NOTE

Developing a First Amendment Framework for the Regulation of Online Educational Data: Examining California's Student Online Personal Information Protection Act

Katherine P. McGrath[*]

TABLE OF CONTENTS

 J.D. Candidate, UC Davis School of Law, 2016; B.A., Loyola Marymount University, 2013. I would like to thank the *UC Davis Law Review* for giving me the opportunity to write and publish this Note. I am grateful to the individuals whose guidance has informed and improved this Note: Joshua Owen, Professor Ashutosh Bhagwat, Laura Pedersen, and the Members of the UC Davis Law Review. I would like to thank my parents for always believing in me and supporting my education.

INTRODUCTION

With the growth of the educational technology industry,[1] many schools and school districts have integrated online and cloud-based tools into classrooms and internal management systems.[2] As the quantity of student data expands,[3] more states are adopting rigorous student data privacy laws.[4] The U.S. Department of Education's outdated approach to protecting student data has led to concerns that more rigorous privacy laws are necessary.[5] On September 29, 2014,

---

[1] *See* Sharon Noguchi, *California Legislature Passes Stiffest U.S. Bill to Protect K–12 Students' Online Data*, SAN JOSE MERCURY NEWS (Aug. 31, 2014, 3:39 PM), http://www.mercurynews.com/education/ci_26444107/online-privacy-california-passes-nations-stiffest-protections-k.

[2] *See* JOEL REIDENBERG ET AL., *Executive Summary* to PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS (2013), *available at* http://ir.lawnet.fordham.edu/clip/2/ (finding that "95% of districts rely on cloud services for a diverse range of functions including data mining related to student performance, support for classroom activities, student guidance, data hosting, as well as special services such as cafeteria payments and transportation planning").

[3] *See* Stephanie Simon, *The Big Biz of Spying on Little Kids*, POLITICO (May 15, 2014, 05:05 AM EDT), http://www.politico.com/story/2014/05/data-mining-your-children-106676 (reporting increasing statistics of student data mining and associated privacy risks).

[4] *See* Steve Mutkoski, *Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide for School Administrators and Legal Counsel*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 511, 528-29 (2014) (noting that similar student data protection bills have been introduced in Virginia, Kentucky, West Virginia, Maryland, Maine, Nevada, Idaho, and California); Maritza Jean-Louis, *California Breaks New Ground in Education Privacy Law with K–12 Student Data Privacy Bill*, PROSKAUER (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/ ("[A]s of April 2014, 83 bills concerning education data security were being considered in 32 states, according to the Data Quality Campaign, a nonpartisan educational advocacy organization.").

[5] *See* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 64 (2014) (calling Congress to "modernize the privacy regulatory framework under the Family Educational Rights and Privacy Act and Children's Online Privacy Protection Act"); Anita Ramasastry, *Who Is Looking at Your Kids' School Data? Why Congress Needs to Take Note*, JUSTIA.COM (Dec. 17, 2013), http://verdict.justia.com/2013/12/17/looking-kids-school-data-congress-needs-take-note (noting that Family Educational Rights and Privacy Act ("FERPA") "permit[s] schools to share student data with companies to which they have outsourced core functions like scheduling, data management, or test analysis . . . [which] allows private contractors to have the same access to data that school officials would have"); Tanya Roscorla, *Congress Urged to Update Student Data Privacy Law*, GOV'T TECH. (June 27, 2014), http://www.govtech.com/education/Congress-Urged-to—Update-Student-Data-Privacy-Law.html (discussing the debate over updating the 40-year-old FERPA and potential chilling effects to innovation); Daniel Solove, *Big Data and Our*

California Governor Jerry Brown signed the Student Online Personal Information Protection Act ("SOPIPA"), the nation's most aggressive[6] student data privacy law to date.[7] SOPIPA applies to operators of online and cloud-based sites, services, and applications that are primarily used and designed for K–12 school purposes.[8] The law prohibits these operators from using, selling, disclosing, and engaging in targeted marketing with K–12 student data.[9]

In a recent United States Supreme Court case, *Sorrell v. IMS Health Inc.*, the Court struck down Vermont's Prescription Confidentiality Law, which restricted the sale and dissemination of prescriber-identifying information.[10] The Court found this law unconstitutional because it premised the content- and speaker-based restrictions on viewpoint discrimination,[11] and the law failed the commercial speech test[12] established in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[13] *Sorrell* generated a wealth of scholarship contemplating the implications it will have on the future of the commercial speech doctrine and data privacy.[14] Although lower

Children's Future: On Reforming FERPA, SAFEGOV.ORG (May 6, 2014), http://www.safegov.org/2014/5/6/big-data-and-our-children's-future-on-reforming-ferpa (discussing the Executive Office of the President's recent report, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, *supra*).

[6] Jim Steyer, *California Continues to Lead the Nation in Child Privacy Protection*, HUFFINGTON POST (Oct. 7, 2014, 3:35 PM EDT), http://www.huffingtonpost.com/jim-steyer/california-continues-to-l_b_5941848.html (noting that California has taken the lead in ensuring student privacy by passing SOPIPA).

[7] *See Governor Brown Issues Legislative Update*, OFFICE OF GOVERNOR EDMUND G. BROWN JR. (Sept. 29, 2014), http://gov.ca.gov/news.php?id=18741.

[8] Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584(a) (2015).

[9] *Id.* § 22584(b)(1)–(4).

[10] *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2663 (2011).

[11] Viewpoint discrimination occurs when the government actively suppresses the expression of certain ideas or subjects on one side of a debate from the marketplace. *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 387-89 (1992) (discussing examples of speech restrictions that do and do not constitute viewpoint discrimination); First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 784-86 (1978) (explaining that the First Amendment is "plainly offended" when "the legislature's suppression of speech suggests an attempt to give one side of a debatable public question an advantage in expressing its views to the people").

[12] *See Sorrell*, 131 S. Ct. at 2663-64.

[13] 447 U.S. 557, 566 (1980).

[14] *See, e.g.*, Marc Jonathan Blitz, *The Pandora's Box of 21st Century Commercial Speech Doctrine:* Sorrell*,* R.A.V.*, and Purpose-Constrained Scrutiny*, 19 NEXUS: CHAP. J.L. & POL'Y 19, 23 (2014) (arguing that the *Sorrell* majority opinion touches upon the tension between the Court's commercial speech framework and their larger First Amendment jurisprudence); Tamara R. Piety, *"A Necessary Cost of Freedom"? The*

courts have been reluctant to interpret *Sorrell* as substantially changing the commercial speech doctrine, many read *Sorrell* to mean that informational data is core speech (i.e., noncommercial speech).[15] Like Vermont's Prescription Confidentiality Law, SOPIPA restricts the use, sale, and dissemination of informational data, which facilitates an important discussion about the proper balance between data privacy and free speech.[16]

This Note argues that SOPIPA's restrictions on operators' speech are unlikely to survive a First Amendment challenge. It proposes constitutionally sound alternatives to help schools better protect student data. Part I introduces the First Amendment, *Sorrell v. IMS Health Inc.*, and SOPIPA. Part II contemplates the level of First Amendment scrutiny applicable to SOPIPA after *Sorrell*. Part III applies strict scrutiny to SOPIPA's restrictions on disclosing and selling covered information. Part IV applies the *Central Hudson* test to SOPIPA's restrictions on targeted marketing. Finally, Part V proposes solutions to SOPIPA's constitutional flaws.

Incoherence of Sorrell v. IMS, 64 ALA. L. REV. 1, 4 (2012) (discussing *Sorrell*'s shift from the traditional *Central Hudson* test to a "content neutrality test" for commercial speech); Nat Stern & Mark Joseph Stern, *Advancing an Adaptive Standard of Strict Scrutiny for Content-Based Commercial Speech Regulation,* 47 U. RICH. L. REV. 1171, 1171-72 (2013) (contending that the Supreme Court should promulgate an adaptive standard of strict scrutiny for content-based commercial speech regulation based on the foundation laid in *Sorrell*); Hunter B. Thomson, *Whither* Central Hudson*? Commercial Speech in the Wake of* Sorrell v. IMS Health, 47 COLUM. J.L. & SOC. PROBS. 171, 173 (2013) (analyzing lower courts' interpretations of *Sorrell* and advocating for the content- and speaker-based approach to commercial speech).

[15] *See, e.g.*, Beeman v. Anthem Prescription Mgmt., LLC, 58 Cal. 4th 329, 342-43 (2013) (discussing the Supreme Court's support for characterizing factual information as speech for First Amendment purposes in *Sorrell* and other cases); Thomson, *supra* note 14, at 192 (noting that "courts thus far generally have been unwilling to credit the case as signaling a fundamental change, even while acknowledging that the decision seems to point in that direction").

[16] *See* Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 873 (2012); *see also* Blitz, *supra* note 14, at 46 ("[I]f privacy sometimes provides a good rationale for government to limit speech, it is not clear that this should be a component of commercial speech doctrine rather than part of a broader First Amendment rule that might apply, in some cases, to commercial and non-commercial speech alike.").

