Commercial Free Speech Constraints on Data Privacy Statutes After *Sorrell v. IMS Health*

BASTIAN SHAH*

Collection and use of big data drive the modern information economy. While big data can produce valuable innovations, it also comes with perils for consumers. In particular, consumers have little ability to protect their privacy online and are unnerved by the hyper-targeted advertising to which they are subjected. In response to these concerns, American states have begun enacting general data privacy laws similar to those passed in Europe. At the same time, the United States Supreme Court has grown wary of laws attempting to restrict companies from distributing and using data for advertising purposes. For instance, in Sorrell v. IMS Health*, the Court found that a Vermont statute aimed at preventing targeted advertising by pharmaceutical manufacturers violated the commercial free speech doctrine. Since* Sorrell*, the constitutionality of data privacy statutes has been ambiguous.*

This Note argues that data privacy laws that empower consumers to meaningfully protect their privacy by opting out of unwanted data collection do not violate the commercial free speech doctrine. Part II defines data privacy and summarizes the objectives current data privacy laws seek to achieve. Part III analyzes commercial speech jurisprudence before and after Sorrell *and discusses the effect of* Sorrell *on commercial free speech jurisprudence and data privacy law. Part IV argues that government interest in empowering consumers by giving them meaningful choices in their online privacy is important enough to survive scrutiny under the post-*Sorrell *commercial free speech paradigm.*

---

* Design & Layout Editor, Colum. J.L. & Soc. Probs., 2020–2021, J.D. Candidate 2021, Columbia Law School. The author would like to thank Professor Philip Hamburger for his thoughtful guidance and for inspiring the central argument of this Note. The author is also grateful to the staff of the *Columbia Journal of Law and Social Problems* for their feedback and fellowship throughout the editorial process.

I. INTRODUCTION

Data privacy statutes are a response to the information age economy. Companies that collect and sell data have experienced rapid growth as the breadth of data they can gather on consumers has expanded. From this data, companies can — with striking accuracy — infer intimate details about consumers.[1] These insights are then sold to advertisers who use them to target advertisements to consumers. Online platforms such as Twitter, Google, and Amazon are ubiquitous; fundamental to modern economic and social life; and collect data on everything their customers do.[2] Data privacy statutes seek to regulate this new relationship between businesses and consumers.[3]

State data privacy statutes, in attempting to respond to citizens' legitimate concerns, risk running afoul of the Supreme Court's expanding interpretation of the First Amendment. In particular, data privacy advocates fear the *Sorrell v. IMS Health* decision "might mean the end of [data] privacy law."[4] This Note argues that, while *Sorrell* does invalidate a wide swath of data privacy laws, some regulation is still possible.

Part II of this Note defines data privacy and sets out three broad objectives for data privacy statutes. Data privacy is a distinct legal concept from traditional, or "pure," privacy, making analogies between the two incongruous at times.[5] While privacy law primarily protects a person's right not to disclose private information, data privacy law regulates how recipients of already disclosed private information may utilize it. Data privacy statutes regulate the utilization of private information to further three objectives: 1) limiting targeted advertising, 2) protecting consumers' private data from loss due to data breaches, and 3) empowering

1. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/RN46-MDT3].

2. *See, e.g.*, TERMS OF SERVICE; DIDN'T READ, https://tosdr.org [https://perma.cc/3M3K-WXXT] (last visited May 27, 2020). Terms of Service; Didn't Read is a website that summarizes the Terms of Service of online platforms and rates their "fairness." It has tracked the data collection policies of over 400 online platforms, including Facebook, Apple, Google, Walmart, Twitter, Amazon, and Reddit.

3. *See, e.g.*, California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.100–1798.199 (Deering 2019); Security and Privacy of Personal Information, NEV. REV. STAT. §§ 603A.010–.290 (2019).

4. Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1521–22 (2015) (citation omitted).

5. 1 DATA PRIVACY, PROTECTION, AND SECURITY LAW § 1.02[1] (2019).

consumers to make meaningful choices about who can and cannot collect and sell their data online.

Part III explains how the *Sorrell* case, and commercial free speech doctrine broadly, affects data privacy statutes. Part III.A summarizes the history of the commercial free speech doctrine, culminating in a discussion of the intermediate scrutiny test announced in *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n.*[6] Part III.B considers the facts, arguments, and holding in *Sorrell*. Part III.C then argues that the *Sorrell* Court calls for a stricter standard of review for some commercial speech regulations above what *Central Hudson* required. Part III.D describes the *Sorrell* Court's argument that "information is speech"[7] and explains how this affects data privacy laws regulating data collectors and data brokers.

Part IV presents a blueprint for how states can draft constitutional data privacy statutes. Here, the Note returns to the three objectives laid out in Part II. Part IV.A argues that data privacy laws seeking to inhibit the practice of targeted advertising are forbidden by *Sorrell*. Part IV.B explores the ambiguities of whether a cybersecurity justification for data privacy laws comports with the commercial speech doctrine. Finally, Part IV.C argues that data privacy statutes seeking to empower consumers by giving them the right to opt out of data collections comport with post-*Sorrell* commercial free speech doctrine. This Note then concludes that states would be wise to adopt the consumer-centric, opt-out approach to data privacy.

II. DATA PRIVACY LAW AND ITS OBJECTIVES

Traditionally, "privacy" is the ability to keep information secret from the rest of the world.[8] In a "pure" privacy interest matter, it is the responsibility of the individual to keep private information secret, and privacy law exists to protect a person's right not to

6. Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557 (1980).

7. Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011).

8. *See* Ostergren v. Cuccinelli, 615 F.3d 263, 282 (4th Cir. 2010) ("'[P]rivate' matters are those one would prefer to keep hidden from other people because disclosure would be embarrassing or compromising.") (citation omitted).

disclose private information.[9] If the holder of the right discloses the private information, then the right to privacy is lost.[10]

Data privacy, as opposed to "pure" privacy, is premised on an individual's interest in controlling the use of certain types of information even after the information has been lawfully disclosed to some other party.[11] A simple example is a Social Security Number (SSN). Americans routinely disclose their SSNs to employers, creditors, and governments, but would consider their privacy violated if any of those entities publicized this information.[12] Pure privacy interests arise from a concern that disclosure will cause embarrassment or social sanction. Data privacy interests predominantly come from a concern that disclosure of data — such as physical and email addresses, date of birth, payment information, another identifying data — will lead to mismanagement or abuse of the information.[13] Some information can straddle both lines. For example, the unwanted disclosure of medical information can cause embarrassment *and* be abused for unscrupulous purposes. The definitional distinction between privacy and data privacy, though, is that in a data privacy matter the person asserting a privacy interest has already voluntarily disclosed the relevant information to another party.[14]

Data privacy laws place obligations and restrictions on businesses that routinely collect, transfer, and use consumers' data.[15] The federal government has addressed data privacy on an industry-by-industry basis.[16] Congress has passed statutes regulating the use of Americans' data in education,[17] healthcare,[18] financial

9. *Id.*; *see also* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1105 (2002).

10. *See Ostergren*, 615 F.3d at 282 ("[P]ersonal matters that have been publicly disclosed can no longer be considered private.").

11. 1 DATA PRIVACY, PROTECTION, AND SECURITY LAW § 1.02[1] (2019).

12. *Ostergren*, 615 F.3d at 282–83.

13. *See id.* ("But people do not feel embarrassed when asked to provide their SSN; nor do they fear that their reputation will suffer when others find out that number. People worry only about how their SSN will be used — more specifically, about whether some unscrupulous person will steal their identity."); *see also* 1 DATA PRIVACY, PROTECTION, AND SECURITY LAW § 1.02[1] (2019).

14. 1 DATA PRIVACY, PROTECTION, AND SECURITY LAW § 1.02[1] (2019).

15. *See id.* § 2.01[3].

16. *See id.* ("U.S. laws associated with data protection ideas have focused on selected sectors . . . and not on general regulation of the use and collection of information.").

17. *See, e.g.*, Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 484 (1974).

18. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

services,[19] and telecommunication,[20] among other sectors. General data privacy statutes that impose standards and regulations broadly to all, or at least most, businesses that collect and store consumers' data have only been passed outside the United States.[21] To address this regulatory gap, states have begun to enact their own general data privacy statutes, including the California Consumer Privacy Act (CCPA) and Nevada's Security and Privacy of Personal Information law, both enacted in 2019.[22] This Note is primarily concerned with these broad data privacy state statutes.

State data privacy statutes govern the relationship between four actors: consumers, data collectors, data brokers, and advertisers.[23] Consumers generate and transmit data whenever they use mobile phones or "smart" devices,[24] visit a website, query a search engine, or engage on a social media site.[25] Data collectors — often businesses offering goods and services online — collect the data consumers generate, including their name, location, age, phone number, email address, what devices they use, what products they bought, what products they searched for but did not buy, content they posted, content they started to write but did not ultimately post, and browser search history.[26] Data brokers then aggregate

---

19. *See, e.g.*, Bank Secrecy Act, 12 U.S.C. § 1829b (2019); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2019).

20. *See, e.g.*, Telephone Consumer Privacy Act, 47 U.S.C. § 227 (2019).

21. The European Union has a General Data Protection Regulation (GDPR). 2016 O.J. (L 119) 1. Since 2000, Canada similarly has a single law that regulates the collection and handling of electronic data by Canadian businesses. Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.).

22. *See, e.g.*, California Consumer Privacy Act (CCPA), CAL. CIV. CODE §§ 1798.100–1798.199 (Deering 2019); Security and Privacy of Personal Information, NEV. REV. STAT. §§ 603A.010–603A.290 (2019).

23. *See generally*, *2019 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEG. (Jan. 3, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx [https://perma.cc/X48D-HJR9].

24. "Smart devices" are generally "internet-enabled versions of ordinary objects equipped with sensors and digital communications capabilities." Gabriel Bronshteyn, *Searching the Smart Home*, 72 STAN. L. REV. 455, 459 (2020). These include cellphones and artificially intelligent assistants, like Amazon's Alexa or Apple's Siri, as well as locks, doorbells, vacuums, kitchen appliances, and televisions. *Id.* at 461–62, 464.

25. *See* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#5bbac53160ba [https://perma.cc/SWV8-KRVP].

