadership in Education Privacy Law: Will California Seize the Throne?*, SAFEGOV (Mar. 27, 2014), http://edu.safegov.org/the-battle-for-leadership-in-education-privacy-law-will-california-seize-the-throne [https://perma.cc/9YJ6-SGLF].
47. *See id.*
48. *See* Trainor, *supra* note 15, at 17.
49. John Watson et al., KEEPING PACE WITH K–12 DIGITAL LEARNING: AN ANNUAL REVIEW OF POLICY AND PRACTICE 66 (11th ed. 2014).
50. *See* Amelia Vance, *Policy Update*, NAT'L ASS'N ST. BOARDS EDUC. (2015), http://www.nasbe.org/wp-content/uploads/NASBE-Policy-Update-2015-Legislative-Session-Data-Privacy_-June-2015.pdf [https://perma.cc/4C2B-GJ23].

these laws seek to ensure that student data is not sold to third parties or otherwise used for commercial purposes.[51]

Educators and edtech companies have expressed concern that some of the more restrictive laws will pose problems for effective digital learning and innovation.[52] Rob Curtin, a long-time employee at Microsoft and current chief privacy officer at an edtech startup, has warned that comprehensive restrictions on the collection and sharing of student data could "stifle innovation" and limit the educational benefits of edtech data.[53] Curtin claims that historical data profiles of an individual student's performance on assessments can be used to personalize lesson plans and instruction.[54] But many advocates and politicians are in favor of strengthening student privacy protections, instituting major reform of the current conglomeration of federal laws that supposedly protect student privacy.[55] There are also many advocacy organizations such as the Future of Privacy Forum and Common Sense Media that advocate for student privacy in the form of new legislation and agreed upon business standards.[56] Some policy makers and parents are susceptible to the knee jerk reaction of maximum privacy protection for students, and some involved in the education industry are concerned that broadly written legislation could eliminate the many benefits of edtech and student data.[57]

The sheer amount of data collected on individual students—and the fact that schools and school districts generally contract out the processing and storage of student data—further exacerbates privacy concerns.[58] Student data can also be very personal in nature. For example, edtech company Edmodo allows students to create profiles as a part of the students' interaction with virtual classrooms.[59] These classrooms provide students

51. *See id.*
52. Watson et al., *supra* note 49, at 66.
53. Orcutt, *supra* note 13.
54. *Id.*
55. *See* Solove & Schwartz, *supra* note 46.
56. *See Common Sense Media Applauds President Obama for Addressing Important Kids and Family Issues in His State of the Union*, COMMON SENSE MEDIA (Jan. 20, 2015), https://www.commonsensemedia.org/about-us/news/press-releases/common-sense-applauds-president-obama-for-addressing-important-kids-and [https://perma.cc/Z4VW-DRTP] [hereinafter *Common Sense Media*]; *Firms Pledge to Protect Student Data*, *supra* note 1.
57. *See* Butch Gemin et al., KEEPING PACE WITH K–12 DIGITAL LEARNING: AN ANNUAL REVIEW OF POLICY AND PRACTICE 116 (12th ed. 2015); Dynarski, *supra* note 8.
58. *See* Krueger & Moore, *supra* note 10, at 20.
59. Natasha Singer, *Data Security Is a Classroom Worry Too*, N.Y. TIMES (June 22, 2013), http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html [https://perma.cc/F5RN-7YNR].

with access to homework assignments, quizzes, and third-party software.[60] These student profiles allow children to upload a picture and other personal information that is visible within the students' class.[61]

In response to concerns provoked by edtech features like student profiles, recently proposed student privacy laws generally aim to increase parental rights over student data and restrict edtech vendors' use of student data for purposes outside of learning, such as the sale of student data or the use of the data for marketing.[62] Commentators expect that coming legislation will impose more privacy requirements on schools and edtech companies in the near future.[63]

Even if future legislation increases privacy protections and requirements, schools may not sufficiently comply with the new regulation. Some schools have likely violated current student privacy laws like FERPA by allowing companies to have access to student data for profit-seeking rather than educational purposes.[64] However, FERPA and other extant laws lack enforcement power.[65] In the absence of a threat of sanctions, there is little incentive for schools and edtech companies to change their behavior.[66] However, reacting to this problem with unnecessarily restrictive laws that still lack enforcement power may be an ill-fitted solution. Furthermore, without proper oversight of educators' technology use, there remains a great risk that products and services lacking acceptable data security practices or engaging in unauthorized student data profiling will find their way into the classroom, even in the presence of a strong enforcement scheme.[67]

2. Precautionary Social Attitudes Towards Student Privacy: inBloom as an Example

The public reaction to the student data practices of the now-defunct edtech company inBloom provides a helpful illustration of the general attitude towards student privacy.[68] Further, inBloom's story also illustrates

60. *Id.*
61. *Id.*
62. *See* Tanya Roscorla, *A National Look at Student Data Privacy Legislation*, GOV'T TECH. (Sept. 12, 2014), http://www.govtech.com/education/National-Look-at-Student-Data-Privacy-Legislation.html [https://perma.cc/C7P5-ZXXC].
63. *See* Watson et al., *supra* note 49, at 66.
64. Dynarski, *supra* note 8.
65. *See* Solove & Schwartz, *supra* note 46.
66. *See* Dynarski, *supra* note 8.
67. *See* Polonetsky & Tene, *supra* note 9, at 950.
68. *See generally* Natasha Singer, *A Student-Data Collector Drops Out*, N.Y. TIMES (Apr. 26, 2014), http://www.nytimes.com/2014/04/27/technology/a-student-data-collector

the importance of public perception in the realm of student privacy, demonstrating how false perceptions and misunderstandings can quickly lead to the demise of a well-funded corporation, even in the absence of wrongdoing.

InBloom was a nonprofit data management and storage company supported by the Gates Foundation.[69] It had many of the same goals as other edtech companies.[70] Specifically, inBloom wanted to analyze student information to better customize lessons for individual students and collect individual student data to help teachers track student progress.[71] Parents were extremely concerned about the prospect of an outside organization holding a vast amount of student data in the cloud, the sheer amount of data that inBloom sought to collect, and inBloom's analysis of this data.[72] Parents and privacy advocates portrayed the company as an entity with questionable motives.[73] Parents also recognized—and were bothered—that schools were generally not equipped to provide effective oversight into how organizations like inBloom were using student information in practice.[74] As public criticism gradually grew into an uproar, inBloom was forced to shut down after only fifteen months.[75] In the end, the nonprofit that "planned to collect and integrate student attendance, assessment, disciplinary and other records from disparate school-district databases, put the information in cloud storage and release it to authorized web services . . . that could help teachers track student's progress" ceased operations without legal wrongdoing. Part II will discuss the current legal landscape that governs edtech companies like inBloom.[76]

II. WHERE WE ARE NOW: EXISTING LAW

Student privacy rights are protected by an overlapping combination of laws. Currently, several federal statutes jointly govern student data privacy. FERPA, the Children's Online Privacy Protection Act of 1998 (COPPA), and the Protection of Pupil Rights Amendment (PPRA) all address

-drops-out.html [https://perma.cc/7YZ8-37ZJ] [hereinafter *Student-Data Collector Drops Out*].