I. BACKGROUND

A. The First Amendment

In general, the First Amendment stands for the proposition that the government cannot restrict expression based on its message, ideas, subject matter, or content.[17] A content-based restriction on speech is one in which the government bans or burdens certain speech based on its communicative content.[18] The First Amendment does not bar content-based restrictions on traditionally unprotected speech, such as obscenity, defamation, fraud, incitement, and speech essential to criminal activity, among other specific categories.[19] Outside of these special categories, content-based laws are presumptively unconstitutional and may only be justified if the government proves that the restriction satisfies strict scrutiny.[20] Strict scrutiny requires the government to show that the restriction advances a compelling governmental interest and is narrowly tailored to achieve that interest.[21]

---

[17] *See* United States v. Stevens, 559 U.S. 460, 468 (2010); Ashcroft v. ACLU, 535 U.S. 564, 573 (2002); Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 65 (1983); Police Dep't of Chicago v. Mosley, 408 U.S. 92, 95 (1972).

[18] *See* McCullen v. Coakley, 134 S. Ct. 2518, 2531 (2014) (distinguishing content-neutral laws from content-based laws); Ward v. Rock Against Racism, 491 U.S. 781, 792 (1989) (determining if a law is content-based turns on "whether the government has adopted a regulation of speech because of disagreement with the message it conveys . . . . The government's purpose is the controlling consideration"); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 771 (1976) (content neutral laws restrict speech without reference to their content).

[19] *Stevens*, 559 U.S. at 468-69; *see Va. State Bd. of Pharmacy*, 425 U.S. at 771 (stating that fraudulent speech is not protected); Brandenburg v. Ohio, 395 U.S. 444, 447-49 (1969) (explaining that states cannot forbid advocacy unless such advocacy is directed to incite lawlessness); Roth v. United States, 354 U.S. 476, 483-84 (1957) (noting that obscenity is outside the protection of the First Amendment); Beauharnais v. Illinois, 343 U.S. 250, 254-58 (1952) (explaining that defamation is not communication that is safeguarded by the Constitution); Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 498 (1949) (holding that the First Amendment does not extend to speech used as an integral part of criminal conduct).

[20] Reed v. Town of Gilbert, 135 S. Ct. 2218, 2226-27 (2015) (discussing the analytical framework for determining if a law is content-based and concluding that the Town of Gilbert's Sign Code is content-based on its face).

[21] *Id.* at 2231; Ashcroft v. ACLU, 542 U.S. 656, 665-66 (2004) (noting that the purpose of strict scrutiny is to "ensure that speech is restricted no further than necessary to achieve the goal"); Reno v. ACLU, 521 U.S. 844, 846 (1997) (requiring that the government pursue less restrictive alternatives that are at least as effective); Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989) (presenting the First Amendment strict scrutiny framework).

The United States Supreme Court has adopted a "common sense distinction" between content-based laws regulating commercial speech and content-based laws regulating other varieties of speech.[22] The Supreme Court formally recognized that commercial speech was protected under the First Amendment in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc*.[23] The test for identifying commercial speech is whether the speech "proposes a commercial transaction."[24] When noncommercial information accompanies speech that promotes a transaction, the classification of commercial or noncommercial speech becomes less clear and requires further analysis.[25] Having an "economic motivation," labeling the speech as "advertising," or referencing a specific product may not independently render the speech "commercial" for First Amendment purposes.[26] However, if all three of these features are present, then there is a "strong case" that the speech is commercial.[27] Based on this guidance, unless the speech merely proposes a transaction, determining which category the speech falls into requires an evaluation of these additional factors.[28]

To determine if a law regulating commercial speech is constitutional, courts apply a four-prong test from *Central Hudson*.[29] First, the burdened commercial speech must not be illegal or

[22] Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 562-63 (1980); *see* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 455-456 (1978).

[23] *See Va. State Bd. of Pharmacy*, 425 U.S. at 771 (ruling that prohibiting prescription drug price advertising was an unconstitutional violation of free speech because it "single[d] out speech of a particular content and [sought] to prevent its dissemination completely").

[24] Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 473-74 (1989); *Cent. Hudson*, 447 U.S. at 561 (embracing a similar definition of commercial speech: "expression related solely to the economic interests of the speaker and its audience"); *Va. State Bd. of Pharmacy*, 425 U.S. at 762; *see also* United States v. United Foods, Inc., 533 U.S. 405, 409 (2001) (employing the same definition); Bhagwat, *supra* note 16 ("The definition of commercial speech turns on the content of the speech being regulated, not the use that the listener plans to make of the information conveyed."); Thomson, *supra* note 14, at 183 ("The guidance the Court has given seems to indicate that speech advocating purchase meets the definition [of commercial speech].").

[25] *See* Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 66 (1983) (analyzing reproductive health informational pamphlets included with condom advertisements).

[26] *Id.* at 66-67.

[27] *Id.* at 67-68 (categorizing the mailings as commercial speech "notwithstanding the fact that they contain discussions of important public issues such as venereal disease and family planning").

[28] *See supra* notes 17–21 and accompanying text.

[29] *See* Stern & Stern, *supra* note 14, at 1171.

misleading.[30] If the speech is illegal or misleading, it falls outside First Amendment protection.[31] Second, the governmental interest the regulation seeks to achieve must be substantial.[32] Third, the regulation must directly advance the asserted interest.[33] And, fourth, the regulation must not be more extensive than necessary to achieve the governmental interest.[34]

B. Sorrell v. IMS Health Inc.

The 2011 Supreme Court case, *Sorrell v. IMS Health Inc.*, is a recent application of the First Amendment protections afforded to informational data.[35] In *Sorrell*, data miners and an association of pharmaceutical manufacturers challenged Vermont's Prescription Confidentiality Law, which restricted the sale and dissemination of prescriber-identifying information.[36] At the District Court and Court of Appeals, Vermont maintained that these restrictions only applied to the sale and dissemination of prescriber-identifying information for marketing purposes.[37] However, at the Supreme Court, Vermont stated that the law should actually be interpreted to ban pharmacies, health insurers, and similar entities from selling prescriber-identifying information for *any* purpose, subject to certain exceptions.[38] The Court noted procedural problems with this alternative interpretation but stated that the Prescription Confidentiality Law "cannot be sustained even under the interpretation the State now adopts."[39]

Based on the text of the statute and the legislative history, the Court concluded that the Prescription Confidentiality Law imposed a

---

[30] Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980).

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 69 (2014); Stern & Stern, *supra* note 14, at 1171 (noting that *Sorrell* "marked the most recent step in the gradual elevation of commercial speech from 'its subordinate position in the scale of First Amendment values' to its status as a form of expression that routinely enjoys robust protection from the Court"); Marcia M. Boumil et al., *Prescription Data Mining, Medical Privacy and the First Amendment: The U.S. Supreme Court in* Sorrell v. IMS Health Inc., 21 ANNALS HEALTH L. 447, 485-90 (2012) (discussing the privacy and speech implications of *Sorrell*).

[36] *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2660 (2011).

[37] *See id.* at 2662.

[38] *Id.*

[39] *Id.*

content- and speaker-based burden on protected commercial speech.[40] First, the ban on the disclosure and sale of prescriber-identifying information for marketing amounted to a content-based burden.[41] Second, the law imposed a speaker-based burden on pharmacies, health insurers, and similar entities.[42] Applying the *Central Hudson* test, the Court required Vermont to demonstrate "that the statute directly advance[d] a substantial governmental interest and that the measure [was] drawn to achieve that interest."[43] It struck down the statute for failing to satisfy the third and fourth prongs of *Central Hudson* because the law indirectly, yet excessively, favored the State's own viewpoint on detailing.[44]

One important caveat to the majority's opinion in *Sorrell* was the "coherency" of the policy in question.[45] If Vermont had pursued its interest through a "more coherent policy," the case would have been "quite different."[46] Justice Kennedy suggested that a "coherent policy" in this context would have prohibited the sale and disclosure of prescriber-identifying information except in "a few narrow and well-justified circumstances" and not based on viewpoint discrimination.[47] Scholars have contemplated the meaning of this caveat and proposed arguments for why or why not *Sorrell* would be instructive in different policy contexts.[48] This Note contributes to the discussion by applying the principles in *Sorrell* to California's Student Online Personal Information Protection Act.

C. The Student Online Personal Information Protection Act ("SOPIPA")

Federal educational laws have failed to keep up with the rapid growth of student data, creating loopholes through which online

[40] *See id.* at 2663.

[41] *Id.*

[42] *See id.*

[43] *See id.* at 2667-68.

[44] *See id.* at 2670-73.

[45] *See id.* at 2668.