26. *See* Duhigg, *supra* note 1; Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html [https://perma.cc/Y3YZ-CABL]; Lois Becket, *Everything We Know About What Data Brokers Know About You*,

the data of numerous collectors and combine that data with public information to produce a strikingly detailed picture of an individual consumer. A data broker can often learn or accurately predict an individual consumer's income, occupation, job history, race, marital status, political leanings, and health conditions.[27] Data brokers then sell this data to advertisers who use the data to target the consumers most likely to be interested in their product.[28] Social media sites, mobile applications, and search engines also use the data they collect or purchase from data brokers to make their services more engaging.[29]

There are many reasons that states seek to regulate the relationship between these four actors. This Note considers three of these reasons. First, state data privacy statutes can limit the most invasive and undesirable practices in online media and targeted advertising. Second, data privacy statutes can proactively mitigate the risks to consumers from data breaches and cybersecurity incidents, rather than merely respond after the fact. Third, data privacy laws can provide consumers with the ability to make meaningful choices about their online privacy.

The first objective of state data privacy statutes is to combat harmful uses of consumer data by data collectors and advertisers. In particular, data privacy laws are often responsive to consumers' distaste for platforms they feel surveil them to sell them products or keep them addicted to the platform.[30] An economic system that

---

PROPUBLICA (June 13, 2014), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you [https://perma.cc/9NW8-KXA6].

27. Becket, *supra* note 26.

28. Singer, *supra* note 26.

29. Siva Vaidhyanthan, director of the University of Virginia Center for Media and Citizenship, notes that Facebook and other social media platforms collect vast amounts of data about how their users interact with their services. *See* Henry Farrell, *It's No Accident that Facebook is So Addictive*, WASH. POST (Aug. 6, 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2018/08/06/its-no-accident-that-facebook-is-so-addictive/ [https://perma.cc/2HXH-938H].

30. *See, e.g.*, NEV. STATE ASSEMBLY COMMITTEE ON COMMERCE AND LABOR, 80TH SESS., MINUTES OF THE MEETING 15 (May 3, 2019), https://www.leg.state.nv.us/Session/80th2019/Minutes/Assembly/CL/Final/1089.pdf [https://perma.cc/2SDC-6AHE] (stating SB220, a Nevada data privacy law, was introduced because "constituents . . . expressed concern about the privacy of their personally identifiable information" after receiving "robocalls" and "pop-up ads" for products they had searched for online); *AB-375 Privacy: Personal Information: Businesses: Senate Floor Analyses*, CAL. LEG. INFO. (Jun. 28, 2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375 [https://perma.cc/EDT4-VF7H] ("Consumers' Web browsing, online purchases, and involvement in loyalty programs also create a treasure trove of information on consumers. Advanced technologies and the use of sophisticated algorithms can create eerily effective profiling and targeted marketing. . . . AB375, the California Consumer Privacy Act of 2018, ensures that

aggregates data on a consumer to target product advertisements at them and deliver more engaging online experiences may not seem threatening. But most consumers are unhappy with the practice because "they do not like having their online behavior tracked and analyzed."[31] As a result, some advertisers work to disguise their use of consumer data when targeting advertisements.[32] Social media and mobile applications are not merely made more engaging through analyzing customer data; they are made more addictive.[33] Addictive social media platforms are making consumers less happy, more stressed, and more anxious.[34] A legislature may well decide that more engaging media and more relevant advertisements are not worth the harms to privacy and well-being of which consumers complain.

A second objective of data privacy statutes is the prevention and mitigation of cybersecurity breaches. In the 2010s, nearly four billion records were stolen from companies that collect and sell personal information.[35] Sixty-four percent of Americans have been the victim of a data breach, and very few trust that the government and large businesses are doing enough to prevent the mishandling

---

consumers enjoy choice and transparency in the treatment of their personal information when accessing the Internet.").

31. Kristen Purcell et al., *Search Engine Use Over Time*, PEW RES. CTR. (Mar. 9, 2012), https://www.pewresearch.org/internet/2012/03/09/main-findings-11/ [https://perma.cc/HZ8V-DG7J] (finding that 68% of Internet users "have an unfavorable view of the practice [of targeted advertising]").

32. Target, the brick and mortar retailer, infamously had a program to use customers' data to predict when they were pregnant and provide coupons for products pregnant women tend to purchase. Duhigg, *supra* note 1. Marketing employees at Target quickly learned women were less likely to use the coupons if they felt they had been "spied on." *Id.* To combat adverse reactions, coupons for baby items were interspersed with randomly selected products, making the targeted advertisements less conspicuous. *Id.*

33. *See* Farrell, *supra* note 29 ("Facebook engineers were for many years influenced by a strain of thought . . . that games could generate 'stickiness' among users, giving users just enough positive feedback to want to return to the game but deny users enough pleasure so that they don't get satiated. . . . Facebook played this game better than most. It's perfectly designed, like a fruit machine in a casino, to give us a tiny sliver of pleasure when we use it and introduce a small measure of anxiety when we do not use it.").

34. *See* Markham Heid, *You Asked: Is Social Media Making Me Miserable*, TIME (Aug. 2, 2017), https://time.com/4882372/social-media-facebook-instagram-unhappy/ [https://perma.cc/3A7J-UPUQ].

35. Aaron Holmes, *Hackers Have Become So Sophisticated That Nearly 4 Billion Records Have Been Stolen from People in the Last Decade Alone/1 /2ere Are the 10 Biggest Data Breaches of the 2010s.*, BUS. INSIDER (Nov. 13, 2019), https://www.businessinsider.com/biggest-hacks-2010s-facebook-equifax-adobe-marriott-2019-10 [https://perma.cc/24Z5-CUDR].

and abuse[36] of their personal data.[37] Their skepticism is justified. Even the largest, most sophisticated technology companies and data brokers have mishandled user data, failing to adhere to basic standards of data protection.[38] Even if businesses were uniformly employing best practices, that would not guarantee the security of consumers' sensitive and personally identifying data. Legislation can mitigate consumers' vulnerability by limiting the information that may be collected and limiting the number of businesses that can purchase or use it.

The third possible objective of state data privacy laws is to empower consumers to protect their own privacy. Consumers cannot opt out of the modern information economy.[39] Many occupations require the use of social media. Brick and mortar stores and online retailers alike collect, buy, and sell consumer data.[40] Putting the onus on privacy-conscious consumers to avoid interacting with data-collecting companies is naïve and futile. It would take the average American 250 hours to completely read the "terms and conditions" they are bombarded with on the Internet each year.[41] Even taking on that effort would not preserve consumers' privacy,

---

36. For the purpose of this Note, an owner of consumer data "mishandles" data when they fail to adhere to cybersecurity best practices, rendering the data vulnerable to theft. Data is "abused" when it is used for an illegal purpose — such as identity theft — and when it is unlawfully obtained — such as through cybercrime or a sale in violation of data privacy law. Finally, this Note describes "misuse" as actions by consumer data owners that, although lawful, goes against the consumer's reasonable expectations of how their data would be used and causes the consumer to feel that their privacy has been violated. An example of data misuse would be an online retailer collecting a customer's email address at checkout, ostensibly to send a receipt, but then selling that personal information to email advertisers with which the consumer had no desire to create a relationship when they entered their email. The sale may have been legal — or even authorized by the consumer's assent to voluminous "terms and conditions" — but a consumer may nonetheless feel their private information had been unscrupulously sold.

37. Aaron Smith, *Americans and Cybersecurity*, PEW RES. CENTER (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/ [https://perma.cc/H79L-CE8W].

38. Twitter, the social media platform, advised all 330 million of its users to change their passwords after internal logs were found in which passwords were stored in plain text, rather than an encrypted format. Taylor Hatmaker, *You Should Change Your Twitter Password Right Now*, TECHCRUNCH (May 3, 2018), https://techcrunch.com/2018/05/03/twitter-password-bug/ [https://perma.cc/QA83-7DJB]. Acxiom, the world's largest data broker, does not use the standard HTTPS encryption protocol on its customer-facing website. Singer, *supra* note 26.

39. *See, e.g.*, Farrell, *supra* note 29 ("For Facebook's model to work . . . users can't have real control over their personal information.").

40. *See* Duhigg, *supra* note 1.

41. *See* David Berreby, *Click to Agree with what? No One Reads Terms of Service, Studies Confirm*, GUARDIAN (Mar. 3, 2017), https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print [https://perma.cc/A52B-NWZS].

as social media companies can collect data on people who do not have an account or even visit the site.[42] Data privacy statutes can give back some semblance of control to consumers through universal standards for privacy policies and opt-out provisions.[43]

III. COMMERCIAL FREE SPEECH AND *SORRELL*

Sorrell is the Supreme Court's most recent case on commercial free speech and will play a central role in any constitutional challenges to data privacy statutes.[44] Part III.A provides a brief summary of commercial free speech jurisprudence prior to *Sorrell*. Part III.B explains the facts and the arguments in *Sorrell*. Part III.C lays out the post-*Sorrell* commercial free speech analysis as it will likely be applied to data privacy statutes. Finally, Part III.D argues that *Sorrell*'s holding applies equally to data privacy statutes regulating data collectors and data brokers, not just those regulating advertisers.

A. COMMERCIAL FREE SPEECH BEFORE *SORRELL*

Commercial speech is speech, usually advertising and marketing, that concerns the commercial interests of the speaker and listener.[45] Commercial speech has not always enjoyed First Amendment protection. In 1942, the Court rejected such an application in *Valentine v. Chrestensen*,[46] holding that the First Amendment imposes no restriction "on government as respects purely commercial advertising."[47] The Court began to reverse course in *Bigelow v. Virginia*,[48] a 1975 case in which the Court overturned the conviction of a newspaper editor under a Virginia law prohibiting

42. Kurt Wagner, *This Is How Facebook Collects Data on You Even If You Don't Have an Account*, VOX (Apr. 20, 2018), https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg [https://perma.cc/226P-BWS7].

43. Under the CCPA, a business must disclose to the consumer what types of information the business collects from customers. CAL. CIV. CODE §§ 1798.100 (Deering 2019). Consumers have a right to opt out of the collection and sale of information that can be tied to the customer's identity. *Id.* § 1798.105. Businesses may not discriminate against customers who opt out by providing an inferior service or charging a higher price. *Id.* § 1789.125.

44. Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).

45. *See Commercial Speech*, BLACK'S LAW DICTIONARY (11th ed. 2019).

46. Valentine v. Chrestensen, 316 U.S. 52 (1942).

47. *Id.* at 53–54 (upholding a New York ordinance forbidding the "distribution in the streets of commercial and business advertising matter[ ]").