69. *Id.*
70. *See id.*
71. *See id.*
72. *See id.*
73. *See id.*
74. *See id.*
75. *See id.*
76. *See id.*

different aspects of student privacy.[77] These statutes have been widely described as outdated, as all three statutes were enacted at a time with vastly different technological, business, and education landscapes.[78] Aside from an update to the COPPA rules, the current student privacy regulatory scheme does not specifically contemplate edtech companies.[79]

State legislatures have passed many student privacy laws in the last few years to try to modernize the law and address gaps in the federal law that have become apparent with the spread of digital technology.[80] For example, recent expansions in state student privacy laws have largely put an end to the once common practice of selling student data generated and gathered by edtech products.[81] The current wave of state laws respond to parental concerns over Internet data security and generally "spell out procedures for collecting, storing, and using student data or prohibit the gathering of certain types of sensitive data, like info related to health, religion, or political affiliations."[82] California passed its landmark student privacy bill—SOPIPA—in the midst of the student privacy legislation wave.[83]

A. SOPIPA

California has long been considered a leader in privacy law.[84] The state is credited as the first to pass a data breach notification law, and also recently passed a groundbreaking law that grants children and young adults the right to permanently delete content they post on various online services and applications.[85] SOPIPA demonstrates that California is also at the forefront of student data privacy law.

SOPIPA is a California student privacy bill that limits "commercial advertising, marketing and profiling by operators of websites or providers of

77. *See* 20 U.S.C. §1232g (2012); 15 U.S.C. §§ 6501–6506 (2012); 20 U.S.C. § 1232h (2012).

78. *See* Polonetsky & Tene, *supra* note 9, at 974–75.

79. *See* Krueger & Moore, *supra* note 10, at 20.

80. *See* Polonetsky & Tene, *supra* note 9, at 972–75; Vance, *supra* note 50.

81. Orcutt, *supra* note 13.

82. *Id.*

83. *See* Polonetsky & Tene, *supra* note 9, at 973–74; Vance, *supra* note 50.

84. *See* Maritza Jean-Louis, *California Breaks New Ground in Education Privacy Law with K–12 Student Privacy Bill*, PROSKAUER PRIVACY BLOG, (Sept. 17, 2014), http://privacylaw.proskauer.com/2014/09/articles/california/california-breaks-new-ground-in-education-privacy-law-with-K–12-student-data-privacy-bill [https://perma.cc/K4D5-LAQH].

85. *Id.*

Internet services or mobile applications."[86] The law specifically governs any "operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes."[87] SOPIPA defines "K–12 purposes" as "purposes that customarily take place at the direction of the K–12 school, teacher, or school district . . . including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school."[88] Notably, influential stakeholder groups like the California Teachers Association, the California State PTA, and Common Sense Media supported SOPIPA,[89] which went into effect at the start of 2016.[90]

SOPIPA is both an attempt to update student data privacy law, and supplements existing federal laws (FERPA, COPPA, PPRA). It is the first comprehensive law and is notable because it explicitly targets edtech companies.[91] SOPIPA specifically targets "operator[s] of [I]nternet web site[s], online service[s], online application[s], or mobile application[s]."[92] Cloud computing services are also included in the category of "online services."[93] And even though SOPIPA is a California law, it applies to companies based outside of California that reach California K–12 students.[94]

1. Prohibited Use and Disclosure of Student Data

SOPIPA prohibits edtech companies ("operators") that collect or create student data from selling the data or using it themselves for the purpose of

86. *See* Jim Halpert & Michelle Anderson, *State Privacy and Security Developments – Looking Back and Looking Ahead*, BLOOMBERG BNA (Feb. 9, 2015); CAL. BUS. & PROF. CODE §§ 22584–22585 (2014).

87. CAL. BUS. & PROF. CODE § 22584(a).

88. *Id.* § 22584(j).

89. S. RULES COMM., S.B. 1177 BILL ANALYSIS, (Cal. 2014) http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_cfa_20140826_135115_sen_floor.html [https://perma.cc/R4UC-X7VC].

90. CAL. BUS. & PROF. CODE § 22585.

91. *See* Krueger & Moore, *supra* note 10, at 21.

92. CAL. BUS. & PROF. CODE § 22584(a).

93. *Id.* § 22584(h).

94. Randy Sabett, *How Student Privacy and California's SOPIPA May Affect You,* JD SUPRA BUSINESS ADVISOR (Nov. 20, 2014), http://www.jdsupra.com/legalnews/blog-how-student-privacy-and-california-93991 [https://perma.cc/MA43-ZSQG].

targeted advertising.[95] Consistent with this prohibition on the use of student data for certain commercial ends, SOPIPA also prohibits the sale of student data.[96] Further, SOPIPA also restricts the creation of a profile of data on an individual student unless the profile is "amassed" for "K–12 school purposes."[97]

Disclosure of "covered information" under SOPIPA is generally prohibited.[98] "Covered information" includes any personally identifiable information created or provided by a student or parent transmitted to an "operator in the course of the use of the operator's site, service, or application for K–12 school purposes."[99] "Covered information" also includes information that is gathered by an operator through the operation of their site, service, or application that "is descriptive of a student or otherwise identifies a student."[100] SOPIPA permits disclosure of "covered information" only if it is made: "in furtherance of the K–12 purpose of the site;" in order to "ensure legal and regulatory compliance;" "to respond to or participate in judicial process;" for certain safety purposes; or if disclosure is made to another service provider with several restrictions attached.[101] This allowable disclosure is clearly limited. While SOPIPA is clear in its general opposition to the use of student data for commercial purposes, the law explicitly permits operators to use information for "maintaining, developing, supporting, improving, or diagnosing [problems with]" their site, service, or application.[102]

2. Affirmative Obligations for Edtech

In addition to the restrictions discussed above, SOPIPA places affirmative obligations on operators. Companies that handle student data must "maintain reasonable security procedures" to protect student data from "unauthorized access, destruction, use, modification, or disclosure."[103] The "reasonable security procedures and practices" must be "appropriate to the

95. Halpert & Anderson, *supra* note 86. Targeted advertising is prohibited on any "site, service, or application when the targeting of the advertising is based upon any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service, or application." CAL. BUS. & PROF. CODE §§ 22584(b)(1)(A)–(B).

96. CAL. BUS. & PROF. CODE § 22584(b)(3).

97. *Id.* § 22584(b)(2).

98. *Id.* § 22584(b)(4).

99. *Id.* § 22584(i)(1).

100. *Id.* § 22584(i)(3).

101. *Id.* § 22584(b)(4).

102. *Id.* § 22584(c).