[46] *Id.*

[47] *See id.*

[48] *See, e.g.*, George R. Gooch et al., *The Moral from Sorrell: Educate, Don't Legislate*, 23 HEALTH MATRIX 237, 259 (2013) ("[T]he majority suggested that Vermont could have constructed 'a more coherent policy,' similar to the HIPAA Privacy Rule. The Court was likely implying that more than one party (detailers) should be excluded from using prescriber-identifying information."); Andrew J. Wolf, *Detailing Commercial Speech: What Pharmaceutical Marketing Reveals About Bans on Commercial Speech*, 21 WM. & MARY BILL RTS. J. 1291, 1292 (2013) (applying a modified commercial speech doctrine in the pharmaceutical context).

companies can use student data for commercial purposes.[49] These loopholes stem from gaps in the Family Educational Rights and Privacy Act ("FERPA"), the Children's Online Privacy Protection Act ("COPPA"), and common vendor contracting policies.[50]

FERPA restricts the use and disclosure of students' personally identifiable information ("PII") contained in written and electronic "education records."[51] Education records include emails, communications, and documents created by students, teachers and administrators.[52] FERPA only protects information contained in education records maintained by an educational agency.[53] Thus, FERPA does not protect information directly obtained from a student or teacher through an online tool not subject to a contract with the educational agency. This is so even though the same information would otherwise be protected if contained in an education record.[54]

COPPA requires websites, apps, and online services that collect personal information from children under 13 to provide proper notice of their data collection, use or disclosure policies, and to obtain verifiable parental consent.[55] It applies to operators of commercial websites, online services, and mobile apps that are directed to children under age 13 and to operators of general audience websites that have actual knowledge that they are collecting, using, or disclosing personal information from children under age 13.[56] COPPA inadequately protects K–12 student data because it only applies to students under 13 and to personal information collected *from* children, not personal information *about* children from parents or school officials.[57]

---

[49] *See* Ramasastry, *supra* note 5; Roscorla, *supra* note 5.

[50] *See Children's Online Privacy Protection Act (COPPA)*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/kids/#Criticism (last visited Oct. 27, 2015); Larry Magid, *Letting Children Under 13 on Facebook Could Make Them Safer*, HUFFINGTON POST (June 4, 2012, 8:58 AM), http://www.huffingtonpost.com/larry-magid/facebook-children-under-13_b_1567010.html (discussing various studies finding that over seven million children under 13 used Facebook); Ramasastry, *supra* note 5; Roscorla, *supra* note 5.

[51] *See* 20 U.S.C. § 1232g (2012).

[52] *Id.* § 1232g(a)(4)(A).

[53] *Id.*

[54] *See* ASSEMB. FLOOR ANALYSIS OF S. THIRD READING, S.B. 1177 (as amended Aug. 21, 2014), 2013–14 Reg. Sess., at 5 (Cal. 2014).

[55] *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[56] *Id.* (providing a COPPA compliance guide for businesses and parents).

[57] *Id.*; *see* S. COMM. ON EDUC., ANALYSIS OF S.B. 1177, 2013–14 Reg. Sess., at 2 (Cal. 2014). For the list of categories included in what COPPA defines as "personal information," see *Complying with COPPA: Frequently Asked Questions*, *supra* note 55.

Personal online information created by a student, parent, or school official that does not qualify as an "education record" and is collected by an operator that has complied or is not required to comply with COPPA may be used for commercial purposes that harm children.[58] The American Psychological Association has recognized that advertising in the educational context may have a stronger effect on children than advertising in other contexts because of repeated exposure to advertisements at school and the perception that the advertised product is endorsed by school officials.[59] Others have raised concerns that many K–12 educational applications, websites, and services do not employ standard encryption protocols to protect unauthorized persons or companies from accessing a student's PII.[60] Although FERPA, COPPA, and California state law require operators of online educational tools to implement reasonable data security measures,[61] none of these laws specifically mandate standard encryption protocols.[62]

Commentators call SOPIPA a "landmark" law in the movement to close the loopholes in current federal student privacy laws.[63] SOPIPA

[58] *See* REIDENBERG ET AL., *supra* note 2 ("[F]ewer than 25% of the agreements specify the purpose for disclosures of student information, fewer than 7% of the contracts restrict the sale or marketing of student information by vendors, and many agreements allow vendors to change the terms without notice."); *Advertising to Children and Teens: Current Practices*, COMMON SENSE (Jan. 28, 2014), https://www.commonsensemedia.org/research/advertising-to-children-and-teens-current-practices (observing that online advertising directed at children often blurs the line between marketing and entertainment, making it difficult to quantify its effects); *see also* Danah Boyd, *Which Students Get to Have Privacy?*, MESSAGE (May 22, 2015), https://medium.com/message/which-students-get-to-have-privacy-e9773f9a064#.4ktorjkfn (identifying four different external threats to students whose data is unprotected).

[59] *See* BRIAN L. WILCOX ET AL., REPORT OF THE APA TASK FORCE ON ADVERTISING AND CHILDREN 55-56 (2004), *available at* http://www.apa.org/pi/families/resources/advertising-children.pdf (noting that "commercial pressures in schools may create desires for products that children do not need or cannot afford and/or that are psychologically or physically harmful to them").

[60] *See* 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.

[61] 20 U.S.C. § 1232g (2013); Assemb. Bill No. 1584, 2014 Leg., 2013–14 Reg. Sess. (Cal. 2014) (requiring local educational agencies to include additional requirements and provisions in their contracts with third-party online educational service providers); *Complying with COPPA: Frequently Asked Questions*, *supra* note 55; *see also infra* Part V.

[62] *See* Singer, *supra* note 60.

[63] California Senator Darrell Steinberg introduced SOPIPA in February 2014 to "close[] loopholes that can be exploited by Internet companies for profit through collecting and sharing students' personal information obtained through online services marketed for school purposes." *Student Online Personal Information Protection Act:*

restricts the speech of "operators," entities that knowingly provide online or cloud-based services, sites, or applications primarily designed for K–12 school purposes.[64] SOPIPA prohibits operators from (1) using student data "to amass a profile about a K–12 student except in furtherance of K–12 school purposes," (2) selling "a student's information, including covered information," and (3) disclosing "covered information," unless certain exceptions apply.[65] Additionally, the law prohibits operators from (4) knowingly engaging in targeted advertising based upon any information created or obtained through the operator's service.[66]

"Covered information" is a term of art in SOPIPA that encompasses an expansive list of information.[67] Covered information includes "personally identifiable information or materials" in any media or format that meets any of SOPIPA's statutory criteria.[68] Although this definition includes "materials" in addition to information, I will refer to this as "PII" because SOPIPA does not provide any clear distinction between information and materials. First, covered information includes PII created or provided by a student; a student's parent or legal guardian; or an agent of the school, school district, or local educational agency.[69] The second category of covered information is PII "created or provided" by an educational agency's employee or agent to an operator.[70] The third type of covered information includes PII that is descriptive of a student, or otherwise identifies a student, and is gathered by an operator through its site, service, or application.[71] Examples of covered information that meet the third category's criteria include the student's name, education record, home address, email address, food purchases, text messages, and search

Hearing on S.B. 1177 Before S. Comm. on Educ., 2013–14 Reg. Sess. 4-5 (Cal. 2014) (statement of Sen. Darrell Steinberg); *Common Sense Applauds California Governor Jerry Brown for Signing Landmark Student Privacy Law*, COMMON SENSE (Sept. 29, 2014), https://www.commonsensemedia.org/about-us/news/press-releases/common-sense-applauds-california-governor-jerry-brown-for-signing (quoting James Steyer, CEO and founder of Common Sense Media).

[64] Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584(a) (2015).

[65] *Id.* § 22584(b).

[66] *Id.* § 22584(b)(1)(A).

[67] *Id.* § 22584(i).

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

activity.[72] The criteria for covered information is so comprehensive that it could include virtually any and all PII generated or received by the online tool.[73]

SOPIPA makes exceptions for de-identified covered information in three distinct circumstances. Although the law does not define the term de-identified covered information, the U.S. Department of Education interprets "de-identified" to mean data lacking any personal identifiers.[74] First, SOPIPA does not prohibit operators from using de-identified covered information to improve their product.[75] Second, operators may use de-identified covered information to demonstrate the product's effectiveness, including in their marketing.[76] Third, SOPIPA permits operators to share *aggregated* de-identified covered information to develop and improve online educational tools.[77]

II. DETERMINING THE APPROPRIATE LEVEL OF SCRUTINY

A. Informational Data: Speech or Commodity?

In *Sorrell*, the Court explored, but refused to definitively answer, whether a restriction on the sale and disclosure of PII is a restriction on speech or conduct.[78] Vermont argued that the transfer, sale, and

---

[72] *Id.*

[73] Information gathered by an operator that "is descriptive of a student or otherwise identifies a student, include[s], but [is] not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information." *Id.*

[74] The U.S. Department of Education's Privacy Technical Assistance Center ("PTAC") defines the de-identified data as: "data [that] describes records that have a re-identification code and have enough personally identifiable information removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual." *De-identified Data*, PRIVACY TECHNICAL ASSISTANCE CTR., http://ptac.ed.gov/glossary/de-identified-data (last visited Dec. 26, 2015) (providing definitions for key words relevant to U.S. Department of Education laws, such as FERPA).