48. Bigelow v. Virginia, 421 U.S. 809 (1975).

publication of any commercial advertising for abortion services.[49] The editor's paper ran an advertisement purchased by a New York organization offering to place women seeking abortions in accredited medical facilities.[50] In finding the law violated the First Amendment as applied, the Court noted several facts in *Bigelow* that were not present in *Valentine*: the Virginia law inserted itself into the internal affairs of New York,[51] the application of the law against the appellant effectively censored the press,[52] and the speech at issue provided important information about a matter of constitutional importance rather than merely proposing a commercial transaction.[53] Rather than viewing *Bigelow* as an exception to *Valentine*'s general rule, the *Bigelow* court did the opposite, describing the ordinance at issue in *Valentine* as "a reasonable regulation of the manner in which commercial advertising could be distributed."[54] The *Bigelow* Court could have drawn a line between unprotected commercial advertising and fundamental, politically salient speech, but instead drew a line between time, place, and manner restrictions and prohibitions on content — a line that runs through all First Amendment jurisprudence.

The Court expanded commercial free speech doctrine further in *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council*,[55] which held that even advertisements simply soliciting business are afforded some First Amendment protection.[56] The plaintiffs, Virginia pharmacists, challenged a law prohibiting them from advertising the price of prescription drugs.[57] *Virginia State*

---

49. *Id.* at 829.

50. *Id.* at 812.

51. "The Virginia Legislature could not have regulated the advertiser's activity in New York, and obviously could not have proscribed the activity in that State." *Id.* at 822–23. "A State does not acquire power or supervision over the internal affairs of another State merely because the welfare and health of its own citizens may be affected when they travel to that State." *Id.* at 824.

52. "If application of this statute were upheld under these circumstances, Virginia might exert the power sought here over a wide variety of national publications or interstate newspapers. . . ." *Id.* at 828.

53. *Id.* at 820–22.

54. *Id.* at 819.

55. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748 (1976).

56. *Id.* at 761–72 ("It is clear . . . that speech does not lose its First Amendment protection . . . even though it may involve a solicitation to purchase or otherwise pay or contribute money.") (citations omitted).

57. *Id.* at 749–50 ("[A] pharmacist licensed in Virginia is guilty of unprofessional conduct if he '(3) publishes, advertises or promotes, directly or indirectly, in any manner whatsoever, any amount, price, fee, premium, discount, rebate or credit terms . . . for any drugs

Board of Pharmacy squarely put the matter of a state regulating the most paradigmatic of commercial speech — an advertisement stating that a seller will sell a product at a certain price — before the Court. In striking down the law, the Court explained that a "an individual advertisement, though entirely 'commercial,' may be of general public interest" and that consumers have an interest in "the free flow of commercial information."[58] The consumers' interest in knowing how much they may be charged for prescription drugs, according to the Court, is advanced by the First Amendment.[59] Since *Virginia State Board of Pharmacy*, the informational value of commercial speech has been the Court's primary rationale for the commercial free speech doctrine.[60]

In *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, the Court articulated an intermediate scrutiny test for balancing state interests with the informational value of commercial speech.[61] To regulate commercial speech, the government needs to advance a "substantial interest."[62] Furthermore, the regulation "must directly advance the state interest involved."[63] Finally, the regulation must be tailored to not be "more extensive than is necessary" to serve the government's substantial interest.[64] The Court, in subsequent applications of *Central Hudson*, made clear that although commercial speech enjoys substantial constitutional protection, it enjoys less protection than noncommercial expression or political speech.[65] *Sorrell v. IMS Health* blurred this distinction.

---

which many be dispensed only by prescription.'") (quoting VA. CODE ANN. § 54-524.35 (1974)).

58. *Id.* at 763–64.

59. *See id.* at 753–54, 760–61.

60. *See, e.g.*, Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563 (1980) ("The First Amendment's concern for commercial speech is based on the informational function of advertising."); Sorrell v. IMS Health Inc., 564 U.S. 552, 566 (2011) ("A consumer's concern for the free flow of commercial speech often may be far keener than his concern for urgent political dialogue.") (citing Bates v. State Bar of Ariz., 433 U.S. 350, 364 (1997)).

61. *Central Hudson*, 447 U.S at 573 (Blackmun, J., concurring). *Central Hudson* was a challenge to a New York regulation banning public utilities from posting "advertising intended to stimulate the purchase of utility services." *Id.* at 559 (internal quotation marks omitted). Note that the Court exempts advertisements likely to deceive consumers or pertaining to unlawful activity from First Amendment protection. *Id.* at 564. Intermediate scrutiny only applies when the commercial speech at issue "is neither misleading nor related to unlawful activity." *Id.* This Note is not primarily concerned with false advertising.

62. *Id.* at 564.

63. *Id.*

64. *Id.* at 566.

65. Bd. of Trs. of State Univ. of New York v. Fox, 492 U.S. 469, 477 (1989) ("Our jurisprudence has emphasized that 'commercial speech enjoys a limited measure of protection,

B. *SORRELL V. IMS HEALTH*

Part III.B discusses *Sorrell v. IMS Health*. Part III.B.1 presents the facts of the case and summarizes Vermont's arguments in favor of its commercial speech regulation. Part III.B.2 describes the Court's reasoning for striking down the law.

1. *Background*

Sorrell involved a challenge to a Vermont statute regulating the practice of "detailing."[66] Detailing is when a pharmaceutical company sends sales representatives, called "detailers," to a doctor's office to persuade that doctor to prescribe the company's drugs.[67] To better target detailing efforts, pharmaceutical companies purchase prescriber-identifiable information — data that reveals the name of a doctor and what medications they prescribe — from pharmacies.[68] Pharmaceutical companies use the prescriber-identifiable information to "ascertain which doctors are likely to be interested in a particular drug."[69]

Vermont passed the Prescription Confidentiality Law to regulate the use and sale of prescriber-identifying information by pharmacies and detailers.[70] The statute prohibited pharmacies from selling prescriber-identifiable information or allowing it to be used for marketing prescription drugs without the prescriber's consent, and prohibited detailers from using such information.[71] Notably, the law allowed pharmacies to share prescriber-identifying information for purposes other than marketing prescription drugs.[72]

---

commensurate with its subordinate position in the scale of First Amendment values,' and is subject to 'modes of regulation that might be impermissible in the realm of noncommercial expression.'") (quoting Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978f.

66. Sorrell v. IMS Health Inc., 564 U.S. 552, 557–58 (2011).

67. *Id.* at 557–58.

68. *Id.* at 558. Pharmacies receive prescriber-identifying information "as a matter of business routine and federal law." *Id.* The fact that some of the prescriber-identifying information at issue was "generated in compliance with a legal mandate," as opposed to voluntarily transmitted from doctor to pharmacy, was considered by the Court but did not factor into its decision. *Id.* at 567–68.

69. *Id.* at 558.

70. *Id.* at 557 (citing 18 VT. STAT. ANN. § 4631(d) (2019)). Using the categories described in Part II, Vermont pharmacies are "data collectors" as they collect prescriber-identifying information. Detailers are "advertisers" who purchase prescriber-identifying information from pharmacies and use it for marketing purposes.

71. 18 VT. STAT. ANN. § 4631(d) (2019).

72. *Sorrell*, 564 U.S. at 562. The Prescriber Confidentiality Law also contains exceptions to the prohibition on selling prescriber-identifying information. 18 VT. STAT. ANN.

IMS Health and other companies involved in the business of detailing brought a facial challenge to the Prescription Confidentiality Law, arguing that it violated the First and Fourteenth Amendments.[73] Vermont argued that 1) the statute was not a regulation of speech,[74] and 2) even if it was a regulation of speech, it regulated only commercial speech and passed intermediate scrutiny under *Central Hudson*.[75]

Vermont advanced two arguments for why the Prescription Confidentiality Law did not regulate speech.[76] First, Vermont argued that the Prescription Confidentiality Law regulated access to information, not expression.[77] According to Vermont, "governmental denial of access to information" for pharmaceutical marketers and pharmaceutical manufacturers is distinct from denial of speech.[78] Second, Vermont argued that the marketing prohibition was a "mere commercial regulation" that imposed only "incidental burdens on speech."[79] Regulations of commercial conduct that, as a byproduct, limit commercial speech are beyond the scope of the First Amendment.[80] For instance, employment laws banning race discrimination may burden an employer's speech by prohibiting them from posting a sign reading "White Applicants Only," but this burden is merely incidental to the ban on discriminatory commercial conduct.[81] Because anti-discrimination laws are "directed at

---

§ 4631(e)(1). Sale of prescriber-identifying information is allowed for purposes such as: "pharmacy reimbursement; prescription drug formulary compliance; patient care management; utilization review by a health care professional, the patient's health insurer, or the agent of either; or health care research." *Id.*

73. Complaint ¶ 1, IMS Health Inc. v. Sorrell, 631 F. Supp. 2d 434 (2009), Nos. 07-cv-188-jgm, 07-cv-220, 2008 U.S. Dist. Ct. Pleadings LEXIS 532, at *2.

74. *See Sorrell*, 564 U.S. at 566–67.

75. *See id.* at 571.

76. *See id.* at 566–67.

77. *Id.* at 567.

78. *Sorrell*, 564 U.S. at 568 (citing Los Angeles Police Dep't v. United Reporting Publishing Corp., 528 U.S. 32, 40 (1999)) (internal quotation marks omitted). This argument is only applicable to the portion of the statutory provision that prohibits "pharmaceutical manufacturers and pharmaceutical marketers" from using "prescriber-identifying information for marketing or promoting a prescription drug." 18 VT. STAT. ANN. § 4631(d). The pharmacies that sell prescriber-identifying information, obviously, already have access to it.

79. *Sorrell*, 564 U.S. at 566–67.

80. *See id.* at 567 ("[R]estrictions on protected expressions are distinct from restrictions on economic activity or, more generally, on nonexpressive conduct. It is also true that the First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech.").

81. *See* Rumsfeld v. Forum for Acad. & Institutional Rights, 547 U.S. 47, 62 (2006) ("Congress, for example, can prohibit employers from discriminating in hiring on the basis of race. The fact that this will require an employer to take down a sign reading 'White

commerce" and "conduct," and only circuitously implicate speech, they do not violate the First Amendment.[82] Vermont argued that the Prescription Confidentiality Law banned only commercial conduct — the sale of sensitive information by pharmacies to detailers — and only incidentally impaired the commercial speech of detailers when selling drugs to doctors.[83] If the Court agreed with either argument, the Prescriber Confidentiality Law would avoid First Amendment scrutiny altogether.[84]

In the alternative, Vermont argued that its statute could pass intermediate scrutiny, if forced to face it.[85] Vermont advanced two substantial government interests it believed the Prescription Confidentiality Law directly advanced.[86] First, the Prescriber Confidentiality Law protected medical privacy, confidentiality, and the doctor-patient relationship.[87] Under the law, physicians could feel secure that their information was not being proliferated for unwanted purposes, and patients could feel secure that physician expertise, not marketing tactics, governed what medications they were prescribed.[88] Second, Vermont argued the law improved public health and reduced healthcare costs.[89] Without highly targeted detailing campaigns, doctors were more likely to prescribe less costly medication.[90]

2. *The Majority Opinion*

Justice Kennedy, writing for a six-Justice majority, found that the Prescriber Confidentiality Law violated the First Amendment.[91] Justice Kennedy asserted that Vermont "imposed content- and speaker-based restrictions on the availability and use of prescriber identifying information . . . sufficient to justify application

---

Applicants Only" hardly means that the law should be analyzed as one regulating the employer's speech rather than conduct.").