103. *Id.* § 22584(d)(1).

nature of the covered information."[104] SOPIPA also requires operators of online websites or services to delete student data at the request of a school or school district, but only if that data is under the control of the school or district.[105]

3. Deidentified Student Data

SOPIPA treats deidentified student data differently from personally identifiable information.[106] Operators are permitted to use deidentified student information that would otherwise be covered by the law within a site, service, or application owned by the operator with the purpose of improving educational products.[107] The deidentified student data can also be used for marketing purposes in order to "demonstrate the effectiveness of the operator's application or service."[108] Furthermore, SOPIPA allows operators to share "aggregated" deidentified covered student data for the development or improvement of other educational products.[109]

4. Enforcement

SOPIPA itself does not contain any explicit enforcement provisions. Drafters expected it to be enforced through California's Unfair Competitions Law (UCL).[110] The UCL permits California's Attorney General, district attorneys, and certain qualifying city attorneys to file an action for unfair competition.[111] Additionally, the UCL permits a "person who has suffered injury in fact and has lost money or property as a result of the unfair competition" to file an action for relief. [112]

B. THE IMPACT OF THE STUDENT PRIVACY PLEDGE

Shortly after the passage of SOPIPA, a number of edtech companies agreed to sign the Future of Privacy Forum's Student Privacy Pledge.[113] The Student Privacy Pledge was designed to address some of the weaknesses in FERPA as well as some of the student privacy issues discussed at the state level.[114]

104. *Id.*
105. *Id.* § 22584(d)(2).
106. *See id.* § 22584(f)(1).
107. *Id.* § 22584(f)(1).
108. *Id.* § 22584(f)(2).
109. *Id.* § 22584(g).
110. CAL. BUS. & PROF. CODE §§ 17200–17209 (West 2015).
111. *Id.* § 17204.
112. *Id.*
113. *Firms Pledge to Protect Student Data*, *supra* note 1.
114. *Id.*

1. Growth of the Pledge

The Future of Privacy Forum developed the pledge with the help of the Software & Information Industry Association.[115] Initially, fourteen companies agreed to take the pledge, including Microsoft and Houghton Mifflin Harcourt.[116] Similar to SOPIPA, companies that took the pledge are "publicly committing themselves not to sell information on kindergartners through 12th graders."[117] The signatory companies also agreed not to use student data to target students with advertisements and not to create profiles of individual students without school or parent permission.[118] In this way, the pledge is largely taking the core provisions of SOPIPA and extending them across state lines.[119] Prior to publicly acknowledging their commitments, the initial signatories ensured they already complied with the requirements of the pledge in their business operations.[120] And while the pledge is not legally binding, failure to uphold their commitment could land signatory companies in hot water with the Federal Trade Commission due to violations of their own public representations of their privacy practices.[121] Some analysts suggest that edtech companies chose to take this pledge in order to "fend off tighter regulation" by "plug[ging] some of the loopholes in federal privacy law."[122]

The pledge has gathered momentum since its initial announcement. While Apple and Google initially refused to sign the pledge, both companies have since signed on.[123] This represents a transition for Google in this area, as the company admitted that it had used student e-mail data for advertising purposes until early 2014.[124] The rapid increase in signatories of the pledge is also, at least partially, the result of President Obama's

115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. *See* CAL. BUS. & PROF. CODE § 22584(g); *see also Firms Pledge to Protect Student Data*, *supra* note 1.
120. *Firms Pledge to Protect Student Data*, *supra* note 1.
121. *Id.*
122. Stephanie Simon, *Student Privacy Pledged; Critics Scoff*, POLITICO (Oct. 7, 2014), http://www.politico.com/story/2014/10/student-privacy-tech-companies-111645 [https://perma.cc/3VEA-53EK].
123. Alistair Barr, *Google Changes Course, Signs Student Data Privacy Pledge,* WALL ST. J. (Jan. 20, 2015), http://blogs.wsj.com/digits/2015/01/20/google-changes-course-signs-student-data-privacy-pledge [https://perma.cc/288N-QBSM].
124. Roscorla, *supra* note 62.

endorsement—and school districts' awareness—of the pledge in negotiations with potential edtech service providers.[125]

2. Criticisms of the Pledge

Critics of the Student Privacy Pledge note that in the absence of concrete federal protections, these types of voluntary efforts can often lack oversight.[126] Some have criticized the privacy pledge for failing to require specific security measures, "such as encryption of logins for sites that collect personal details about students."[127] Some companies that have signed the pledge do not even have basic encryption for their login process.[128]

While large, wealthy companies like Google and Apple are signatories of the pledge, the pledge does not stop them from collecting data produced by students in the classroom. For example, Google is a large provider of low-cost laptop computers to schools around the country.[129] Google's Chromebook is extremely attractive to schools because it is cheap and able to easily perform many functions valuable to teachers.[130] The Chromebook comes with Google's free Apps for Education services pre-installed to make the Chromebook even more appealing to teachers and schools.[131] When schools receive their Chromebooks, a feature known as "Google Sync" is enabled. Google Sync sends each student user's browsing history to Google.[132] Furthermore, the data remains associated with each student's personal account, which contains personal information such as his birthday.[133] According to the Electronic Frontier Foundation, Google's practices regarding student use of Chromebooks demonstrate that it is far

125. *See* Barr, *supra* note 123.

126. *Firms Pledge to Protect Student Data*, *supra* note 1.

127. Natasha Singer, *Data Security Gaps in an Industry Student Privacy Pledge*, N.Y. TIMES (Feb. 11, 2015), http://bits.blogs.nytimes.com/2015/02/11/data-security-gaps-in-an-industry-student-privacy-pledge [https://perma.cc/385Z-3MSU].

128. *Id.*; *see also* Natasha Singer, *Digital Learning Companies Falling Short of Student Privacy Pledge,* N.Y. TIMES (Mar. 5, 2015), http://bits.blogs.nytimes.com/2015/03/05/digital-learning-companies-falling-short-of-student-privacy-pledge [https://perma.cc/4GQE-9XZP] (noting how odd it is that many companies signed a pledge that requires them to "maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information" without an "elementary security measure" like full encryption for their login process) [hereinafter *Digital Learning Companies Falling Short*].

129. Nate Cardozo, *Internet Companies: Confusing Consumers for Profit*, ELECTRONIC FRONTIER FOUND. (Oct. 14, 2015), https://www.eff.org/deeplinks/2015/10/internet-companies-confusing-consumers-profit [https://perma.cc/5MVE-8Z24].

130. *See id.*

131. *See id.*

132. *Id.*

133. *Id.*

too difficult to determine what a company is doing with student data.[134] While students and school districts have the option to opt out of Google Sync, most school districts were unaware that Google was collecting their browsing data.[135] If Google, a highly visible and established company, and a signatory of the Student Privacy Pledge, is still engaged in this highly questionable collection of student data, it raises larger concerns about the student data practices of lesser known edtech companies and those who have refused to sign the pledge.

C. FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974

FERPA was the first law to establish student privacy rights, passed in 1974.[136] It defined which parties are permitted to access and share student data.[137] It was also the first to clarify parental rights in their children's information.[138] However, FERPA is largely "ineffective in protecting student privacy in today's digital age."[139]

1. Application and Boundaries of FERPA

FERPA applies to all schools that receive federal funding.[140] It regulates a school's ability to disclose "personally identifiable information" from a student's "education records."[141] Education records are defined as records that "contain information directly related to the student" and "are maintained by an educational agency or institution or by a person acting for such agency or institution."[142] Examples of education records include student grades or disciplinary records.[143] The law requires parental consent prior to the release of education records or any personally identifiable information.[144] Under FERPA, the student's parents have control of their child's privacy rights until the student is no longer a minor.[145]

134. *Id.*
135. *See id.*
136. Tudor, *supra* note 17, at 291.
137. Polonetsky & Tene, *supra* note 9, at 959.
138. *Id.* at 960.
139. Solove & Schwartz, *supra* note 46.
140. 20 U.S.C. §1232g (2012).
141. *Id.* § 1232g(b)(1).
142. *Id.* §1232g(a)(4)(A).
143. Khizar Sheikh & Kimberly Goldberg, *Schools and Digital Education Technologies*, 288 N.J. LAW. 34, 35 (2014).
144. 20 U.S.C. § 1232g(b)(1).
145. Tudor, *supra* note 17, at 291.

There are many exceptions to FERPA that allow school districts to disclose information without parental consent.[146] Two major exceptions are most relevant to the present discussion.[147] First, schools may disclose "directory information" to third-party vendors if disclosure "would not generally be considered harmful or an invasion of privacy."[148] Directory information includes "the student's name, address, telephone listing, date and place of birth . . . [and] dates of attendance."[149] Second, schools may disclose personally identifiable information without consent if "a vendor performs a function that otherwise would be performed by a school employee, has a legitimate interest in that data, and the school directly controls the vendor's use and maintenance of the data."[150] Although disclosure to a vendor is permitted under this exception, a vendor may only use the disclosed personally identifiable information for the authorized purpose and may "not permit any other party to have access to such information without the written consent of the parents of the student."[151] Additionally, FERPA requires that the school keep track of all parties that have accessed the student's education record and the reason that it permitted access to the data.[152]

2. Criticisms of FERPA

There are several criticisms of FERPA. Most importantly, it lacks a sufficient enforcement mechanism, and thus there is little incentive for companies to comply with it.[153] Under FERPA, the Secretary of Education has a duty to take any "appropriate actions to enforce" the law.[154] Even though the text of the statute may describe a wide range of penalties available, the only sanction available to the Department of Education is the power to stop all federal funding to the school.[155] While this penalty seems harsh and might lead schools to comply, the Department of Education has never imposed it,[156] largely because the sanction is impractically severe.[157]

146. Sheikh & Goldberg, *supra* note 143, at 35.
147. *See id.*
148. 34 C.F.R. § 99.3 (2012).
149. 20 U.S.C. § 1232g(a)(5)(A).
150. Sheikh & Goldberg, *supra* note 143, at 35 (citing 20 U.S.C. § 1232g(b) and 34 C.F.R § 99.31(a)(1)).
151. 20 U.S.C. §1232g(b)(4)(B).
152. *Id.* §1232g(b)(4)(A).
153. *See* Solove & Schwartz, *supra* note 46.
154. 20 U.S.C. § 1232g(f).
155. *See* Solove & Schwartz, *supra* note 46.
156. *Id.*
157. *Id.*

Thus the lack of adequate sanctions available for FERPA violations has resulted in "essentially nonexistent" enforcement.[158]

FERPA may also be ill-equipped to deal with the rapid increase in the use of digital technology in schools and is in desperate need of an update or supplemental law.[159] As mentioned, third party companies and organizations often handle student data in today's world. Significantly, FERPA regulation only applies to schools.[160] The Department of Education is therefore unable to enforce the law against third-party businesses, even if these businesses are in control of data that would otherwise be regulated by FERPA.[161] Once the data leaves the school's hands (which happens frequently in today's world), there is no enforcement threat. Along these lines, FERPA also lacks modern data security requirements.[162]

FERPA runs into significant problems when the school uses a cloud computing service provider to analyze or store student data.[163] It fails to assign any real responsibilities to the cloud service provider.[164] In fact, when student data is shared with a cloud computing provider, the provider's data security responsibilities are largely governed by its contract with the school.[165] If the school claims that it is simply outsourcing its own functions when it shares data with the third party, the school is permitted to disclose the otherwise protected education records.[166] A study by Fordham Law School found that contracts between schools and third-party vendors generally did not prohibit the sale or marketing of students' information and did not provide for proper oversight of third-party handling of sensitive data.[167]

158. *Id.*
159. *See id.*; *see also* Polonetsky & Tene, *supra* note 9, at 960, 962.
160. Solove & Schwartz, *supra* note 46.
161. *Id.*
162. "FERPA provides little to no guidance about data governance and security obligations." Polonetsky & Tene, *supra* note 9, at 968.
163. Solove & Schwartz, *supra* note 46 (citing Joel R. Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, FORDHAM CTR. ON LAW & INFO. POL'Y (Dec. 13, 2013), http://ir.lawnet.fordham.edu/clip/2 [https://perma.cc/52AK-AVLL]).
164. *See id.*
165. *See id.*
166. *See id.*
167. *See id.*

D. CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998

Congress passed COPPA to protect the personally identifiable information of children under the age of thirteen on the Internet.[168] The law arose from the increasing ubiquity of Internet use and the worry that corporations, other organizations, and individuals were collecting personal data from children.[169] COPPA was also enacted on the basis that children lack the judgment required to use the Internet safely and are thus in need of additional protection.[170]

Because the statute applies to children, it naturally applies to student data as well. Although it has several problems, COPPA adequately protects children while they use the Internet in many ways. Specifically, it gives parents control over the information that a website operator may collect from their child (under 13).[171] COPPA only applies to website operators or online services that are "directed to children" or websites and services that have "actual knowledge that [they are] collecting personal information from a child."[172] Parental consent must be obtained by the website operator or online service provider prior to collecting a child's information.[173] A school may provide consent in place of a parent "only for use of data for school purposes and for no other commercial purpose."[174] Under COPPA, the definition of "personally identifiable information" has been expanded and may include information not included under FERPA and PPRA.[175]

The statute applies to edtech companies that operate educational websites.[176] However, the FTC recently announced that the statute does not apply to data collection by schools and certain online test providers.[177] Unlike FERPA and PPRA, entities that violate COPPA are subject to civil penalties in an action brought by a state attorney general.[178] Additionally,

168. *See* 15 U.S.C. §§ 6501–6506 (2012).
169. Hoofnagle, *supra* note 14 (chapter 7 manuscript at 1–2).
170. *See id.* (chapter 7 manuscript at 2).
171. *See* 15 U.S.C. § 6502(b)(1).
172. *Id.* § 6502(a)(1).
173. Polonetsky & Tene, *supra* note 9, at 970.
174. *Id.*
175. Sheikh & Goldberg, *supra* note 143, at 35.
176. *Id.*
177. Lesley Fair, *Testing, Testing: A Review Session on COPPA and Schools*, FED. TRADE COMM'N (Jan. 23, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/01/testing-testing-review-session-coppa-schools [https://perma.cc/8ARE-2FBM].
178. *See* Sheikh & Goldberg, *supra* note 143, at 35.

those in violation of the statute may be subject to a FTC enforcement action that can result in fines in excess of $1 million.[179]

Many website and online service operators attempt to work around the requirements of COPPA by explicitly stating that their platform or product is intended to be available only to children thirteen years or older.[180] However, younger children are often able to work around this requirement and continue to use the online product without receiving the intended protections of COPPA.[181]

Additionally, while COPPA requires that website operators obtain parental consent and provide a privacy policy that details the website's data collection practices prior to collecting a child's covered information, it is common for operators to reserve the right to unilaterally amend their privacy policy.[182] This places the burden on the parent to monitor the privacy policies for any changes.[183] Otherwise, children could unintentionally be exposed to suspect data collection and use practices.[184]

Because Congress acted quickly when it enacted COPPA, the statute lacks an extensive legislative history.[185] This has made it difficult to identify congressional intent behind COPPA. Thus, COPPA has been used as both "an information privacy law and an online safety measure."[186] The law largely attempts to achieve both goals and, in so doing, fails to comprehensively address children's online privacy in an effective manner.