[75] *See* BUS. & PROF. § 22584.

[76] *See id.*

[77] *Id.*

[78] *See* Bambauer, *supra* note 35, at 71 (discussing the *Sorrell* opinion); Bhagwat, *supra* note 16, at 860.

use of prescriber-identifying information were conduct, not speech.[79] In response, Justice Kennedy, writing for the majority, noted that "the creation and dissemination of information are speech within the meaning of the First Amendment."[80] He further stated: "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."[81] Based on Justice Kennedy's guidance, this Note adopts the view that the creation, collection, and dissemination of informational data regulated by SOPIPA, including "covered information" and the broader category of "student information," is speech, not conduct. Lower courts have also cited Justice Kennedy's guidance in *Sorrell* to conclude that information is speech.[82]

Nevertheless, some argue that *Sorrell*'s proposition that information is speech is merely dicta, rather than a conclusion of law.[83] However, if the use, sale, and dissemination of PII is not speech, then PII must be a commodity, and activities related to it must be conduct.[84] The *Sorrell* opinion refutes this argument. The Court compared the Vermont law to a hypothetical law prohibiting magazine publishers from

[79] *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2665 (2011).

[80] *Id.* at 2653 ("[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct." (some internal quotation marks omitted)); *see also* Rubin v. Coors Brewing Co., 514 U.S. 476, 481 (1995) ("information on beer labels" is speech); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759 (1985) (plurality opinion determining that a credit report is "speech").

[81] *Sorrell*, 131 S. Ct. at 2667.

[82] *See, e.g.*, Jian Zhang v. Baidu.com Inc., No. 11 CIV. 3388 JMF, 2014 WL 1282730, at * 6 (S.D.N.Y. Mar. 28, 2014) (ruling that a company's Internet search engine results were protected by First Amendment based in part on *Sorrell*'s proposition that the collection and communication of facts are protected by the First Amendment); Telesweeps of Butler Valley, Inc. v. Kelly, No. 3:12-CV-1374, 2012 WL 4839010, at *7 (M.D. Pa. Oct. 10, 2012) ("The information was most likely speech entitled to protection because '[f]acts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs.'") *aff'd sub nom.* Telesweeps of Butler Valley, Inc. v. Attorney Gen. of Pa., 537 F. App'x 51 (3d Cir. 2013); Beeman v. Anthem Prescription Mgmt., LLC, 58 Cal. 4th 329, 342-43 (2013) (discussing the Supreme Court's support for characterizing factual information as speech for First Amendment purposes in *Sorrell* and other cases).

[83] *See, e.g.*, Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1507 (2015) (arguing that even after *Sorrell*, "the 'data is speech' argument makes no sense from a First Amendment perspective").

[84] Neil Richards makes a similar argument and describes information contained in databases as having "more value as a saleable commodity than for the purposes for which it was originally collected." Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1157 (2005).

purchasing or using ink to illustrate that both laws would have the effect of restricting protected speech.[85] The same logic applies to SOPIPA. Even if we assume that the student information is a commodity, SOPIPA restricts it in such a way as to prevent operators from sharing and using it for certain communicative purposes.

Sorrell should be read to require courts to first determine if the law restricting speech is content- and speaker-based, and second, to consider whether the restriction is consistent with the applicable level of First Amendment scrutiny.[86] Thus, if an operator challenges SOPIPA based on the First Amendment, a court will have to consider which level of scrutiny is appropriate. In making this decision, a court may be inclined to apply *Central Hudson* based on the similarities between SOPIPA and Vermont's Prescription Confidentiality Law in *Sorrell*, or it may apply strict scrutiny because SOPIPA restricts noncommercial speech.[87] To harmonize these concerns, a court faced with determining the constitutionality of SOPIPA should first address *Sorrell*'s threshold question of content neutrality, and then apply

[85] *Sorrell*, 131 S. Ct. at 2667.

[86] *See* 1-800-411-Pain Referral Serv., LLC v. Otto, 744 F.3d 1045, 1054 (8th Cir. 2014) (noting that in *Sorrell* "the Court devised a new two-part test for assessing restrictions on commercial speech"); United States v. Caronia, 703 F.3d 149, 163-64 (2d Cir. 2012) ("*Sorrell* engaged in a two-step inquiry. First, the Court considered whether the government regulation restricting speech was content- and speaker-based . . . . Second, the Court considered whether the government had shown that the restriction on speech was consistent with the First Amendment under the applicable level of heightened scrutiny."). Hunter B. Thomson also advocates for adding the two key questions in *Sorrell* to a First Amendment commercial speech analysis. Thomson, *supra* note 14, at 201. He identifies these two additional inquiries as: (1) "[W]hether the government regulation restricting speech was content- and speaker-based," and (2) "Whether 'government had shown that the restriction on speech was consistent with the First Amendment under the applicable level of heightened scrutiny.'" *Id.* at 193.

[87] *See* Educ. Media Co. v. Insley, 731 F.3d 291, 298 (4th Cir. 2013) ("[L]ike the Court in *Sorrell,* we need not determine whether strict scrutiny is applicable here, given that, as detailed below, we too hold that the challenged regulation fails under intermediate scrutiny set forth [in] *Central Hudson*."); Fleminger, Inc. v. U.S. Dep't of Health & Human Servs., 854 F. Supp. 2d 192, 197 (D. Conn. 2012) ("*Sorrell* did not impact the traditional framework for evaluating commercial speech under the First Amendment."); Yeager v. AT&T Mobility, LLC., No. CIV. S-07-2517 KJM, 2011 WL 3847178, at *5 (E.D. Cal. Aug. 30, 2011) (noting that *Sorrell* does not abrogate the commercial speech tests in *Central Hudson* or *Bolger*); N.J. Dep't of Labor & Workforce Dev. v. Crest Ultrasonics Corp., 82 A.3d 258, 268 (N.J. Super. Ct. App. Div. 2014) ("In the wake of the Supreme Court's post-*Sorrell* silence and inaction, many federal and state courts are continuing to apply the standard set forth in *Central Hudson*.").

either strict scrutiny and/or *Central Hudson*, depending upon the purpose and effect of the law's provisions.[88]

B. SOPIPA Is a Content-Based Restriction on Noncommercial and Commercial Speech

The informational data regulated by SOPIPA bears some resemblance to the prescriber-identifying information considered in *Sorrell* in two ways. First, both types of information represent facts about individuals. Second, private entities collect both types of information. The *Sorrell* Court concluded that Vermont's Prescription Confidentiality Law restricted commercial speech because it restricted a form of advertising with prescriber-identifying information.[89] The Prescription Confidentiality Law responded to a particular commercial phenomenon; namely, detailers employed by pharmaceutical companies using prescriber-identifying information to market non-generic drugs.[90] Yet, unlike the Prescription Confidentiality Law, SOPIPA restricts the use of student informational data for both commercial and *noncommercial* purposes.[91]

Scholars have contemplated the level of scrutiny noncommercial informational data should be afforded under the First Amendment. Jane Bambauer argues that the First Amendment supports an implicit right to create knowledge, which extends to the creation and transferability of data.[92] Based on this theory, she proposes the application of strict scrutiny in noncommercial contexts.[93] Ashutosh Bhagwat has argued that while personal data is speech, its private nature warrants a lesser level of judicial scrutiny.[94] Although much of the covered information regulated by SOPIPA may be technical, it does not appear to be inherently commercial. The only listed category within the covered information definition that could reasonably fall under commercial speech is data about students' "food purchases."[95] However, even though food purchase data refers to a transaction, it is not "related solely to the economic interests of the speaker and its

---

[88] *See 1-800-411-Pain Referral Serv.*, 744 F.3d at 1054; *Caronia*, 703 F.3d at 163-64.

[89] *Sorrell*, 131 S. Ct. at 2667.

[90] *Id.* at 2660-64.

[91] *See* Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584 (2015).

[92] Bambauer, *supra* note 35, at 60.

[93] *See id.* at 61-62.

[94] *See* Bhagwat, *supra* note 16, at 880.

[95] *See* BUS. & PROF. § 22584.

audience."[96] For example, data about a student's food purchasing history is socially valuable for child health applications.[97]

Student informational data — including covered information, contextually describing a student's online behavior, search activity, preferences, and patterns — is socially valuable.[98] Hypothetically, an online application that asks a child to keep a log of how many and which books she reads each week may be important to authors, publishers, parents, and non-governmental researchers. Insofar as certain covered information is even slightly socially important, it follows that the disclosure of such information warrants full First Amendment protection.[99] Student informational data is expansive enough to have cultural, psychological, and educational significance warranting strict scrutiny.[100] For example, information about learning habits could potentially be used to create important knowledge for the social sciences, health and development research, and the technology industry in for- and non-profit contexts. Because the level of First Amendment scrutiny turns on the content and purpose of the speech, this Note assesses each of SOPIPA's prohibitions separately.[101]

---

[96] *See supra* notes 24–28 and accompanying text.