82. *Sorrell*, 564 U.S at 567.
83. *See id.* at 566–67.
84. *See id.* at 566–68.
85. *See id.* at 572.
86. *Id.*
87. *Id.*
88. *Id.* at 575–76.
89. *Id.* at 576.
90. "[D]etailing affects the cost of medications, because it is 'confined to high-margin, high-profit drugs, for which the manufacturer has a substantial incentive to increase sales.'" 2007 Vt. Acts & Resolves 80 § 1(15). This marketing behavior "'contributes to the strain on health care budgets for individuals as well as health care programs.'" *Id.*
91. *Sorrell*, 564 U.S. at 557.

of heightened scrutiny."[92] The Court found that Vermont could not justify its law under *Central Hudson* because Vermont "burdened a form of protected expression that it found too persuasive. At the same time, the State [ ] left unburdened those speakers whose messages are in accord with its own views."[93]

The majority quickly rejected both of Vermont's arguments for not applying First Amendment scrutiny.[94] The "access to information" argument was rejected because the Court had only recognized a distinction between speech and access to information where the government had held the information and prohibited private parties from obtaining it.[95] The Court declared the doctrine inapplicable in "a case in which the government is prohibiting a speaker from conveying information that the speaker," here, the pharmacy, "already possesses."[96] The incidental burden argument was also dismissed because "the creation and dissemination of information are speech within the meaning of the First Amendment."[97] As such, the burden on speech is not incidental to the Prescriber Confidentiality Law, but rather its main objective.[98]

Justice Kennedy proceeded to apply the *Central Hudson* intermediate scrutiny test to the Vermont law,[99] finding that neither of Vermont's proffered justifications withstood scrutiny.[100] Justice Kennedy noted the possibility that "physicians have an interest in keeping their prescription decisions confidential" but did not

---

92. *Id.* at 571. It is noteworthy that Justice Kennedy referred to "heightened scrutiny" as the applicable standard of review for regulations that impose content-and speaker-based restrictions on commercial speech. *Id.* The *Central Hudson* majority never used the term "heightened scrutiny," but Justice Blackmun did refer to the promulgated test as an "intermediate level of scrutiny" in his concurrence. Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 573 (1980) (Blackmun, J., concurring). The importance of this word choice is discussed in Part III.C, *infra*.

93. *Sorrell*, 564 U.S. at 580.

94. *Id.* at 567–69.

95. *Id.* at 567–68; *see also* Los Angeles Police Dep't v. United Reporting Publishing Corp., 528 U.S. 32 (1999) (upholding a California law prohibiting the public from obtaining arrestees' addresses and using arrestees' addresses for commercial gain).

96. *Sorrell*, 564 U.S. at 568 (citing *United Reporting*, 528 U.S. at 40) (internal quotation marks omitted).

97. *Id.* at 570 (citations omitted). Part III.D, *infra*, discusses the effect of this holding on data collectors and data brokers.

98. *Sorrell*, 564 U.S. at 570.

99. *See id.* at 572 ("To sustain the targeted, content-based burden § 4631(d) imposes on protected expression the state must show at least that the statute directly advances a substantial government interest and that the measure is drawn to achieve that interest.") (citing Bd. of Trs. of State Univ. of New York v. Fox, 492 U.S. 469, 480–81 (1989); Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980)).

100. *Id.* at 572 (citations omitted).

comment on the substantiality of that interest.[101] Instead, he held that the law was not sufficiently tailored to an interest in prescriber confidentiality, because only detailers were prohibited from buying prescriber identifying information.[102] Pharmacies could still compromise physician and patient privacy by selling the data to educational institutions, journalists, governments, researchers, and anyone else except those seeking to use the information to market brand name drugs.[103] Vermont's regulatory scheme therefore bore little relation to the privacy interests it claimed to advance, inviting suspicion that its true goal was to limit the speech of detailers specifically.[104]

Vermont's second proffered objective, reducing the costs of medical services, fared even worse. Although the resulting public health benefits of lower healthcare costs were a substantial government purpose, the majority opinion held that Vermont's law did not *directly* advance the purpose of lowering health care costs, stating:

> The State seeks to achieve its policy objectives through the indirect means of restraining certain speech by certain speakers — that is, by diminishing detailers' ability to influence prescription decisions. Those who seek to censor or burden free expression often assert that disfavored speech has adverse effects. But the "fear that people would make bad decisions if given truthful information" cannot justify content-based burdens on speech. . . . That the state finds expression too persuasive does not permit it to quiet the speech or to burden its messengers.[105]

Rather than address the underlying reasons for the high price of brand-name drugs, or incentivizing or persuading physicians to prescribe generics, Vermont indirectly pursued its goals by impairing the ability of detailers to persuade physicians to prescribe their brand-name products.[106] Justice Kennedy noted that the original rationale for giving First Amendment protection, articulated in *Virginia Board of Pharmacy*, was that "'people will perceive their

101. *Id.*
102. *Id.* at 573.
103. *Id.*
104. *Id.*
105. *Id.* at 577–78 (citations omitted).
106. *Id.* at 577.

own best interests if only they are well enough informed, and that the best means to that end is to open the channels of communication rather than to close them.'"[107] The Prescription Confidentiality Law sought to close, or at least narrow, the channels of communication between detailers and doctors.[108] The Court struck down the restrictions on the sale and use of prescriber-identifying information for pharmaceutical marketing as violations of the First Amendment rights of detailers.[109]

C. *SORRELL*'S EFFECT ON COMMERCIAL SPEECH DOCTRINE

Justice Kennedy wrote in *Sorrell* that the Prescription Confidentiality Law placed a "content- and speaker-based burden" on detailers that "require[d] heightened judicial scrutiny."[110] The Court in *Central Hudson* promulgated a test that Justice Blackmun, concurring in the judgment, called "an intermediate level of scrutiny."[111] Justice Kennedy created ambiguity about what, if anything, this difference in word choice denoted, leading one scholar to describe the opinion as "incoherent."[112] Some have read *Sorrell* as maintaining the *Central Hudson* status quo; others have read it as making commercial speech regulations substantially more constitutionally suspect.[113] This Part puts forward a middle-ground reading of *Sorrell* — it argues that *Sorrell* raised the level of scrutiny applied to some, but not all, commercial speech regulations.

The most straightforward reading of *Sorrell* is that it made no change in commercial speech doctrine at all. "Heightened

---

107. *Id.* at 578 (quoting Virginia Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 770 (1976)); *see also supra* Part III.A.

108. *Sorrell*, 564 U.S. at 578.

109. *Id.* at 580.

110. *Id.* at 569–70.

111. Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 573 (1980) (Blackmun, J., concurring).

112. Tamara R. Piety, *"A Necessary Cost of Freedom"? The Incoherence of* Sorrell v. IMS, 64 ALA. L. REV. 1, 54 (2012) ("[T]he [*Sorrell*] Court rendered the commercial speech doctrine incoherent and sowed further confusion about what the appropriate test is.").

113. *Compare* Hunter B. Thomson, *Whither* Central Hudson*? Commercial Speech in the Wake of* Sorrell v. IMS Health, 47 COLUM. J.L. & SOC. PROBS. 171, 195 (2013) (noting that "most courts construing *Sorrell* have been reluctant to hold that it represented new doctrine and instead have held that *Sorrell* is consistent with prior precedent[ ]"), *with* Piety, *supra* note 112, at 4 (placing *Sorrell* in a line of cases that have, "over time, interpreted the *Central Hudson* test more strictly so that some commentators have observed that what began life as an intermediate scrutiny test has evolved into a strict scrutiny test in all but name") (citation omitted).

scrutiny," after all, is often synonymous with "intermediate scrutiny."[114] As discussed above, Justice Kennedy faithfully applied the *Central Hudson* intermediate scrutiny standard to Vermont's Prescription Confidentiality Law.[115] This interpretation has found support in at least one circuit court. In *R.J. Reynolds Tobacco Co. v. FDA*,[116] the Circuit Court of Appeals for the District of Columbia adopted the view that *Sorrell* made no change to commercial speech doctrine.[117] Instead, *R.J. Reynolds* interpreted *Sorrell* as a reminder that stymying a disfavored speaker's speech is not a substantial government interest.[118]

Nonetheless, numerous scholars have interpreted Justice Kennedy's use of "heightened scrutiny" to mean something else — something more stringent — than the intermediate scrutiny test promulgated in *Central Hudson*.[119] Justice Breyer, dissenting in

---

114. *See Heightened Scrutiny*, BLACK'S LAW DICTIONARY (11th ed. 2019).

115. *See supra* Part III.B; *see also* Agatha M. Cole, *Internet Advertising After* Sorrell v. IMS Health*: A Discussion on Data Privacy & the First Amendment*, 30 CARDOZO ARTS & ENT. L.J. 283, 308 (2012) ("[T]he Court's articulation of its standard in assessing Vermont's ability to demonstrate 'a substantial government interest' and to show 'that the measure is drawn to achieve that interest,' cites several intermediate scrutiny cases, suggesting that 'heightened scrutiny' is ostensibly more akin to intermediate scrutiny than strict scrutiny.") (citations omitted).

116. R.J. Reynolds Tobacco Co. v. FDA, 696 F.3d 1205 (D.C. Cir. 2012).

117. *Id.* at 1221–22 (D.C. Cir. 2012).