Aside from its shortcomings as to its limited scope and emphasis on parental consent, the following example demonstrates COPPA's other failures. Google Apps for Education is governed by COPPA.[187] Google places the burden on the school district to acquire the required parental consent under COPPA.[188] The company applies the standard privacy policy for all users to children.[189] Effectively, parents have the choice to consent to Google's terms, or "refus[e] to allow their child to participate in the educational activities associated with the Google Education App."[190] In

179. *See id.*
180. Polonetsky & Tene, *supra* note 9, at 971.
181. Hoofnagle, *supra* note 14 (chapter 7 manuscript at 3).
182. Tudor, *supra* note 17, at 320.
183. *See id.*
184. *See id.*
185. *See* Hoofnagle, *supra* note 14 (chapter 7 manuscript at 2).
186. *Id.*
187. *See* Tudor, *supra* note 17, at 321.
188. *Id.*
189. *Id.*
190. *Id.* at 322.

addition, once Google obtains parental consent through the school as its intermediary, Google has "reserved the right to unilaterally amend its privacy policy, which essentially renders the policy meaningless."[191] This demonstrates that COPPA ultimately lacks teeth and can easily be worked around.

E. PROTECTION OF PUPIL RIGHTS AMENDMENT

Like FERPA, the Protection of Pupil Rights Amendment (PPRA) applies to educational agencies that receive federal funding, and does not contain a private right of action.[192] Specifically, the statute regulates student participation in surveys or evaluations that reveal specific types of information.[193] In addition, the statute restricts a school's ability to disclose, use, or sell student information that falls under the statute for marketing purposes without first notifying the student's parents and presenting them with the opportunity to opt-out.[194] However, the restrictions in PPRA do not apply when "the collection, disclosure, or use of personal information collected from students [is] for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions."[195]

The distinction between PPRA and FERPA is that PPRA is implicated when a school collects certain types of personal information from a student, while FERPA protects a student's education records from disclosure.

III. SOPIPA AS A SOLUTION TO SHORTCOMINGS IN STUDENT PRIVACY LAW

An effective solution to the issues edtech presents must consider privacy concerns specific to children as well as stakeholder expectations of student data privacy. SOPIPA addresses some, but not all, relevant concerns, making it an admirable yet imperfect attempt to enhance student privacy protections in the face of the developing edtech industry.

A. PRIVACY CONCERNS SPECIFIC TO CHILDREN

U.S. law often treats children as a distinct class in need of increased protection. For example, children cannot enter into enforceable contracts, and society does not perceive children as "rational actors who can bargain

191. *Id.*
192. *See* Tudor, *supra* note 17, at 296.
193. *See* 20 U.S.C. § 1232h(b) (2012).
194. *See id.* § 1232h(c)(2); *see also* Polonetsky & Tene, *supra* note 9, at 972.
195. 20 U.S.C. § 1232h(c)(4)(A).

for their privacy in the marketplace."[196] Children are also unable to consent to personal data collection.[197] In light of these principles, edtech companies must be cautious in determining the scope and manner of data collection, and permitted data use, of data collected from children. Children engage with society in their roles as students in K–12 systems. Students are presumably less concerned than adults about the dangers of creating a large personal data profile that is highly accessible to companies and potential criminals.[198] They are also less likely to be able to comprehend that once data is created, and is somehow associated with their account, profile, or other personal identifier, the information exists in perpetuity and may follow them in their future endeavors.

B. STUDENT DATA PRIVACY EXPECTATIONS

It is common practice for schools to collect student data for administrative and performance purposes. Collection of data points such as student attendance, grades, test results, and low-income status by the school receives little resistance and is generally accepted.[199] Collection and use of this data is essential to a well-functioning and successful school, and creates opportunity for educator and student improvement.[200] Using student data to measure and analyze performance is also important, as demonstrated by federal programs such as the No Child Left Behind Act and President Obama's Race to the Top Initiative.[201]

However, the rapid adoption of digital technology in schools is causing a lot of uncertainty. Lawmakers, educators, parents, and edtech companies are still engaging in public discussions to define the appropriate nature of students' privacy expectations. Much of this debate has centered on a desire to protect students from unnecessary exposure to commercial activity. However, it is common for schools to be complicit in exposing students to various advertisements and branded merchandise throughout the school (whether that is through product use, fundraisers, etc.).[202] This exposure does not employ individual student data for marketing or other commercial purposes and thus does not implicate student privacy concerns.

196. Hoofnagle, *supra* note 14 (chapter 7 manuscript at 1); *see* Wouter M. P. Steijn & Anton Vedder, *Privacy Under Construction: A Developmental Perspective on Privacy Perception*, 40 SCI., TECH., & HUMAN VALUES 615, 615 (2015).

197. *See* Hoofnagle, *supra* note 14 (chapter 7 manuscript at 16).

198. *See* Steijn & Vedder, *supra* note 196, at 616.

199. *See* Krueger & Moore, *supra* note 10, at 20.

200. *See* Polonetsky & Tene, *supra* note 9, at 940.

201. *See id.* at 941–42.

202. *See* Cardozo, *supra* note 129; *see also* Polonetsky & Tene, *supra* note 9, at 949–54.

Lawmakers face the key question of where to draw the line on commercial activity in schools. Targeted advertising of students and the sale of student data are generally viewed as activities that should be prohibited.[203] Other commercial activity is a much closer call. For example, many edtech companies use student data to improve their education products and services, for research and development purposes in creating new education products and services, and to improve products and services that have nothing to do with education.[204] While some of this activity is undoubtedly beneficial to students and educators in the form of improved and more efficient educational technology, some of this activity is also much more beneficial to companies with access to the student data and may not benefit students. This presents lawmakers with the question of whether to allow edtech companies to use and benefit from student data when students are seeing at most marginal benefits in return. Because much of this activity is important to edtech companies, we must consider how companies are still able to use student data for commercial purposes under SOPIPA and whether commercial use is permitted at all.