[97] *See, e.g.*, J. Williams et al. *A Systematic Review of the Influence of the Retail Food Environment Around Schools on Obesity-Related Outcomes*, 15 OBESITY REVS. 15, 359-374 (2014) (reviewing studies that examine the association between food outlets near schools, students' food purchases, and body weight).

[98] *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 5, at 56.

[99] *See* Junger v. Daley, 209 F.3d 481, 484 (2000) (noting that "all ideas having even the slightest redeeming social importance . . . have the full protection of the First Amendment") (quoting Roth v. United States, 354 U.S. 476, 484 (1957)).

[100] *See generally* TECHNOLOGY AND PSYCHOLOGICAL WELL-BEING 34-76 (Yair Amichai-Hamburger ed., 2009) (discussing the psychological and social effects online educational tools have on society and on youth); Wu He, *Examining Students' Online Interaction in a Live Video Streaming Environment Using Data Mining and Text Mining*, 29 COMPUTERS IN HUM. BEHAV. 90, 90-102 (2013) ("[U]sing data mining and text mining techniques for a large amount of online learning data can yield considerable insights and reveal valuable patterns in students' learning behaviors."); Jui-long Hung & Ke Zhang, *Revealing Online Learning Behaviors and Activity Patterns and Making Predictions with Data Mining Techniques in Online Teaching*, 4 MERLOT J. ONLINE LEARNING & TEACHING 426, 426-37 (2008) (using student online learning behaviors to improve instructional strategy and course design improvement).

[101] *See* 1-800-411-Pain Referral Serv., LLC v. Otto, 744 F.3d 1045, 1054 (8th Cir. 2014) ("The first question to ask is whether the challenged speech restriction is content- or speaker-based, or both."); *see also id.* at 1054-61 (applying *Sorrell* and *Central Hudson* to each part of the law in question).

1. Disclosing and Selling Covered Information

SOPIPA restricts operators from disclosing covered information except in certain narrow circumstances, and from selling "a student's information, including covered information."[102] In *Sorrell*, the Court accepted the Vermont District Court's conclusion that "[a] restriction on disclosure is a regulation of speech, and the 'sale' of [information] is simply disclosure for profit."[103] Similar to disclosing covered information, selling a student's information is not necessarily commercial speech even though it involves a transaction. The substantive content of the student's information being sold may not "propose a transaction."[104] Thus, the sale of noncommercial student information, including covered information, could be analogous to the sale of a literary work in the sense that both are "speech for profit," and yet are not commercial speech.[105] Since SOPIPA only permits the disclosure of covered information to government or government-affiliated researchers, it precludes an operator from selling covered information to a non-governmental research institution. It is easy to imagine hypothetical ways in which non-governmental research institutions could use this information for biological, social, and educational development studies. For example, perhaps a private research group would like to use de-identified online behavioral information to study the acquisition of hand-eye coordination through technology.

Based on this analysis, SOPIPA's ban on disclosing covered information and selling a student's information is a content-based restriction on noncommercial protected speech.[106] The law is content-based for two reasons. First, SOPIPA specifically limits the use and sale of certain information based on its subject matter.[107] Second, the law's definition of "covered information" is not limited to information

[102] Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584 (2015).

[103] Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011) (citing IMS Health Inc. v. Sorrell, 631 F. Supp. 2d 434, 445-46 (D. Vt. 2009)).

[104] *See* Bhagwat, *supra* note 16, at 863-64 (noting that the prescriber-identifying information in *Sorrell* does not inherently propose a transaction, nor is prescriber-identifying information solely related to economic interests).

[105] *See* Metromedia, Inc. v. City of San Diego, 453 U.S. 490, 512-15 (1981) (distinguishing between billboards that contain commercial speech and billboards that contain noncommercial speech).

[106] *See* BUS. & PROF. § 22584.

[107] *See id.*

that proposes a transaction.[108] These findings form the foundation for the strict scrutiny review presented in Part III.[109]

2. Engaging in Targeted Marketing

SOPIPA imposes a comprehensive ban on targeted marketing. The law prohibits operators from engaging in targeted advertising based upon "*any* information, including covered information . . . that the operator has acquired because of the use of that operator's site."[110] Although the statute does not explicitly define targeted advertising, this practice involves tracking an individual's online activities to deliver customized advertisements.[111] Thus, the statute seeks to prevent operators from communicating targeted advertisements based upon any information generated through the use of their online tool. SOPIPA does provide a narrow exception to this ban in which operators may directly market educational products to parents so long as such marketing is not based on covered information obtained through the use of the operator's service.[112] Nevertheless, since the targeted marketing restriction applies to "any information," operators would presumably be precluded from using information completely unrelated to students, such as technical features of the online tool, for targeted advertising purposes.[113]

Unlike disclosing covered information, engaging in targeted advertising more closely fits under the umbrella of commercial speech because the content and purpose of the speech is to "propose a commercial transaction" to a potential customer.[114] Targeted advertisements for economic *and* non-economic purposes, such as to

[108] *See id.*

[109] *See infra* notes 165–66 and accompanying text.

[110] BUS. & PROF. § 22584 (emphasis added).

[111] *See* Yuen Yi Chung, *Goodbye Pii: Contextual Regulations for Online Behavioral Targeting*, 14 J. HIGH TECH. L. 413, 431-32 (2014) (discussing targeted marketing practices and suggesting legislative approaches to regulate such practices).

[112] It is important to note that this section only applies to one category of customers: parents. Operators are prohibited from directly marketing to students, teachers, and other educational service providers who many find the information useful. Moreover, there is not an option for a person to opt-in to targeted marketing if she so desires. *See* Student Online Personal Information Protection Act, S.B. 1177, 2013–14 Reg. Sess. § (o) (Cal. 2013).

[113] BUS. & PROF. § 22584.

[114] *See* United States v. United Foods, Inc., 533 U.S. 405, 409 (2001) (defining "commercial speech").

educate the consumer, would still be considered commercial speech under Supreme Court precedent.[115]

3. Using Information to Amass a Profile for a Non-K–12 Purpose

On its face, using information to amass a profile does not appear to be speech under the First Amendment because it is not communicative in nature.[116] Although the First Amendment specifically applies to speech, its protection may extend to expressive conduct with "sufficient communicative elements."[117] To determine if sufficient communicative elements bring expressive conduct within the scope of the First Amendment, courts ask "whether [a]n intent to convey a particularized message was present, and [whether] the likelihood was great that the message would be understood by those who viewed it."[118] For example, the U.S. Supreme Court has recognized that wearing an anti-Vietnam War armband[119] and desecrating the U.S. flag[120] are politically expressive conduct protected by the First Amendment.

The act of using student online information to amass a profile likely fails the expressive conduct inquiry. First, although an operator may amass a profile with the intention of using the profile to convey a particularized message based on the student information *after* the profile is generated,[121] it is unlikely that the operator intends to communicate a message by the actual act of amassing the profile. Amassing a data profile is typically achieved by a computer algorithm.[122] Second, even if an operator intended to convey a

115 *See* Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 475 (1989) (holding that communications can "constitute commercial speech notwithstanding the fact that they contain discussions of important public issues").

116 *See* BUS. & PROF. § 22584.

117 Texas v. Johnson, 491 U.S. 397, 404 (1989).

118 *Id.* (internal quotation marks omitted).

119 *See* Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 505 (1969).

120 *Johnson*, 491 U.S. at 420.

121 *See* John Koetsier, *Data-Driven Digital Marketing Triples Conversion Rates (Study)*, VENTUREBEAT (June 3, 2014, 8:01 AM), http://venturebeat.com/2014/06/03/data-driven-digital-marketing-triples-conversion-rates-study/ (discussing recent trends revealed by an Adobe report on targeted marking practices).

122 Julie Brill, *Demanding Transparency from Data Brokers*, WASH. POST (Aug. 15, 2013) https://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84_story.html (explaining how Acxiom, one of the largest commercial data brokerage firms, obtain information through cookies and processes the data with "sophisticated algorithms").

particular message by amassing a profile, it is unlikely that viewers would understand such a message expressed by a raw data profile.

Some may object to this characterization of amassing a data profile. One could argue that amassing a profile is expressive conduct warranting First Amendment protection because the "practical operation" and purpose of SOPIPA's ban on using information to amass a profile is to restrict advertising.[123] The California Senate Judiciary Committee noted that SOPIPA's restrictions on amassing a profile implicated commercial speech protection under the First Amendment.[124] One could also point to certain circumstances where data profiles themselves are intentionally amassed and made available to communicate a comprehensible message.[125] Nevertheless, the text of SOPIPA restricts the *use* of information obtained by operators for a certain activity, except in furtherance of a K–12 purpose.[126] Since this provision restricts a computer process that is not clearly communicative in nature, it falls outside of the First Amendment inquiry of this Note.