118. *Id.*

119. *See* Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 858 (2012) ("[T]he Court blurred the distinction between strict and intermediate scrutiny; a blurring that suggests a willingness . . . to reconsider the treatment of commercial speech as a category of lower-value, less-protected speech.") (citations omitted); Marcia M. Boumila et al., *Prescription Data Mining, Medical Privacy and the First Amendment: The U.S. Supreme Court in* Sorrell v. IMS Health Inc., 21 ANNALS OF HEALTH L. 447, 456 (2012) ("[T]he Court . . . struck down the Prescription Confidentiality law on grounds that the regulation imposed content- and speaker-based burdens on protected speech, thus warranting 'heightened' — not intermediate — scrutiny.") (citation omitted); Isabelle Bibet-Kalinyak, *A Critical Analysis of* Sorrell v. IMS Health, Inc.*: Pandora's Box at Best*, 67 FOOD DRUG L.J. 191, 208 (2012) ("In the second part of the opinion, the Court upheld that [the Prescription Confidentiality Law's] specific, content-based burden on protected expression warrants a strict standard of judicial scrutiny . . . . Justice Kennedy held that, whenever the basis of the regulation reflects aversion or disagreement for the content of disfavored speakers' speech . . . heightened judicial scrutiny is the proper standard. . . . Furthermore, the Court found Vermont's arguments for intermediate scrutiny unpersuasive.") (citations omitted); Thomson, *supra* note 113, at 205–06 ("A series of decisions culminating in *Sorrell* has elevated the rigor of judicial review of commercial speech to something stronger than the intermediate scrutiny applied to it under the *Central Hudson* framework."); Ashutosh Bhagwat, *In Defense of Content Regulation*, 102 IOWA L. REV. 1427, 1450 (2017) ("[I]n the recent *Sorrell* case . . . Justice Kennedy's majority opinion strongly suggested that even though the Vermont Statute protecting prescriber-identifying information was a regulation of commercial speech, it should have been subject to 'heightened judicial scrutiny.' While the Court ultimately backed off these suggestions and applied intermediate

Sorrell, also noted that Justice Kennedy's invocation of "heightened scrutiny" suggested "a standard yet stricter than *Central Hudson*."[120] This interpretation is more nuanced than simply looking up "heightened scrutiny" in a legal dictionary, and the arguments advanced by Justice Breyer and his supporting scholars are worth considering.

First, Justice Kennedy, in explaining when a law is subject to his "heightened scrutiny" standard, cited cases applying strict scrutiny.[121] For instance, to support the proposition that "heightened scrutiny is warranted" when a law imposes "a specific, content-based burden on protected expression," Justice Kennedy cited *Turner Broadcasting System, Inc. v. FCC*.[122] *Turner Broadcasting System* held that "speaker-based laws demand strict scrutiny when they reflect the Government's preference for the substance of what favored speakers have to say (or aversion to what the disfavored speakers have to say)."[123] Ultimately, the Court in that case applied intermediate, not strict, scrutiny, but only because it found the law at issue was content-neutral.[124] Justice Kennedy also cited *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Board*[125] — which applied strict scrutiny to a law that financially disincentivized publishing a criminal's description of their crime — as justification for applying heightened scrutiny to content- and speaker-based restrictions on commercial speech.[126]

Second, Justice Kennedy, by basing his call for heightened scrutiny on the imposition of "content- and speaker-based burdens," appeared to be identifying a subset of commercial speech regulations that he found more odious, and subject to more stringent

---

scrutiny — albeit, the ultra-strict modern variety — the implications for the future are obvious.") (citations omitted).

120. Sorrell v. IMS Health Inc., 564 U.S. 552, 588 (2011) (Breyer, J., dissenting). Justice Breyer further noted that "[t]o apply a strict First Amendment standard virtually as a matter of course when a court reviews an ordinary economic regulation" would usurp the legislative role because "to apply a 'heightened' First Amendment standard of review whenever [a commercial regulation] burdens speech would transfer from legislatures to judges the primary power to weigh ends and to choose means[.]" *Id.* at 584–85.

121. *Details, Detailing, and the Death of Privacy*, *supra* note 119, at 857 ("As a consequence, the Court stated, the law must survive 'heightened judicial scrutiny,' and proceeded to cite a number of cases applying strict scrutiny to content-based restrictions on fully protected speech.") (citation omitted).

122. *Sorrell*, 564 U.S. at 565 (citing Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 658 (1994)).

123. *Turner Broad. Sys.*, 512 U.S. at 658 (citation omitted).

124. *Id.* at 661–62 (citations omitted).

125. Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.

126. *See Sorrell*, 564 U.S. at 566 (citing *Simon & Schuster*, 502 U.S. at 112).

judicial review, than other commercial speech regulations. "Vermont's law does not simply have an effect on speech" Justice Kennedy noted, "but is directed at certain content and is aimed at particular speakers."[127] That fact, Justice Kennedy argued, "is sufficient to justify application of heightened scrutiny.[128] In his dissent, Justice Breyer pointed out that "neither of these categories — 'content-based' nor 'speaker-based' — has ever before justified greater scrutiny when regulatory activity affects commercial speech."[129] As such, Justice Breyer was adamant that the majority "is suggesting a standard yet stricter than *Central Hudson*."[130] If the "heightened scrutiny" Justice Kennedy called for was synonymous with *Central Hudson*, then there would have been no need to point to content-based burdens on commercial speech.[131] The fact that the law burdened commercial speech at all would have justified applying *Central Hudson*.[132]

The considerable evidence that *Sorrell* introduced a stricter (if not strict) level of "heightened" scrutiny into commercial speech jurisprudence raises the question: When does this "heightened" scrutiny standard apply? A satisfactory answer to this question requires further parsing of the ambiguities of the *Sorrell* holding. One possibility is that *Sorrell* collapses the distinction between commercial speech and pure speech.[133] This Note proffers another possibility: that *Sorrell* increases the scrutiny applied to commercial speech restrictions only when they enact both content- *and* speaker-based distinctions.

The more radical reading of *Sorrell* is that it requires a stricter, "heightened" scrutiny when a law imposes content-based burdens on commercial speech alone. Such a reading would collapse the distinction between commercial speech and pure speech established since *Central Hudson*.[134] Distinguishing between

---

127. *Sorrell*, 564 U.S. at 567.

128. *Id.* at 571.

129. *Id.* at 588 (Breyer, J., dissenting).

130. *Id.*

131. *See id.* ("The Court (suggesting a standard yet stricter than *Central Hudson*) says that we must give *content-based* restrictions that burden speech 'heightened' scrutiny.") (emphasis in original).

132. *See* Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563–66 (1980).

133. *See* Thomson, *supra* note 113, at 173.

134. *Compare* Thomson, *supra* note 113 at 173 ([*Sorrell*] "has all but collapsed the distinction between the level of First Amendment Protection accorded to commercial speech and noncommercial speech"), *with* Bd. of Trs. v. Fox, 492 U.S. 469, 777 (1989) (noting that,

commercial and non-commercial speech involves making a content-based distinction.[135] Any commercial speech regulation, then, would be subject to heightened scrutiny, as defined by *Sorrell*.[136] Decades of precedent that "make clear that the First Amendment offers considerably less protection" to commercial speech would be endangered.[137]

A holistic review of Justice Kennedy's *Sorrell* opinion belies a heightened scrutiny standard for content-based commercial speech restrictions, absent speaker-based distinctions. Those who interpret *Sorrell* as requiring heightened scrutiny for solely content-based burdens on speech point to Justice Kennedy's statement that the Prescription Confidentiality Law "is designed to impose a specific, content-based burden on protected expression," from which he held that "it follows that heightened judicial scrutiny is warranted."[138] Interestingly, Justice Kennedy then cites two cases for this proposition, one referring to content-based burdens on speech, and another referring to speaker-based burdens on speech.[139] Justice Kennedy further undercuts the idea that his heightened scrutiny standard applies to commercial speech regulations that are merely content-based by stating that the government can "justify its content-based law" by meeting the three-part test promulgated in *Central Hudson*.[140] The notion that Justice Kennedy is applying a "heightened scrutiny" greater than intermediate scrutiny to

---

under *Central Hudson* commercial free speech occupies a "subordinate position in the scale of First Amendment values") (internal quotation omitted).

135. Piety, *supra* note 112, at 36 ("[T]here must be some quality by which courts identify and distinguish commercial from non-commercial speech: a distinction that is obviously content-based."); *see also* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748, 761 (1976) ("If there is a kind of commercial speech that lacks all First Amendment protection . . . it must be distinguished by its content."); Thomson, *supra* note 113, at 202 ("Regardless of the precise contours of what falls under the category of commercial speech, the category of expression is distinguished by it content.").

136. *See Thomson*, supra note 113, at 173 ("By declaring that content-based restrictions trigger heightened review in an area of law that is distinguished by the content of speech, the Court appears to have elevated the First Amendment protection accorded to commercial speech.").

137. Sorrell v. IMS Health Inc., 564 U.S. 552, 583 (2011) (Breyer, J., dissenting).

138. *Id.* at 565; *see also* Thomson, *supra* note 113, at 187 n.114 (citing the same portion of *Sorrell* as support for heightened scrutiny of content-based commercial speech regulation).

139. *Sorrell*, 564 U.S. at 565 (citing Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 418 (1993) (content-based burden); Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 658 (speaker-based burden)); *see also* Trans Union Corp. v. FTC, 267 F.3d 1138, 1141 (D.C. Cir. 2001) (citing *Discovery Network* as evidence "content-based" burdens "cannot alone trigger strict scrutiny").

140. *Sorrell*, 564 U.S. at 571–72 (citing *Central Hudson*, 447 U.S. at 557).

mere content-based commercial speech regulation is thus directly contradicted by his own words.

Justice Kennedy's view of commercial speech regulations that enact content- *and* speaker-based restrictions is, in contrast, strikingly consistent. Admonishments against regulation based on the identity or interest of the speaker are repeated throughout the opinion.[141] The proposition that content- *and* speaker-based restrictions trigger heightened scrutiny finds far more support in *Sorrell* than the proposition that content-based restrictions alone, i.e., all commercial speech regulations,[142] impose such a burden on the government.

In using *Sorrell* to develop a framework for constitutionally permissible state data privacy law, then, this Note makes two recommendations. First, legislators should avoid triggering the "all but dispositive" "heightened scrutiny" that was announced in *Sorrell*.[143] Second, to avoid that "heightened scrutiny," legislators must not impose speaker-based restrictions on commercial speech, which are already content-based by nature. By doing so, a state data privacy issue should be subject to intermediate scrutiny.

D. *SORRELL* AND DATA PRIVACY: COMMERCIAL DATA IS COMMERCIAL SPEECH

The *Sorrell* Court found that the Prescription Confidentiality Law — a regulation on the sale of prescriber-identifying data — violated the First Amendment rights of detailers.[144] Detailers used data about prescribing habits in order to efficiently and effectively target their marketing campaigns to physicians.[145] Online advertisers use data to efficiently and effectively target their advertising to consumers.[146] Thus, *Sorrell* applies to data privacy laws that

---

141. *See id.* at 565 ("Vermont's law goes even beyond mere content discrimination, to actual viewpoint discrimination") (citation and internal quotation marks omitted); *id.* at 572 ("[*Central Hudson*] standards ensure . . . that the law does not seek to suppress a disfavored message"); *id.* at 573 ("The explicit structure of the statute allows the information to be studied and used by all but a narrow class of disfavored speakers."); *id.* at 577 ("The State seeks to achieve its policy objectives through the indirect means of restraining certain speech by certain speakers."); *id.* at 580 ("[T]he State has left unburdened those speakers whose messages are in accord with its own views. This the State cannot do.").