C. SOPIPA AS A SOLUTION

Prominent commentators are concerned that the recent waves of state student privacy laws have a tendency to be reactionary in nature and fail to be sufficiently forward-looking in their response to the perceived student privacy problem.[205] In order to fully evaluate SOPIPA and to determine whether it is an effective solution, an understanding of how it will affect different types of edtech companies and an examination of the behavioral incentives and disincentives it creates for these companies are necessary. Many of the problems with the current patchwork of student privacy laws, aside from their fragmentation and limited scope, stem from the laws' inability to incentivize companies to properly secure student data or even comply with the law. This analysis will also assess how SOPIPA addresses common parent and teacher complaints concerning the current state of the law. Finally, it is important to examine the California legislature's goals in enacting SOPIPA and its success in achieving those goals.

In its legislative analyses, the California Assembly expressed that SOPIPA was needed to supplement the primary protections of FERPA because:

203. Polonetsky & Tene, *supra* note 9, at 952.
204. *See id.* at 951.
205. *See id.* at 990.

> the growing use of online educational programs and mobile applications has led to an increasing flow of personal information directly from students and teachers to developers of educational programs and applications, and there are no restrictions on how this information may be used, other than restrictions that developers may impose on themselves . . . .[206]

The Assembly went on to review a number of current privacy policies of various edtech companies.[207] The investigation found that companies had reserved the right to disclose student personal information to other companies, absolved themselves of responsibility for "mishandling student information," and reserved the right to "unilaterally change its privacy policy at any time."[208] SOPIPA was designed to "limit[] the use of personal information that [was] obtained through" students use of "online educational programs and mobile applications."[209] Specifically, the legislature was uncomfortable that the current regulatory scheme does not protect students' personal information, which would have been otherwise protected under FERPA if obtained from school records.[210]

SOPIPA successfully covers much of what was left in the gaps of pre-existing federal laws.[211] It brings student privacy law into the modern edtech era. It also successfully addresses the goals of the California legislature.[212] Under SOPIPA, companies are only permitted to disclose student personal information to other companies under select circumstances.[213] It also imposes meaningful penalties on edtech companies who mishandle student information, while not crippling their operations. For example, companies are required to "implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information," while also protecting "that information from unauthorized access, destruction, use, modification, or disclosure."[214] This places an affirmative obligation on companies and attempts to hold them responsible for failing to institute

206. S.B. 1177 BILL ANALYSIS: SENATE THIRD READING, at 7 (Cal. 2014), http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_cfa_20140821_233112_asm_floor.html [https://perma.cc/FVA4-NKMJ].

207. *Id.*

208. *Id.*

209. *Id.*

210. *Id.*

211. *See* CAL. BUS. & PROF. CODE § 22584 (2014).

212. *Id.*; *see* S. RULES COMM., S.B. 1177 BILL ANALYSIS, (Cal. 2014), http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_cfa_20140826_135115_sen_floor.html [https://perma.cc/BVJ9-88HX].

213. CAL. BUS. & PROF. CODE § 22584(b)(4).

214. *Id.* § 22584(d)(1).

proper security procedures and failing to reasonably protect student data.[215] Additionally, SOPIPA succeeds in protecting information that would have been protected under FERPA if it were disclosed by a school by prohibiting operators from disclosing personally identifiable information and further restricting their use of this information.[216] Further, SOPIPA often casts a wider net than FERPA does because it applies to other student information in addition to personally identifiable information. For example, SOPIPA prohibits an operator from "sell[ing] a student's information, including covered information."[217] While "covered information" refers to personally identifiable information under SOPIPA, this language presumably covers student information in addition to "covered information."[218]

The following analysis will look to several themes in student privacy that SOPIPA addresses, or fails to address, to evaluate whether SOPIPA is an adequate model for comprehensive, federal student privacy legislation.

1. Sale of Student Data and Targeted Advertising

Many privacy advocates believe that edtech companies should be prohibited from selling student data and using it to target advertisements at individual students.[219] A 2014 study by the privacy advocate group Common Sense Media determined that eighty-six percent of those surveyed believed that "oversight is necessary to ensure [children's] private information is not exploited for commercial purposes and stays out of the hands of the wrong people."[220]

SOPIPA explicitly and directly responds to these concerns by making it unequivocally illegal to sell any student data to a third party, no matter the content or circumstances.[221] Likewise, targeted advertising, whether on the operator's own site, service, or application, or any other site, service, or application, is prohibited if the information employed for the advertising was gathered from the use of the operators' (the entity engaged in targeted advertising in this case) site, service, or application.[222] This provision seems

215. *See id.*

216. *See id.* § 22584(b); *see also* S.B. 1177 BILL ANALYSIS: SENATE THIRD READING, at 7 (Cal. 2014), http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_cfa_20140821_233112_asm_floor.html [https://perma.cc/Y3CS-MSFT].

217. CAL. BUS. & PROF. CODE § 22584(b)(3).

218. *See id.*

219. Gemin et al., *supra* note 57, at 116.

220. *See Student Privacy Survey*, COMMON SENSE MEDIA, https://www.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf [https://perma.cc/3FYM-RJ7S].

221. *See* CAL. BUS. & PROF. CODE § 22584(b)(3).

222. *See id.* § 22584(b)(1)(A)–(B).

to function as a practical ban on targeted advertising, even if only deidentified data is used. While there is a provision that would permit the operator to use deidentified data in marketing, this would only be permitted to show the "effectiveness of the operator's products or services," not to specifically target advertising.[223] Overall, SOPIPA effectively responds to concerns about the commercialization of student data.

However, it is important to question whether the California legislature's goal of ending targeted advertising is always beneficial to students. Should some targeted advertising be permitted? For example, after a student completes a test or particular course of study in an application or other software program, and the company has collected data on the student's performance, there may be educational benefits in allowing a company to recommend a new program to the student and his parents based on this student's data.[224] This would promote education customization and would help connect students with the most appropriate learning tools. But SOPIPA would likely prohibit targeting of this nature. While SOPIPA does permit marketing of educational products directly to parents, it prohibits marketing to parents that employs "covered information."[225] SOPIPA's prohibition on targeted advertising[226] likely prohibits an operator from targeting a student's parent or teacher with advertising based on the student's past performance on the operator's site or service, which might have yielded educational benefits. This might be a drawback and unintended consequence of SOPIPA.

2. New Market Incentives

Another drawback to SOPIPA is that it may disincentivize entrepreneurs from entering the edtech industry by increasing baseline compliance costs. SOPIPA may therefore reduce edtech companies' revenue, which could reduce the viability of edtech startups, and thus reduce the diversity of products available for schools to choose from.

Many edtech startups offer a free service or operate on the increasingly common freemium model.[227] Generally, companies that offer their product or service for free must intend to generate revenue in a different manner, often through monetizing customer data.[228] If edtech companies are prohibited from selling customer data or offering targeted advertising, these

223. *See id.* § 22584(f)(2).
224. *See* Polonetsky & Tene, *supra* note 9, at 951–52.
225. CAL. BUS. & PROF. CODE § 22584(o).
226. *Id.* §§ 22584(b)(1)(A)–(B).
227. *See* Polonetsky & Tene, *supra* note 9, at 952–53; *see also Silicon Valley*, *supra* note 7.
228. *See* Polonetsky & Tene, *supra* note 9, at 950.

revenue streams will not be available to them. It will thus be harder for edtech companies to make money. Lack of a viable revenue generation model, could, in turn, lead to a reduction in the pool of available VC funding because VC firms are reluctant to fund companies with no prospect of making money. Indeed, VC firms and other early investors are already concerned about the absence of monetization in many edtech startup business models.[229]

Further, these comprehensive restrictions on the commercial use of student data may lead many companies to face the challenge of finding an alternative way to monetize their product or service, or abandon the edtech industry altogether. Other companies may initially offer their product or service for free in hope that the customer will purchase an enhanced service in the future.[230] Edtech companies may also face increased compliance costs from having to adhere to the many new requirements in SOPIPA. Therefore, an edtech company that lacks distribution and an existing platform ecosystem to drive revenue may find it more difficult to stay afloat under the SOPIPA regime. However, one could argue that companies that rely on the sale of student data and targeted advertising are not companies with sustainable business models in the first place.