C. SOPIPA Imposes a Speaker-Based Restriction on Speech

SOPIPA only restricts the speech of certain online educational sites and service providers: operators of online and cloud-based applications primarily designed for K–12 purposes.[127] The law does *not* apply to websites primarily designed for a *non*-K–12 purpose or to brick-and-mortar entities *directly* receiving covered information through non-online means.[128] For example, a gaming website open to the general public could legally ask users for a first and last name, email address, age, and year in school to develop a profile in which a customized game is generated for the user. SOPIPA would not apply to

---

[123] Sorrell v. IMS Health, Inc., 131 S. Ct. 2653, 2663 (2011); R.A.V. v. St. Paul, 505 U.S. 377, 391 (1992) (emphasizing the importance of considering the "practical operation" of a law in First Amendment analysis); Brill, *supra* note 122.

[124] *See Privacy: Students: Hearing Before the S. Judiciary Comm.*, 2013–14 Reg. Sess. 4-5 (Cal. 2014).

[125] *See* Natasha Singer, *A Data Broker Offers a Peek Behind the Curtain*, N.Y. TIMES (Aug. 31, 2013), http://www.nytimes.com/2013/09/01/business/a-data-broker-offers-a-peek-behind-the-curtain.html (discussing Acxiom's free website that lets consumers view some of the information the company has collected about them).

[126] Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584 (2015).

[127] *Id.*

[128] An example of a brick-and-mortar entity with such access could be a parent collecting student contact information from students or parents to host a private event.

the gaming website, which could lawfully obtain, use, disclose, or sell "covered information" and K–12 "student information," assuming the website operator complied with COPPA and other applicable laws.[129] Nevertheless, limiting the scope of the law to operators is likely reasonable because studies show that operators are the most likely entities to have access to *online* student data, which is at issue here.[130]

III. SOPIPA'S DISCLOSURE AND SALE RESTRICTIONS: STRICT SCRUTINY ANALYSIS

Based on the conclusion that SOPIPA's disclosure and sale restrictions are content-based restrictions on noncommercial speech, these two provisions must survive strict scrutiny to stand.[131] Strict scrutiny requires California to show that the content-based restrictions on covered information (1) advance a compelling governmental interest and (2) that they are narrowly tailored to achieve that interest.[132]

A. Does the California Legislature Advance a Compelling Governmental Interest?

The legislative history and text of SOPIPA indicate that the purpose of the law is to protect student privacy by limiting the use of personal information obtained through privately operated online commercial educational tools.[133] The law's author, Senator Darrell Steinberg, stated in multiple committee hearings that SOPIPA is designed to prohibit the commercial use of student PII; specifically, advertising.[134] The State cited the growing use of technology in classrooms and recent Privacy Technical Assistance Center ("PTAC")[135] guidance as evidence

[129] *See Complying with COPPA: Frequently Asked Questions*, *supra* note 55.

[130] *See* REIDENBERG ET AL., *supra* note 2, at 18-19.

[131] *See supra* Part II; *supra* notes 18–21 and accompanying text.

[132] *See supra* note 21 and accompanying text.

[133] *Student Online Personal Information Protection Act: Hearing on S.B. 1177 Before S. Comm. on Educ.*, *supra* note 63; ASSEMB. FLOOR ANALYSIS OF S. THIRD READING, S.B. 1177 (as amended Aug. 21, 2014), 2013–14 Reg. Sess., at 5-6 (Cal. 2014).

[134] *Student Online Personal Information Protection Act: Hearing on S.B. 1177 Before S. Comm. on Educ.*, *supra* note 63 (quoting Sen. Darrell Steinberg: "SOPIPA would prohibit the commercial use of student personal information for any secondary purposes including advertising").

[135] The PTAC is an online resource operated by the U.S. Department of Education designed to educate the public about "data privacy, confidentiality, and security practices" related to education by providing information and guidance materials. *About PTAC*, U.S. DEP'T OF EDUC. (2015), http://ptac.ed.gov/About.

that operators using student data for commercial purposes is a problem.[136]

A court may find that the interest in ensuring student informational privacy is compelling on a number of grounds. First, the California Constitution grants citizens the inalienable right to privacy.[137] Second, a court may conclude that lawmakers deliberately designed the scope of SOPIPA to close loopholes in existing federal student privacy laws.[138] On the other hand, a court may be suspicious of SOPIPA's legislative history. In *Sorrell*, the Court acknowledged that as technology develops, informational privacy presents many concerns.[139] Nevertheless, the Court clearly stated that "[i]n considering how to protect those [privacy] interests . . . the State cannot engage in content-based discrimination to advance its own side of a debate."[140] SOPIPA's legislative history indicates that California lawmakers believed a content-based law regulating online student data obtained by operators could mitigate the harms posed by the "potential commercial value" of student's online PII.[141]

Although the legislative history suggests that lawmakers have a negative view of the commercial use of student data, it does not appear that the State is only advancing one side of the debate under the guise of legislation. FERPA, an entire regulatory scheme designed to protect student information, is a testament to the legitimacy of protecting students' personal educational information.[142] Furthermore, the 114th

---

[136] *Student Online Personal Information Protection Act: Hearing on S.B. 1177 Before S. Comm. on Educ.*, *supra* note 63; S. COMM. ON EDUC., ANALYSIS OF S.B. 1177, 2013–14 Reg. Sess., at 5 (Cal. 2014).

[137] CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

[138] *See* N.J. Dep't of Labor & Workforce Dev. v. Crest Ultrasonics, 82 A.3d 258, 269-70 (N.J. Super. Ct. App. Div. 2014) (concluding that the asserted governmental interest is substantial "based upon a fair conception of the deliberately circumscribed nature of the law's scope"); *see also supra* note 50 and accompanying text (discussing SOPIPA's legislative history).

[139] Sorrell v. IMS Health Inc., 131 S.Ct. 2653, 2672 (2011) ("The capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure.").

[140] *Id.* at 2672; *see also* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978).

[141] *See* ASSEMB. FLOOR ANALYSIS OF S. THIRD READING, S.B. 1177 (as amended Aug. 21, 2014), 2013–14 Reg. Sess., at 5 (Cal. 2014).

[142] *See generally* Paul Schwartz & Daniel Solove, *The Battle for Leadership in Education Privacy Law: Will California Seize the Throne?*, SAFEGOV.ORG (Mar. 27, 2014), http://safegov.org/2014/3/27/the-battle-for-leadership-in-education-privacy-law-will-

Congress is currently considering the bipartisan Student Digital Privacy and Parental Rights Act of 2015, introduced by Representatives Luke Messer (R-Ind.) and Jared Polis (D-Colo.) in April 2015.[143] Dozens of technology leaders, education organizations, and privacy advocates support this bill.[144] Student data deserves special protection because minors are often required to volunteer personal information to operators' tools to participate in class activities or complete homework.[145] The overwhelming public support for more rigorous student data privacy laws suggests that the California legislature was acting on public mandate, not its own agenda.[146] In addition to this public and congressional support, leading educational technology companies and advocacy organizations have signed a pledge not to sell, engage in targeted advertising, or use students' personal data for unauthorized purposes.[147] Moreover, one study found that 89% of registered voters polled were "very" or "somewhat" worried about companies using students' personal data to market directly to them.[148] In weighing these arguments and the legislative history, it is most likely that a strong compelling interest, and not merely a ploy for viewpoint discrimination, supports SOPIPA.[149]

california-seize-the-throne (discussing the need for states to step in and protect student information in the digital age because "FERPA is not getting the job done").

143 *See* Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (1st Sess. 2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/2092/text.

144 Press Release, Luke Messer, Rep. Ind., Messer, Polis Introduce Landmark Bill to Protect Student Data Privacy (Apr. 29, 2015), *available at* https://messer.house.gov/media-center/press-releases/messer-polis-introduce-landmark-bill-to-protect-student-data-privacy.

145 *See* Mutkoski, *supra* note 4, at 528-29.

146 *See* Brown v. Entm't Merch. Ass'n, 131 S. Ct. 2729, 2740 (2011) (discussing public parental support for restrictions on the sale of videogames to minors).

147 Charley Locke, *Edtech Companies Pledge to Protect Student Data Privacy*, EDSURGE (Oct. 7, 2014), https://www.edsurge.com/n/2014-10-07-edtech-companies-pledge-to-protect-student-data-privacy (discussing the pledge and naming Microsoft and Houghton Mifflin Harcourt among the signatories).

148 Joy Resmovits, *Immense Unease over Advertisers Nabbing Student Data: Poll*, HUFFINGTON POST (Jan. 22, 2014), http://www.huffingtonpost.com/2014/01/22/student-data-privacy-poll_n_4640688.html (discussing public concern about targeted marketing based on student PII).

149 *See Entm't Merch.*, 131 S. Ct. at 2740; *cf.* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2670-73 (2011) (explaining that the Vermont law's legislative history and poor drafting indicated that it was merely a tool to suppress speech disfavored by the legislature).