142. *See e.g.*, Piety, *supra* note 112 at 1–5.

143. *Sorrell*, 564 U.S. at 571.

144. *See id.* at 580.

145. *See id.* at 558.

146. *See supra* Part II.

similarly burden the commercial speech of advertisers. This Part goes beyond advertisers and turns to the question of what effect, if any, *Sorrell* has on the other actors regulated by data privacy laws.

Data collectors and data brokers are also frequently subject to data privacy laws.[147] The Prescription Confidentiality Law, in fact, regulated pharmacies in their capacity as collectors and distributers of prescriber-identifying information.[148] *Sorrell* briefly grappled with the question of whether the Prescription Confidentiality Law also violated the First Amendment rights of pharmacies by addressing the question of whether "prescriber-identifying information" itself "is speech for First Amendment purposes."[149] Ultimately, the Court sidestepped the question by basing its holding on the law's impact on the commercial speech of detailers.[150] Nonetheless, the *Sorrell* Court's brief consideration of "the rule that information is speech"[151] suggests its willingness to extend First Amendment protections to data collectors and brokers.

That data brokers and data collectors, like the pharmacies in *Sorrell*, are speakers is simultaneously counter-intuitive and plainly obvious. People do not normally view scraping and selling data as speaking, let alone expressive behavior covered by the First Amendment. It is clear, however, that "'the creation and dissemination of information are speech within the meaning of the First Amendment.'"[152] Data published in a scientific journal is speech.[153] A lawyer disclosing a client's phone number and email address to a coworker is clearly speaking;[154] that the content of the speech is personal information is irrelevant. A data broker obtains data about consumers, including personal information, and charges a fee to disclose it. It is speaking by disclosing the

147. *See supra* Part II.

148. *See Sorrell*, 564 U.S. at 552.

149. *Id.* at 570.

150. *Id.* ("The State asks for an exception to the rule that information is speech, but there is no need to consider that request in this case. The State has imposed content- and speaker-based restrictions on the availability and use of prescriber-identifying information.").

151. *Id.*

152. *Id.* (quoting Bartnicki v. Vopper 532 U.S. 514, 575 (2001)).

153. *See generally*, ONY, Inc. v. Cornerstone Therapeutics, Inc., 720 F.3d 490, 498 (2d Cir. 2013) (dismissing Lanham Act claim against non-fraudulent data published in a scientific journal on First Amendment principles).

154. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implication of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1056 (2000) (including "bans on lawyers revealing information about their clients" in a list of restrictions on speech).

information it knows. Using this straightforward understanding of speech, Professor Eugene Volokh describes privacy laws as "a right to stop people from speaking about you."[155]

Were the pharmacies in *Sorrell*, by selling prescriber-identifying information, simply speaking to detailers about doctors? Did the Prescriber Confidentiality Law violate the First Amendment rights of pharmacies by stopping them from speaking to detailers about doctors? The lower court in *Sorrell* did not think so. It described prescriber-identifying information as no more similar to speech than beef jerky; both are simply products to be sold.[156] The Supreme Court, in contrast, was clear that information does not cease to be speech simply because "it results from an economic motive."[157] "The fact that newspapers and books are sold" does not diminish their central place in First Amendment jurisprudence.[158] Ultimately, the *Sorrell* Court rested its ruling on the burden the law placed on detailers.[159] But even in refusing to decide the issue, the Court noted "there is . . . a strong argument that prescriber-identifying information is speech."[160]

Critics of *Sorrell* have described this portion of the ruling as a finding that "data is speech."[161] Professor Neil M. Richards warns that such a finding would usher in a new "digital *Lochner*," referring to an era where the Court enacted its "conservative economic, libertarian view," "'substituting judicial for democratic decisionmaking where ordinary economic regulation [was] at issue.'"[162] Digital *Lochner*, he argues, will be an era where ordinary economic regulations are struck down by a Court enacting a libertarian vision of the First Amendment "that somehow equates 'data' with 'speech.'"[163]

Professor Richards is not the only one worried about digital *Lochner*. The dissenting justices in *Sorrell* similarly forecast that

---

155. *Id.* at 1049.
156. IMS Health Inc. v. Ayotte, 550 F.3d 42, 53 (1st Cir. 2008).
157. Sorrell v. IMS Health Inc., 564 U.S. 552, 567 (2011).
158. New York Times Co. v. Sullivan, 376 U.S. 254, 266 (1964) (noting that it was "immaterial" to the First Amendment analysis of the case that the speech in question appeared in a paid advertisement in the New York Times).
159. *Sorrell*, 564 U.S. at 570.
160. *Id.*
161. *See In Defense of Content Regulation*, *supra* note 119 at 1445 ("[T]he Court avoided the broader issue of whether facts and data are speech . . . [b]ut the implications of the majority's language are clear enough."); *see also* Richards, *supra* note 4 at 1524.
162. Richards, *supra* note 4 at 1529–30 (quoting *Sorrell*, 564 U.S. at 603).
163. *Id.* at 1513.

the ruling will open "a Pandora's Box of First Amendment challenges to many ordinary regulatory practices" that "reawakens *Lochner*[ ]."[164] As society continues to be "transformed into digital form," the need for data privacy laws will increase, as will the consequences for failing to act.[165] The consequences of digital *Lochner* are dramatic, and it will only become more untenable as the marketplace of ideas, marketplace of data, and the actual economic market become synonymous.[166] Professor Richards insists that digital *Lochner* must be rejected.[167] Maybe so, but *Sorrell* suggests that a majority of justices support taking steps toward digital *Lochner*, and believe that data is speech.[168]

But the situation is not as bleak as Professor Richards paints it, at least for data privacy. A rule that data is speech raises the question: what kind of speech? The answer is critical because it informs the level of scrutiny data regulations may receive, and as such it "will depend on context."[169] There is ample evidence that, in the context of data privacy law, consumers' data is commercial speech.[170]

Commercial speech commonly means speech that "'propose[s] a commercial transaction,'"[171] but also encompasses "expression related solely to the economic interests of the speaker and its audience."[172] In *Dun & Bradstreet v. Greenmoss Builders*,[173] the Supreme Court used the economic interest definition of commercial speech to justify applying the *Central Hudson* test to a credit report that contained false information.[174] In 2001, the Court of

164. *Sorrell*, 564 U.S. at 602.

165. Richards, *supra* note 4 at 1530.

166. *Id.* at 1531 ("If our lives become digital, but data is speech, regulation of many kinds of social problems will become impossible.").

167. *Id.*

168. *Id.* at 1516 (describing *Sorrell* as favoring a "broad First Amendment Protection against all privacy rules" and that its "First Amendment critique of privacy does, or should, apply to privacy law in the data context").

169. Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 105 (2014). Professor Bambauer further contends that "data disseminated in an advertisement," which would encompass most data implicated by data privacy law, "will receive the lesser protections afforded to commercial speech under the *Central Hudson* test just like any other advertising speech." *Id.*

170. *See generally id.* at 72–75.

171. Bd. of Trs. v. Fox, 492 U.S. 469, 473 (1983) (quoting Virginia Pharmacy Bd. v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976)).

172. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 561 (1980).

173. Dun & Bradstreet v. Greenmoss Builders, 472 U.S. 749 (1985).

174. *Id.* at 762. Because the information in the credit report was false, the first prong of the *Central Hudson* test dictated that it receives no First Amendment protection. *Id.*

Appeals for the District of Columbia applied *Dun & Bradstreet* in reviewing an FTC determination that "lists of names and addresses" sold by a consumer reporting agency to "target marketers" were consumer reports and could not lawfully be sold under the Fair Credit Reporting Act (FCRA).[175] One year after *Sorrell* was decided, the District Court for the Eastern District of Pennsylvania similarly applied a commercial speech inquiry to consumer report information.[176] The FCRA cases all lead to the same conclusion. Data collected from consumers, compiled for commercial interests, and designed to be sold for the purpose of advertising — i.e., the work of data collectors and data brokers — constitutes commercial speech.

Sorrell suggests that data is speech. When a law burdens the ability of data collectors or data brokers to create and disseminate data, it burdens speech.[177] Because those data are "related solely to the economic interests" of the data brokers, data collectors, and advertisers, they are commercial speech.[178] After *Sorrell*, data privacy laws are subject to a commercial speech inquiry regardless of whether they regulate the targeted advertisements that rely on consumer data or the data brokers and data collectors who provide that data.

IV. BLUEPRINT FOR POST-*SORRELL* DATA PRIVACY LAWS

Although *Sorrell* places considerable constraints on data privacy laws, it does not make effective regulation impossible. This Part considers in turn the three objectives for state data privacy laws previously outlined.[179] Part IV.A explains why *Sorrell*'s changes to commercial free speech doctrine invalidate state data privacy laws directed at target advertising. Part IV.B argues that data privacy laws that seek to protect consumers from cybercrime face significant obstacles, leaving room to doubt their constitutionality. Part IV.C addresses data privacy laws that empower

("This particular interest warrants no special protection when — as in this case — the speech is wholly false.").

175. Trans Union Corp. v. FTC, 245 F.3d 809, 818 (D.C. Cir. 2001).

176. King v. General Info. Servs., 903 F. Supp. 2d 303 (E.D. Penn. 2012).

177. Sorrell v. IMS Health, 564 U.S. 557, 570 (2011) ("[T]he creation and dissemination of information are speech within the meaning of the First Amendment.").

178. *Central Hudson*, 447 U.S. at 561.

179. *See supra* Part II.

consumers to make choices about their online privacy and finds that these laws are the most likely to survive scrutiny under *Sorrell*.

A. DATA PRIVACY LAWS DIRECTED AT TARGETED ADVERTISING

The addictiveness and effectiveness of social media platforms and highly targeted advertising is a matter of public concern and impetus for some data privacy regulations.[180] Nonetheless, *Sorrell* is emphatic that commercial speech, even under an intermediate scrutiny standard, is not justified by fear that the regulated speech is "too persuasive."[181] States seeking to implement data privacy statutes must proffer a government purpose other than the social ills of targeted advertising to justify regulation of information websites, advertisers, and data brokers are allowed to collect.[182] However, a data privacy statute is not invalidated merely because it burdens targeted advertising by reducing the amount of data advertisers have at their disposal.[183]

Among the ambiguity and incoherence present throughout *Sorrell*, the majority makes one point absolutely clear: the persuasive "force of speech" cannot "justify the government's attempts to stifle it."[184] The impetus in *Virginia State Board of Pharmacy* for granting First Amendment protection to commercial speech was the public's "strong interest in the free flow of commercial information."[185] Prohibiting commercial speech based on "fear that people would make bad decisions" if exposed to the speech subverts the First Amendment's purpose in this area.[186] In *Sorrell*, Vermont argued that "lowering the costs of medical services and promoting public health" were substantial government interests.[187]

---

180. *See supra* Part II.