The restriction on the use of student data for targeted advertising and the ban on the sale of student data may encourage companies to compete in other ways and find new ways to make money. For example, SOPIPA allows companies to continue to use student data that they create or gather on their site or service "in furtherance of K–12 school purposes."[231] While it is not entirely clear what exactly constitutes a "K–12 purpose," this provision suggests that companies can continue to use the student data that they collect to improve their products or develop new products. Because SOPIPA blocks certain revenue streams that technology companies have relied on in the past, companies now need to find other ways to get a bigger piece of the limited money allocated by states to their education system.[232] Edtech companies may be able to grow their share of the funding pie by becoming an integral part of classrooms and schools and by developing products that can successfully perform tasks that would have previously been the responsibility of a teacher, administrator, assistant, or other staff member. In the long run, this would allow schools to cut staffing costs and free up more dollars to spend on technology.

229. *See Silicon Valley*, *supra* note 7.

230. *See id.* Companies could also offer a free trial and charge once the trial is completed.

231. CAL. BUS. & PROF. CODE §§ 22584(b)(2), (b)(4)(A) (2014).

232. *See Silicon Valley*, *supra* note 7.

For companies that are more established and operate on a platform model, SOPIPA may discourage them from developing a K–12 version of their product or service so as to avoid the obligation of compliance with the law's strict regulations. This, in turn, could have ramifications similar to the loophole in COPPA, where some companies choose to explicitly not target children under thirteen (even though this does not prohibit children from using their site or service). In effect, this may incentivize companies not to install the protections required under the law, but it would not stop teachers and students from using the specific platform. Under these circumstances, students would not be protected by SOPIPA and would thus receive little data privacy protection.

Although SOPIPA may introduce some problematic incentives, it also likely creates positive market incentives that are consistent with the overall goals of the law. If large companies that operate platforms want to target students, the law effectively forces them to create a K–12 version of their product so as to comply with the law. Many of the larger companies in the edtech space are capable of creating student versions of their products and are incentivized to do so in order to access a large number of students. An example of such a student version is the ad-free version of Gmail that Google offers to educational institutions.[233] Microsoft also offers ad-free versions of its Office 365 for Education applications and its Bing search engine.[234] These products targeted at students serve a useful business purpose. For example, the student version of Gmail familiarizes children with Google and its platform so that when they complete school, they will want to continue to use Google's platform, helping Google to gain new users, and ultimately make more money.[235]

In addition, even edtech companies not based in California will almost assuredly serve California students and be subject to SOPIPA because it is relatively easy for most edtech companies to scale.[236] This fact may incentivize edtech companies to release SOPIPA-compliant websites or online services even when the product is not being used by students in California. That said, there is always the chance that companies decide that the law is too burdensome and either choose to stay out of the California

233. *See* David Nagel, *Google Turns Off Ad Scanning in Apps for Education Permanently*, JOURNAL (Apr. 30, 2014), https://thejournal.com/articles/2014/04/30/google-turns-off-ad-scanning-in-apps-for-education-permanently.aspx [https://perma.cc/67E7-N6ZE].

234. Polonetsky & Tene, *supra* note 9, at 980.

235. *See* Jeff Gould, *Google Admits Data Mining Student Emails in its Free Education Apps*, SAFEGOV (Jan. 31, 2014), http://safegov.org/2014/1/31/google-admits-data-mining-student-emails-in-its-free-education-apps [https://perma.cc/64GB-6RSD].

236. *See* Sabett, *supra* note 94.

market or develop a version of their site or application for use only in California.

3. Data Security

While security concerns have been at the forefront of the national privacy debate, SOPIPA only requires that operators "maintain reasonable security procedures and practices appropriate to the nature of the covered information."[237] The law fails to give further guidance regarding what would constitute "reasonable security procedures."[238] This provision is alarmingly ambiguous because data security is a significant challenge for many edtech startups. Given that many edtech companies have significant gaps in their security procedures, an unclear security standard presents a very legitimate concern for parents.[239]

The incentives created by SOPIPA's security provision largely depend on the manner in which the provision is interpreted in future enforcement actions. If the term "reasonable security procedures" is not given more specificity, it may be that companies, particularly startups, will treat the provision as an indication that security standards are not going to be taken seriously under SOPIPA. While there may be some consensus as to what constitutes "reasonable security procedures" in other areas of the law, this provision may invite certain companies to ignore security standards. This may be particularly true in an area of the law that has lacked proper enforcement and oversight in the past, lacks a well-developed modern body of law, and deals with students, a group that possesses characteristics distinct from the general population.

4. Data Deidentification

SOPIPA is silent as to the standard that operators will be held to in terms of the level of personal data deidentification it requires. Therefore, one potential concern is that SOPIPA inadequately protects student privacy because it allows companies too much latitude in their use of deidentified data. Because privacy risks may remain when deidentified student data is not "irreversibly made anonymous," the effectiveness of deidentification

237. *See* CAL. BUS. & PROF. CODE § 22584(d)(1) (2014).

238. *See* Sabett, *supra* note 94.

239. *See* Natasha Singer, *Uncovering Security Flaws in Digital Education Products for Schoolchildren,* N.Y. TIMES (Feb. 8, 2015), http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html [https://perma.cc/6PLY-ZQDZ]; *see also Digital Learning Companies Falling Short, supra* note 128.

largely turns on the standard for deidentification used in the law, and the way that law is enforced. [240]

The Department of Education provides guidance insofar as it offers a definition of deidentified data, but SOPIPA does not appear to explicitly require companies to adhere to this guidance.[241] The Department of Education defines data deidentification as "the process of removing or obscuring any personally identifiable information from student records in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them."[242] Even this statement has an element of ambiguity. This ambiguity could lead to conduct that was intended to be prohibited when the California legislature passed the law.

5. Enforcement, Ambiguity, and Educator Awareness

A law is generally only as strong as its enforcement. Many of FERPA's failures can be attributed to its poor enforcement provisions.[243] While SOPIPA seems to address some of the enforcement issues with the current federal scheme, particularly FERPA, questions remain as to how effectively the law will be enforced.

Much of SOPIPA provides exceptions for certain conduct on the part of operators if the conduct is "in furtherance of a K–12 purpose."[244] Prominent cybersecurity and privacy lawyer Randy Sabett has suggested that because SOPIPA is a new law, its definition of what constitutes a K–12 purpose is not entirely clear.[245] Because the definition of this term is key to the enforcement of the law, any ambiguity could lead to a number of loopholes that would allow operators to use student data for a commercial purpose disguised as a K–12 purpose under the law.