B. Is SOPIPA Narrowly Tailored to Achieve the Asserted Governmental Interest?

There is a strong argument that SOPIPA is not narrowly tailored to achieve the government's interest in greater student PII protection because the law is over-inclusive and there are less-restrictive alternatives.[150] First, SOPIPA's ban on disclosing covered information is over-inclusive because its restrictions go far beyond student data.[151] Each restriction imposed on operators applies to a different category of information.[152] Operators cannot engage in targeted marketing with *any* information the operator has obtained because of anyone's use of the operators site, service, or application.[153] The sale restriction applies to all "student information," which includes PII, but also presumably includes de-identified information. The restriction on amassing a profile for a non-K–12 purpose applies to "information."[154] Thus, of the law's four key restrictions, only the ban on disclosure exclusively applies to PII.[155] This over-inclusive regulation of students' non-PII is entirely outside of the stated purpose of SOPIPA and is broadly, rather than narrowly, construed to achieve greater informational privacy for students.[156]

A significant counterargument to this position is that SOPIPA is not excessive but rather a "coherent policy" that meets Justice Kennedy's preferred policy design.[157] SOPIPA is arguably more coherent than Vermont's Prescription Confidentiality Law for two reasons. First, SOPIPA prohibits all operators of K–12 educational online sites, services, and applications from disclosing, selling, using, and engaging in targeted marketing with covered information, not just one party within the sector.[158] Second, SOPIPA's restrictions apply in all but a

---

150 *See Entm't Merch.*, 131 S. Ct. at 2740-42 (striking down a California law banning the sale of and imposition of label restrictions on violent videogames sold to minors under strict scrutiny for being under- and over-inclusive).

151 Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584 (2015).

152 *Id.*

153 *Id.* (emphasis added).

154 *Id.*

155 *Id.*

156 *Id.*; *see* Brown v. Entm't Merch. Ass'n, 131 S. Ct. 2729, 2740-42 (2011).

157 Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2668 (2011); *see also* Gooch et al., *supra* note 48, at 259 ("[T]he majority suggested that Vermont could have constructed 'a more coherent policy,' similar to the HIPAA Privacy Rule. The Court was likely implying that more than one party (detailers) should be excluded from using prescriber-identifying information.").

158 BUS. & PROF. § 22584.

few narrow exceptions.[159] The problem here is that the exceptions themselves are not narrowly drawn. For example, SOPIPA restricts the sale of "student information," which may include de-identified noncommercial speech, but provides that an operator may *use* de-identified student covered information to improve and to market their educational products.[160] Operators may also *share* de-identified covered information to develop and improve educational sites, services, and applications.[161] Neither of these exceptions specifically permit the sale of student information — de-identified or otherwise — for any purpose.[162] In a context such as this, where technical terminology is critical, a court may find that SOPIPA's over-inclusive restrictions and inconsistent terminology are not narrowly drawn to protect students' PII from commercial harms.[163] Part V presents solutions lawmakers may consider to achieve greater student data privacy without running afoul of the First Amendment.[164]

IV. SOPIPA'S BAN ON TARGETED MARKETING: *CENTRAL HUDSON* ANALYSIS

SOPIPA prohibits commercial speech by foreclosing operators' ability to engage in targeted marketing on any site with *any* information collected through the use of their K–12 online site, service, or application.[165] Such a ban on commercial speech triggers the four-pronged *Central Hudson* test: (1) the burdened commercial speech must not be illegal or misleading; (2) the governmental interest the law seeks to achieve must be substantial; (3) the law must directly advance the asserted interest; (4) the law must not be more extensive than necessary to achieve the governmental interest.[166]

SOPIPA satisfies the first two prongs of *Central Hudson*. First, assuming the operator complied with the applicable laws (such as

159 *See id.*; Gooch et al., *supra* note 48, at 259; Kristina L. Miller, *Shrinking Drug Costs Without Silencing Pharmaceutical Detailers: Maryland's Options After* Sorrell v. IMS Health, 16 J. HEALTH CARE L. & POL'Y 215, 232 (2013).

160 BUS. & PROF. § 22584.

161 *Id.*

162 *Id.*

163 *See Privacy: Students: Hearing Before the S. Judiciary Comm.*, *supra* note 124.

164 *See* Gooch et al., *supra* note 48, at 259 ("Any state that implements a prescription confidentiality law based on those suggestions would still be taking a risk when other, less-objectionable approaches might be equally effective.").

165 BUS. & PROF. § 22584.

166 Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980).

COPPA), generally engaging in targeted marketing with informational data is legal.[167] Second, as discussed in Part III.A, SOPIPA's text and legislative history support the conclusion that the government's asserted interest is to protect students' online PII.[168] A court is likely to find that California's constitutional commitment to individual privacy and the risks posed to students by the commercial exploitation of their PII[169] render this privacy interest substantial.[170]

SOPIPA also meets the third prong of *Central Hudson*. A court is likely to find that SOPIPA directly advances student data privacy because the law brings third parties with access to data that would otherwise be protected under federal law within the realm of state protection.[171] The Judiciary Committee further stated that SOPIPA would withstand such scrutiny because "children are vulnerable to advertisements they may be exposed to as a result of required education."[172] In effect, SOPIPA will require operators of K–12 websites, services, and applications, who do not contract, or have no contact whatsoever, with schools, to refrain from disclosing, using, selling, or engaging in targeted marketing with covered information.[173] The law also imposes additional duties on operators to provide adequate safeguards for student data.[174] Legal scholars are already encouraging operators to proactively ensure that their security and usage practices comply with SOPIPA.[175]

---

[167] *See supra* notes 62–71 and accompanying text.

[168] *Student Online Personal Information Protection Act: Hearing on S.B. 1177 Before S. Comm. on Educ.*, *supra* note 63; ASSEMB. FLOOR ANALYSIS OF S. THIRD READING, S.B. 1177 (as amended Aug. 21, 2014), 2013–14 Reg. Sess., at 5-6 (Cal. 2014).

[169] *See Advertising to Children and Teens: Current Practices*, COMMON SENSE (Spring 2004), https://www.commonsensemedia.org/research/advertising-to-children-and-teens-current-practices (observing that online advertising directed at children often blurs the line between marketing and entertainment, making it difficult to quantify its effects); Boyd, *supra* note 58 (identifying four different external threats to students whose data is unprotected).

[170] *See supra* notes 137–41 and accompanying text.

[171] *See supra* notes 51–63 and accompanying text.

[172] *Privacy: Students: Hearing Before the S. Judiciary Comm.*, *supra* note 124.

[173] Michelle J. Anderson & Jim Halpert, *New Student Data Privacy Laws: Top Points for School Contractors and K–12 Education Sites, Apps and Online Services*, DLA PIPER (Jan. 6, 2015), https://www.dlapiper.com/en/us/insights/publications/2015/01/new-student-data-privacy-laws/ (noting that the SOPIPA is "directly applicable to vendors whether or not the contract warns them of the new requirements").

[174] Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584 (2015).

[175] *See* Anderson & Halpert, *supra* note 173 (suggesting that operators take the following steps immediately to ensure SOPIPA compliance: talk to business and marketing teams, align protocols to state-specific requirements, and inventory and

Although considering the "least-restrictive-means" is not necessary when restricting commercial speech, a court may conclude that SOPIPA's ban on targeted marketing fails the fourth prong of *Central Hudson*.[176] The line of cases applying the *Central Hudson* test illustrates the Court's increasingly anti-paternalistic commercial speech jurisprudence.[177] *Rubin v. Coors Brewing Co.*[178] and *44 Liquormart, Inc. v. Rhode Island*[179] are two examples of this evolution.[180] In *Rubin*, the Court assessed whether a federal ban on displaying alcohol content information in advertising fit "with other provisions of the government's regulatory scheme."[181] In *44 Liquormart*, the Court emphasized that a liquor price advertising ban violated the First Amendment because it failed *Central Hudson*'s third and fourth prongs by achieving the state's goal in an impermissibly indirect and excessive way.[182] The policy analysis in *Sorrell* represents the Court's willingness to reject commercial speech restrictions on the basis of potentially feasible alternatives.[183]

SOPIPA's targeted marketing ban is arguably more extensive than necessary. The law forbids operators from using targeted advertising when such advertising includes *any* information obtained through use of the tool for a K–12 purpose.[184] Thus, in reality, operators are banned from utilizing any and all data generated by students, educational agency employees, or parents who use the operator's service. The two advertising exceptions are: (1) using de-identified information for marketing, and (2) directly advertising to parents

update existing agreements with educational institutions).

176 *See* Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 477 (1989) ("[W]e have specifically held [the *Central Hudson* test] does *not* require least restrictive means.").

177 *See* Stern & Stern, *supra* note 14, at 1179; *see, e.g.*, 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 502 (1996) (prohibiting advertisement of liquor prices violated the liquor stores' First Amendment right to free speech); City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 426 (1993) (noting that "commercial speech can be subject to greater governmental regulation than non-commercial").

178 Rubin v. Coors Brewing Co., 514 U.S. 476 (1995).

179 *44 Liquormart*, 517 U.S. at 484.

180 *See* Wolf, *supra* note 48, at 1305-06.