181. Sorrell v. IMS Health Inc., 564 U.S. 552, 578 (2011).

182. *Id.* at 579.

183. *Id.* at 567 ("[T]he First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech.").

184. *Id.* at 577. It is worth reiterating here that false and misleading advertising is not afforded First Amendment Protection. *See* Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 564 (1980). Speech that is persuasive because it is false is not protected. *Id.*

185. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748, 764 (1976).

186. *Sorrell*, 564 U.S. at 577 (citing Thompson v. Western States Medical Center, 535 U.S. 357, 374.).

187. *Sorrel*, 564 U.S. at 576.

The *Sorrell* Court agreed.[188] But rather than address the underlying reasons for the high price of medical services, Vermont simply hindered efforts to market expensive drugs.[189] The Court found that *Central Hudson* intermediate scrutiny was not met because the law did not directly advance Vermont's public health interest.[190] Any data privacy law justified by addressing the effectiveness of targeting advertising would similarly be invalidated, even under the permissive intermediate scrutiny of *Central Hudson*.

B. DATA PRIVACY LAWS THAT MITIGATE THE EFFECTS OF CYBERCRIME

Cybercrime poses great risks to consumers.[191] Nefarious actors may obtain personal information about a consumer,[192] which can lead to identify theft, fraud, and harassment.[193] Data breaches have only become more frequent and more costly in recent years.[194] The volume of data collected and transferred online, as well as the increasing value of information about consumers, has exacerbated the problem.[195] Data privacy laws that limit what and how much data a company can collect on a consumer reduce the volume of data any one consumer stands to lose from any one data breach.[196] Limitations on the sale of consumer data can address situations in which data is mishandled or abused by an entity that the consumer does not know exists or has no relationship with.[197]

The ability of cybersecurity-based data privacy statutes to survive commercial speech inquiry is unclear. There is some support for the proposition that protecting consumers from cybercrime is a

188. *Id.* at 577.
189. *Id.*
190. *Id.*
191. *See* Paul Wagenseil, *What to Do After a Data Breach*, TOM'S GUIDE (Apr. 15, 2019), https://www.tomsguide.com/us/data-breach-to-dos,news-18007.html [https://perma.cc/3F48-HRKV].
192. *See id.*
193. *See* Tiffany Hsu, *Data Breach Victims Talk of Initial Terror, Then Vigilance*, N.Y. TIMES (Sept. 9, 2017), https://www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html [https://perma.cc/J6LM-X248].
194. *See* Holmes, *supra* note 35.
195. *See* Bill Carey, *Top 3 Factors Driving the Rise in Data Breaches*, IT TODAY (Feb. 27, 2020), http://www.ittoday.info/Articles/Factors_in_Data_Breaches.htm [https://perma.cc/VB37-6S3P]; *see also*, Sheryl Falk et al., *Minimizing Privacy Risk With Data Minimization*, LAW.COM (Sept. 2, 2019), https://www.law.com/corpcounsel/2019/09/02/minimizing-privacy-risk-with-data-minimization [https://perma.cc/BWL6-FP76].
196. *See* Falk, *supra* note 195.
197. *See supra* Part II.

substantial government interest.[198] However, similar crime- and fraud-based justifications for regulating speech have often failed on directness and tailoring grounds.[199]

Sorrell, as well as cases regulating both in-person and online speech, may prove that the government has a substantial interest in protecting consumers from cybercrime. The *Sorrell* Court notes that an "interest in protecting consumers from 'commercial harms," including fraud, can justify content-based commercial speech regulations.[200] Furthermore, the Court recognizes "the prevention of fraud, the prevention of crime, and the protection of privacy" as substantial government interests when reviewing regulation of in-person speech under intermediate scrutiny.[201] The prevention of cybercrime, by analogy, may be a substantial government interest justifying regulation of online solicitation.

The District Court for the District of Columbia considered this analogy most directly in *Sandvig v. Sessions*,[202] which included a First Amendment challenge to the Computer Fraud and Abuse Act (CFAA).[203] *Sandvig* presented a public forum, not commercial speech, issue, but the case is still instructive since the court applied intermediate scrutiny.[204] The government argued the "Access Provision" of the CFAA that criminalized the unauthorized access of data on private websites served important interests in preventing cybercrime and what it called "the digital equivalent of trespassing."[205] The plaintiff disputed the trespass analogy but did not dispute that preventing cybercrime was a significant

198. *See, e.g.*, Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (finding that "significant interests appear to underlie the Access Provision" of the Computer Fraud and Abuse Act, "passed to prevent computer theft and other cybercrime").

199. *See, e.g.*, Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150 (2002) (finding a city ordinance requiring door-to-door solicitors to get a permit insufficiently tailored to the interest of preventing crime); Vill. of Schaumberg v. Citizens for a Better Env't, 444 U.S. 620, 638 (1979) (invalidating an ordinance governing solicitations by charitable organizations because it protected residents' privacy "only in the most indirect of ways").

200. Sorrell v. IMS Health Inc., 564 U.S. 552, 579 (2011).

201. *Watchtower Bible*, 536 U.S. at 164–65 (reviewing under intermediate scrutiny a city ordinance requiring door-to-door solicitors to apply for a permit); *see also* Vill. of Schaumberg v. Citizens for a Better Env't, 444 U.S. 620, 636 (1979) ("The Village urges that [the ordinance regulating solicitation] is intimately related to substantial government interests 'in protecting the public from fraud, crime, and undue annoyance.' These interests are indeed substantial.").

202. Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018).

203. *Id.* at 10.

204. *Id.* at 29–30 (rejecting strict scrutiny and proceeding to apply an intermediate scrutiny standard).

205. *Id.* at 30.

interest.[206] For its purposes of deciding a standing issue, it was enough for the district court to note that the plaintiff did not dispute that cybercrime was a significant interest.[207] The court in *Sandvig* never actually held that preventing cybercrime was a substantial interest, nor did it meaningfully explore the legitimacy of analogizing cybercrime to physical theft and trespass. Taken together, *Sorrell* and *Sandvig* point towards cybercrime prevention as a significant interest, but direct support for the proposition is lacking.

The fate of data privacy law under the second and third prongs of the *Central Hudson* test — that the statute directly advances the substantial government interest and is drawn to achieve that interest[208] — is even less clear. In-person speech regulations justified by the prevention of crime and fraud often fail on these grounds. Such regulations have been found too "indirect" where "less intrusive and more effective" measures — laws against fraud — are available.[209] Courts have held them insufficiently tailored to the stated government interest when they are significantly over- or under-inclusive of the conduct the regulation is designed to deter.[210] For instance, a city ordinance requiring all door-to-door solicitors to apply for a permit — which the city argued prevented commercial fraud and criminal behavior disguised as solicitation — was overinclusive because it regulated noncommercial solicitations and underinclusive because criminals could easily obtain a permit under false pretenses.[211]

Data privacy laws that seek to prevent cybercrime raise similar directness and tailoring concerns. Like in-person fraud, cybercrime is, by definition, against the law. More direct methods of regulation, like mandating minimum cybersecurity standards for data collectors, are also "less intrusive" on commercial speech.[212] Similarly, any prohibitions on the collection and transfer of consumer data are likely to be overinclusive. Data collectors, data brokers, and advertisers do not always employ ineffective means

206. *Id.*
207. *Id.*
208. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 566 (1980).
209. Vill. of Schaumberg v. Citizens for a Better Env't, 444 U.S. 620, 639 (1979).
210. Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 168 (2002).
211. *Id.* at 168–69.
212. *Schaumberg*, 444 U.S. at 639.

of securing their data, and they will not all be the victims of data breaches.

The realities of modern cybersecurity may, however, distinguish data privacy laws from those regulating door-to-door salespeople. *Central Hudson*'s directness and tailoring tests exist within the context of the state's proffered substantial interest.[213] The existence of a more direct or more narrowly tailored regulation does not alone invalidate a law if that regulation would be inadequate to achieve the proffered substantial government interest.[214] A data privacy law is not considered insufficiently direct unless "a less intrusive *and more effective*" measure is available.[215] The more direct approach of imposing cybersecurity regulatory standards suffers from the reality that the best cybersecurity methods available are not sufficient to prevent all cybertheft or data mishandling.[216]

Further, the mere fact that cybercrime is illegal is not nearly as persuasive an argument against directness as it is in the in-person commercial speech context. As compared to in-person theft or fraud, cybercrime is more impersonal and remote, and perpetrators are very rarely prosecuted.[217] A more narrowly drawn approach might be a requirement that when a company suffers a data breach resulting in loss of personal data, the company must notify all affected consumers. Such an approach is undermined by the difficulty in pinpointing which consumers have been affected, especially if the data breach also resulted in a loss of company

---

213. *See Central Hudson*, 447 U.S. at 564 ("[T]he regulatory technique must be in proportion to [the state's] interest.").

214. *See id.* ("[I]f the governmental interest could be served *as well* by a more limited restriction on commercial speech, the *excessive* restriction restrictions cannot survive.") (emphasis added); *Schaumberg*, 444 U.S. at 637 (striking down a commercial speech restriction where the state's "legitimate interest . . . can be better served by measures less intrusive").

215. *Schaumberg*, 444 U.S. at 639 (emphasis added); *see also Central Hudson*, 447 U.S. at 564 ("[T]he restriction must directly advance the state interest involved; the regulation may not be sustained if it provides *only ineffective or remote support* for the government's purpose.") (emphasis added).

216. *See supra* Part II.

217. *See* Roger A. Grimes, *Why it's so Hard to Prosecute Cybercriminals*, CSO (Dec. 6, 2016), https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html [https://perma.cc/X88F-7YE5] (detailing the jurisdictional issues and difficulties gathering evidence that pose unique challenges to identifying and prosecuting cybercriminals); Nick Selby, *Local Police Don't Go After Most Cybercriminals. We Need Better Training.*, WASH. POST (Apr. 21, 2017), https://www.washingtonpost.com/posteverything/wp/2017/04/21/local-police-dont-go-after-most-cybercriminals-we-need-better-training/ [https://perma.cc/U8SC-ZB2U] (attributing the lack of cybercrime prosecutions to insufficient cybercrime expertise in local police forces and severe resource shortages in the FBI).

records. The only information that is certain to be safe from a data breach is information that was never collected in the first place. If a court is convinced that more direct or more narrowly tailored regulations would fall short of achieving the state interest in preventing cybercrime, then data privacy laws may survive First Amendment challenges where laws based on prevention of in-person crime and fraud have failed.