SOPIPA may also be unable to combat a lack of teacher and administrator awareness of student privacy law and issues. For example, if a teacher is not aware that a product may not meet SOPIPA's standards, and the product does not go through a district- or school-wide review, there is little that the law can do. This is especially true in the case of free edtech products, which are naturally more likely to fall short of the comprehensive

240. *See* Polonetsky & Tene, *supra* note 9, at 975.

241. *See id.*

242. U.S. DEP'T OF EDUC. PRIVACY TECHNICAL ASSISTANCE CTR., PTAC-GL, DATA DE-IDENTIFICATION: AN OVERVIEW OF BASIC TERMS (updated May 2013), http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf [https://perma.cc/5PYM-XHWT].

243. *See* Solove & Schwartz, *supra* note 46.

244. *See* CAL. BUS. & PROF. CODE § 22584.

245. *See* Sabett, *supra* note 94.

privacy standards in SOPIPA. Additionally, because teachers have some autonomy, free products are much less likely to go through any sort of privacy or data security review at the school or district level.[246] And because it is difficult for a law to address a lack of teacher or administrator awareness of privacy issues, teacher training on the issue is integral to an adequate regulatory scheme. Additionally, most schools lack an individual that is an expert in student privacy issues.[247] An ideal scheme would provide for an individual that teachers and administrators can seek assistance from when there is a potential privacy issue. This individual would ideally work in each school, but at the very least the school district should employ a privacy expert. Without such a specialist, it will be very burdensome for teachers to ensure that they comply with the law.

While it remains to be seen how SOPIPA will be enforced, any SOPIPA enforcement must be informed, active, and significant in order to ensure broad compliance.

6. Transparency, Consent, and Communication

Parents and other privacy advocates have also made it clear that they value transparency, consent, and communication in connection with the collection and use of student data by edtech companies.[248] Specifically, parents value control over their child's data. However, SOPIPA fails to give parents and students the right to request deletion of their information, leaving that power only to schools, and only when schools have control over the information.[249] This lack of control raises further questions about the potential for student data to follow a student down the line. Without proper controls and assurances, student data could conceivably be used in the future to discriminate against certain individuals in the college application or job-seeking process.[250] This seems to be a legitimate concern in the absence of a strong deletion requirement, especially if SOPIPA lacks strong enforcement or strong security requirements. Furthermore, the longer data

246. *See* Polonetsky & Tene, *supra* note 9, at 950.

247. *See id.* at 978.

248. *See* Bradley Shear, *Edtech Must Embrace Stronger Student Privacy Laws*, JOURNAL (May 28, 2015), https://thejournal.com/articles/2015/05/28/ed-tech-must-embrace-stronger-student-privacy-laws.aspx [https://perma.cc/63AD-3V8E].

249. *See* CAL. BUS. & PROF. CODE § 22584(d)(2).

250. *See* Shear, *supra* note 248, at 8.

is stored, the greater amount of time it is subject to security risks such as data breaches or hacking.[251]

Despite the restrictions SOPIPA places on edtech companies, many argue that a comprehensive scheme is good for companies in the long run and will lead to further adoption of digital technology in schools.[252] If some schools have held off on the adoption of digital technology because of privacy concerns, a comprehensive student privacy law could lead to more digital technology use. Further, SOPIPA's comprehensive nature and support from public authorities, including various privacy advocates and the Obama Administration, will likely increase parents' trust in edtech products.[253] Edtech support of the Student Privacy Pledge signals to parents and educators that many of these companies are at least somewhat worried about the public's lack of trust in their data use. Some experts suggest that if edtech companies were completely transparent about their student data practices, parents and teachers would no longer be hesitant to use their products.[254]

SOPIPA does not require edtech companies to clearly disclose their data collection, use practices, or security measures implemented to protect student information.[255] While it may be onerous for companies to comply with an enhanced disclosure requirement, perhaps the transparency provided by such a disclosure would quell the complaints of the most zealous student privacy advocates. Direct communication with parents and teachers can only be seen as positive in this regard. Allowing parental access to their child's data may also help parents see the potential benefits of current edtech and student data use. As in the case of inBloom, a lack of communication and transparency on the part of the edtech company can lead to a disastrous public response and eliminate the educational benefits of certain types of edtech.[256]

251. Student data is valuable to criminals for identity theft purposes later in the student's life. *See* Katie Kilfoyle Remis, *Locking Down Student Data*, DISTRICT ADMIN. 55, 55 (2015).

252. *See generally* Shear, *supra* note 248; *see also* Polonetsky & Tene, *supra* note 9, at 976–77.

253. *See* S. RULES COMM., S.B. 1177 BILL ANALYSIS, (Cal. 2014), http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_cfa_20140826_135115_sen_floor.html [https://perma.cc/HM9D-CQTV]; *see also Common Sense Media*, *supra* note 56.

254. *See* Shear, *supra* note 248, at 8.

255. *See* CAL. BUS. & PROF. CODE § 22584 (2014).

256. *See Student-Data Collector Drops Out*, *supra* note 68.

IV. CONCLUSION

SOPIPA does not address the concerns of all relevant stakeholders in its attempt to strike a balance between student data privacy protection, edtech innovation, and educational benefits. Due to compromise, ambiguity, and omission, the law does not entirely align with all student privacy best practices suggestions. However, SOPIPA successfully enhances student privacy protections while updating and closing many of the gaps in current law. And while SOPIPA makes compliance with student privacy law somewhat more difficult for edtech companies, particularly startups, it is not overly burdensome. Through compromise, SOPIPA continues to allow edtech companies to use student data to develop products and innovate in many circumstances.

Adequate enforcement of any student privacy law is difficult in the face of schools' limited resources and the inevitable responsibility of teachers and administrators to vet the data practices of edtech companies. In the face of this reality, there must be efforts made to educate schools and teachers about the privacy risks posed by edtech outside of SOPIPA in order to ensure a high likelihood of effective enforcement and widespread compliance.

Further, federal reform is needed to simplify the student data privacy regulatory scheme, which has only increased in complexity with the passage of various state laws on the subject. A single unified federal law would not only be easier for companies to comply with, but would also likely be easier for the government, schools, and parents to enforce. While SOPIPA may need to be tweaked to be passed at the federal level, and some ambiguities in the law may need to be clarified, the law is certainly a step in the right direction and would provide an effective template for the design of a future federal law.[257]

257. In reality, SOPIPA, and its interaction with other laws, adds to the complexity of the federal student privacy scheme. President Obama has endorsed SOPIPA as a template for future federal legislation. *See* Emma Brown, *Obama to Propose New Student Privacy Legislation*, WASH. POST (Jan. 19, 2015), https://www.washingtonpost.com/local/education/obama-to-propose-new-student-privacy-legislation/2015/01/18/2ad6a8ae-9d92-11e4-bcfb-059ec7a93ddc_story.html [https://perma.cc/AA5S-3F7M].