181 *Rubin*, 514 U.S. at 488-89 (1995) (noting that inconsistencies in the Federal Alcohol Administration Act and other alcohol regulations undermine challenged provision's efforts to prevent "strength wars"); *see* Stern & Stern, *supra* note 14, at 1181.

182 *See 44 Liquormart*, 517 U.S. at 502 (prohibiting advertisement of liquor prices violated the liquor stores' First Amendment right to free speech).

183 *See* Stern & Stern, *supra* note 14, at 1187.

184 Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584 (2015).

based on non-covered information.[185] The first exception may be impracticable because the law differentiates between using, disclosing, and selling information.[186] This may mean that an operator's ability to use the information does not authorize the operator to disclose or sell it for marketing purposes. Disclosing and selling de-identified information is often necessary to contract with a third party to carry out a marketing campaign.[187] However, the second exception appears to strike an appropriate balance between barring the use of PII for targeted marketing and still permitting some advertising to relevant non-student consumers. This second parental exception may save the law from failing the fourth prong of *Central Hudson* because it provides a narrow exception for advertising to a certain class of adults.[188]

V. PROPOSED SOLUTIONS

SOPIPA's constitutional obstacles jeopardize the privacy of student data. To better protect this data of considerable importance and vulnerability, lawmakers may consider various alternatives.

A. Limit SOPIPA to "Covered Information"

The over-inclusive nature and odd effects of SOPIPA are primarily rooted in the law's inconsistent and imprecise treatment of types of student data. Of the law's four key restrictions, the ban on disclosure is the only restriction that exclusively applies to covered information.[189] By restricting targeted marketing of "any information" and restricting the sale of "student information" and the use of "information," SOPIPA confuses the entire objective of the law: protecting the *personal* information of students.[190] If the law simply

185 *Id.*

186 *Id.*

187 *See* Koetsier, *supra* note 121.

188 *See* Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 564 (2001) (striking down a Massachusetts statute prohibiting tobacco advertising within 1,000 feet of a school because "the sale and use of tobacco products by adults is a legal activity . . . [and] tobacco retailers and manufacturers have an interest in conveying truthful information about their products to adults"); Educ. Media Co. v. Insley, 731 F.3d 291, 301 (4th Cir. 2013) (ruling that an alcohol labeling ban failed the fourth *Central Hudson* prong "because it prohibits large numbers of adults who are 21 years of age or older from receiving truthful information about a product that they are legally allowed to consume").

189 BUS. & PROF. § 22584.

190 *Id.*

restricted using, selling, disclosing, and engaging in targeted marketing with students' personally identifiably information, it would look much more like a coherent, narrowly drawn law capable of withstanding both the *Central Hudson* test and strict scrutiny.[191]

B. Restrict the Dissemination of Student Data Through Statutory Contractual Requirements

The Supreme Court has expressed a preference toward achieving policy objectives through methods that do not inhibit speech.[192] In *Sorrell*, the Court thoroughly analyzed policy alternatives Vermont could have pursued to achieve its interests without substantially burdening speech.[193] In California, one such alternative law is California Education Code Section 49073.1 ("Digital Pupil Records Law"), passed on the same day as SOPIPA and currently in effect.[194] The Digital Pupil Records Law regulates contracts between educational agencies and third parties to store, manage, and retrieve digital pupil records, and/or to provide educational software.[195]

The Digital Pupil Records Law fits within the school-centric framework of FERPA and provides guidance to schools working with operators that have access to student information.[196] The Digital Pupil Records Law's definition of "pupil records" mirrors FERPA's "education records" term and responds to the technological changes in student information. The law defines "public records" to include: (1) information directly related to a student and maintained by the local educational agency, and (2) information directly obtained from a student through software or online applications that the student was directed to use by a teacher or local educational agency employee.[197] The law also states that "pupil records" excludes de-identified information used by a third party to improve the tool, to customize learning, or for marketing.[198]

The Digital Pupil Records Law resolves ambiguities in the status of student data and requires schools to contractually establish safeguards

---

191 *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2668 (2011); Gooch et al., *supra* note 48, at 259.

192 *Sorrell*, 131 S. Ct. at 2668-70.

193 *Id.*

194 CAL. EDUC. CODE § 49073.1 (2015).

195 *Id.*

196 *Id.*

197 *Id.*

198 *Id.*

for online student data.[199] It requires contracts with third parties involved with digital pupil record management to include "a statement that pupil records continue to be the property of and under the control of the local educational agency."[200] All contracts must also expressly prohibit third parties from using PII in pupil records for targeted advertising.[201] Encouraging formal contracts with educational online service providers supports a paradigm shift in which operators will have an economic incentive to work with schools through contracts instead of under the radar.[202] Categorizing student PII as "pupil records" strikes a balance between restricting commercial speech based on formal educational matters and just any technical data collected by a K–12 site.[203]

One objection to using the Digital Pupil Records Law as an alternative to SOPIPA is that operators who are not under contract with local educational agencies are able to obtain and use student data.[204] Even though sites not under contract are outside the scope of the Digital Pupil Records Law, the law could be amended to include quasi-contracts in which teachers agree to the terms of an online K–12 service before using it in their classroom, which is discussed further in the following section.

C. Require Operators to Obtain Stakeholders' Prior Informed Consent

If lawmakers designed SOPIPA as an opt-in or opt-out informed consent law, it may burden less speech and have a better chance at surviving First Amendment scrutiny.[205] Courts and scholars have proposed such a model to facilitate thoughtful free speech and still

---

199 *Id.*

200 *Id.*

201 *Id.*

202 Under AB 1584, operators are only prohibited from using student PII in targeted marketing, not *any* and *all* data generated by their sites. *Id.*

203 *Id.*

204 Jim Steyer, *Bill Would Safeguard Students' Data from Cloud-Computing Providers*, COMMON SENSE (Sept. 3, 2014), https://www.commonsensemedia.org/blog/bill-would-safeguard-students-data-from-cloud-computing-providers (noting that AB 1584 applies "when schools contract with outside companies for digital educational software and record management services").

205 *See* Gooch et al., *supra* note 48, at 259 ("[T]he Court suggested that if Vermont changed its prescription confidentiality law from an opt-in to an opt-out structure like Maine's law, then the proposed law 'might burden less speech' but 'would not necessarily save' the statute. Third, the Court advised that physicians should simply close their doors to drug reps — a private-sector solution to the problem not subject to the First Amendment.").

protect personal privacy.[206] The Court has upheld similarly designed laws. For example, in *Milavetz, Gallop & Milavetz, P.A. v. United States*, the Court upheld a requirement that attorneys providing bankruptcy-assistance services include a statement in their advertisements alerting consumers that they specialize in debt relief and bankruptcy.[207] The Court found that these warning statements directly advanced the state's interest in informing consumers without being excessively paternalistic because the warnings were not an "affirmative limitation" on protected speech.[208]

Instead of attempting to control speech with student data, this informed consent alternative will have the positive outcome of educating students, teachers, and parents about online privacy before exchanging online tools for their personal data.[209] Hypothetically, this solution could require operators to inform users of the online educational tool about the purpose of data collection, commercial uses, and the user's responsibility to make a choice about how they use the site based on this information.

CONCLUSION

Although the law surrounding data privacy and the First Amendment is still unsettled, examining current trends is helpful to foreshadow potential legal developments.[210] By examining SOPIPA through the lens of a recent U.S. Supreme Court data privacy ruling, the potential magnitude of *Sorrell* becomes even clearer. *Sorrell* suggests that the disclosure and sale of student online information is fully protected speech requiring strict scrutiny.[211] The case also supports applying the *Central Hudson* test to SOPIPA's restriction on

---

[206] *See generally* Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 437 (2013) (discussing "3-E Approach" focusing on education, empowerment, and targeted enforcement as a possible model).

[207] Milavetz, Gallop & Milavetz, P.A. v. United States, 559 U.S. 229, 252-53 (2010).

[208] *Id.* at 249.

[209] *See* Thierer, *supra* note 206, at 437 ("In recent years, many child safety scholars and child development experts have worked to expand traditional online education and media literacy strategies to place the notion of 'digital citizenship' at the core of their lessons.").

[210] *See generally* Michael Heise, *The Past, Present, and Future of Empirical Legal Scholarship: Judicial Decision Making and the New Empiricism*, 2002 U. ILL. L. REV. 819 (discussing trends and influences of legal scholarship).

[211] *See supra* Part II.

targeted marketing and potentially amassing a profile.[212] A careful look at SOPIPA demonstrates that even a seemingly "coherent policy" designed to protect PII privacy presents significant threats to First Amendment protections.[213] A court reviewing a challenge to SOPIPA may conclude that it fails both strict scrutiny and the *Central Hudson* test because the law is over-inclusive and there are less-restrictive alternatives.[214] This analysis may be useful to judges faced with selecting and applying the appropriate level of scrutiny for similar data privacy laws circulating on a national and state level.[215]

[212] *See supra* Part II.

[213] *See supra* Parts III.

[214] *See supra* Parts III–IV.

[215] *See supra* notes 89–91 and accompanying text.