Lastly, cybersecurity-based data privacy laws must avoid making speaker-based distinctions, lest they trigger *Sorrell*'s "heightened scrutiny."[218] Legislators may accidentally run afoul of this principle by only regulating certain industries.[219] For example, a recent Vermont law requiring data brokers, and no other entities, to register annually with the Secretary of State likely triggers heightened scrutiny for that reason.[220] The Vermont legislature rationalizes this speaker-based regulation by pointing out the cybersecurity "risks associated with the widespread aggregation and sale of data about consumers" to businesses with which the consumer has no relationship or knowledge.[221]

Speaker-based distinctions are more sensible for data privacy regulations based on cybersecurity, where different industries pose different risks to consumers, than for those based on protecting consumer privacy. Disclosure of personal information to any speaker necessarily harms privacy.[222] Determining which industries present the greatest cybersecurity risk to consumers and legislating accordingly is the kind of ordinary marketplace regulation impeded by "digital *Lochner*."[223] *Sorrell* reviewed a law justified by privacy concerns, not cybersecurity concerns.[224] Given the

---

218. *See supra* Part III.C.

219. *See supra* Part III.C. In *Sorrell*, Vermont prohibited pharmacies "from selling or disseminating prescriber-identifying information for marketing. The information, in other words, could be sold or given away for purposes other than marketing . . . . Under that reading, pharmacies may sell the information to private or academic researchers . . . but not, for example, pharmaceutical marketers." Sorrell v. IMS Health Inc., 564 U.S. 552, 562–63 (2011). That the law singled out the pharmaceutical industry, but not drug research, was a speaker-based restriction. *Id.*

220. VT. STAT. ANN. tit. 9 § 2446(a) (2019). Vermont defines a "data broker" as "a business, or unit or unites of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." *Id.* § 2430.

221. 2017 Vt. Acts & Resolves 171 § 1(a)(1)(D) (2018).

222. *See Sorrell*, 564 U.S. at 572–73 (holding that the Prescription Confidentiality Law was not tailored to advance medical privacy because prescriber-identifying information could still be sold to many parties).

223. *See* Richards, *supra* note 4 at 1529–31; *see also supra* Part III.D.

224. *See Sorrell*, 564 U.S. at 572.

opportunity to review a cybersecurity-based data privacy law, the Court could (and as this Note argues, should) reconsider its sweeping decision to apply a stricter, "heightened scrutiny" standard *any* time a law burdening commercial speech enacts speaker-based distinctions.[225] But at present, *Sorrell* controls.

While the invalidity of data privacy statutes premised on the social ills of target advertising is clear, the fate of data privacy statutes justified by mitigating cybersecurity risks is anything but clear. Such laws can be analogized to similar commercial speech regulations, but the Court has never weighed in on the strength of the analogy. It is therefore indeterminate whether data privacy law can meet the *Central Hudson* test by advancing an interest in preventing cybercrime. Furthermore, *Sorrell*'s broad language likely inhibits the state's ability to make commonsense, albeit speaker-based, distinctions about which actors and industries pose the greatest cybersecurity risk.

C. DATA PRIVACY LAWS THAT EMPOWER THE CONSUMER

The current marketplace for consumer information heavily favors businesses that collect, sell, and use consumer data; consumers have little ability to choose how and whether to share their information.[226] Data privacy laws can shift some control back into the hands of consumers. The Court has found privacy protection to be a substantial government purpose, both in *Sorrell* and in previous cases addressing in-person commercial speech.[227]

States often seek to protect data privacy by requiring businesses to honor a consumer's "opt out" request, prohibiting the

---

225. *See supra* Part III.C. For instance, the Court could, in considering when some speaker-based commercial speech regulations are appropriate, return to the logic it applied in *R.A.V. v. St. Paul*, where it said:

> When the basis for the content discrimination consists entirely of the very reason the entire class of speech at issue is proscribable, no significant danger of idea or viewpoint discrimination exists. Such a reason, having been adjudged neutral enough to support exclusion of the entire class of speech from First Amendment protection, is also neutral enough to form the basis of distinction within the class.

R.A.V. v. St. Paul, 505 U.S. 377, 388 (1992). This implies that if there was a content-neutral rationale for a particular commercial speech regulation — necessarily a content-based regulation — and that rationale also provided a neutral justification for applying the regulation to a particular group of speakers, then the law may not violate the First Amendment despite being speaker-based.

226. *See supra* Part II.

227. *See Sorrell*, 564 U.S. at 572–73; Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 165 (2002).

business from collecting or selling certain types of data from that consumer.[228] *Sorrell* indicated that "private decisionmaking" such as opt-out provisions "can avoid government partiality and thus insulate privacy measures from First Amendment challenge."[229] Although the Prescription Confidentiality Law might have "burdened" less speech if physicians had to opt out of the sale of their prescriber-identifying information rather than opt in,[230] the Court was quick to note that that would not have saved the law.[231] A physician could only prevent one type of speaker, detailers, from purchasing their information.[232] No other speakers were prevented from obtaining prescriber identifying information, regardless of the physician's consent.[233] It was thus a "contrived choice."[234]

Therefore, simply formulating a data privacy law as an individual right to opt out would not save it from challenge — the legislature cannot arbitrarily decide which parties must honor an opt-out request and which are exempt.[235] By making the law broadly applicable to all relevant entities — whether they be data collectors, data brokers, or advertisers — consumers would be empowered to decide with which actors they want to share their data.[236] Additionally, providing consumers an individual right to opt out of data collection by companies directly advances the government purpose of empowering consumers to protect their own online privacy.[237]

Granting an individual right to opt out of data collection is also narrowly drawn to advance the interest of consumer

228. Such a provision exists in the California Consumer Privacy Act, CAL CIV. CODE § 1798.120 (Deering 2019), and Nevada's Security Privacy of Personal Information statute, NEV. REV. STAT. § 603A.345(2) (2019).

229. *Sorrell*, 564 U.S. at 574.

230. *See id.* at 574 ("Vermont's law might burden less speech if it came into operation only after an individual choice.").

231. *See id.* at 574 ("[A] revision to that effect would not necessarily save § 4631(d).").

232. *Id.*

233. *Id.*

234. *Id.*

235. *See id.* at 574 ("Rules that burden protected expression may not be sustained when the options provided by the state are too narrow.").

236. Notably, such a law would also avoid "speaker-based" distinctions and would not trigger a heightened level of scrutiny under *Sorrell*. *See supra* Part III.C. If particular speakers are receiving more opt-out requests than others, it would be because of consumer choice, not government disfavor.

237. *See* Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 566 ("[W]e must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.").

empowerment.[238] The tailoring requirement of *Central Hudson* has been a stumbling block for other privacy-premised commercial speech restrictions.[239] In *Watchtower Bible & Tract Society v. Village of Stratton*,[240] permitting requirements for door-to-door solicitation were more intrusive and less effective than city ordinances already in place requiring solicitors to honor "No Solicitation" signs.[241] In *Sorrell*, a Vermont physician unhappy with detailing efforts could prevent harassment and assure their patients that expert medical judgment was the only factor in their prescribing decisions by simply refusing to meet with detailers.[242] Vermont's privacy protection interest did not justify burdening speech to achieve ends physicians could easily achieve themselves by shutting the door.[243]

These arguments are inapposite to data privacy laws that provide consumers with opt-out rights for online data collection. As noted, it is practically impossible for a consumer to avoid the online marketplace for data — they can neither avoid having their data collected nor avoid encountering the advertisements and websites that are specifically targeted to them.[244] Therefore, the only way a consumer can keep certain data collectors from obtaining their information is by opting out of data collection for the services they use. This was not an issue faced by physicians protected by the Prescriber Confidentiality Law or by homeowners in the Village of Stratton. Data privacy laws that empower consumers to opt-out of online data collection are essentially a "No Solicitation" sign for the Internet.[245]

Protecting privacy is a substantial government interest.[246] However, commercial speech restrictions seeking to protect privacy have often failed on tailoring grounds.[247] By providing

238. *See id.* at 565 ("The second criterion recognizes that the First Amendment mandates that speech restrictions be narrowly drawn.") (internal citation and quotations omitted).

239. *See* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 168 (2002).

240. *Id.*

241. *Id.*

242. Sorrell v. IMS Health Inc., 564 U.S. 552, 575 (2011).

243. *Id.*

244. *See supra* Part II.

245. Vill. of Schaumburg v. Citizens for a Better Env't, 444 U.S. 620, 639 (calling a "No Solicitation" sign a "less intrusive and more effective" measure to protect privacy from in-person marketers).

246. *See Sorrell*, 564 U.S. at 572–73; *Watchtower Bible*, 536 U.S. at 165.

247. *See Sorrell*, 564 U.S. at 575; *Watchtower Bible*, 536 U.S. at 168.

consumers an opt-out, the state would be using less burdensome means to empower consumers to protect their own privacy in a space where other protective measures are inadequate.[248] Data privacy laws are most likely to survive a commercial speech inquiry if it empowers consumers, through opt-out provisions, to meaningfully protect their own privacy.

V. CONCLUSION

The harms to consumers from unfettered collection and dissemination of their personal and online data are many. The likelihood that a consumer's data will fall into the wrong hands increases as the amount of data collected from them increases. Moreover, it is possible for a company that a consumer has no prior relationship or agreement with may mishandle or misuse the consumer's data. Even the most responsible consumer is unable to effectively protect their data. However, the Supreme Court in *Sorrell* announced a skepticism of legislative proposals that disallow certain companies from using data for disfavored purposes.

Free commercial speech is also an important interest. Americans are economic actors as much as, if not more than, political actors. As such, they have an interest in access to commercial information without a substantial government thumb on the scale. Nevertheless, this justification for commercial speech is undermined if consumers' privacy is compromised to present hyper-targeted advertisements on addictive platforms that represent serious cybersecurity threats. The industrial age *Lochner* Court impeded legislative attempts to regulate the societal harms that came with the new industrial economy.[249] With the *Sorrell* decision, the Court has chosen the same course for the information age as they did in the industrial age, and is inching closer towards digital *Lochner*.

Much of data privacy law cannot withstand digital *Lochner*, but some can. Data privacy law motivated by a desire to blunt the effectiveness of targeted advertising does not comport with the Court's disdain for regulation of disfavored speakers. Data privacy

248. *Sorrell*, 564 U.S. at 574.

249. Richards, *supra* note 4 at 1529 ("Afraid that laws regulating economic transactions could lead to wealth redistribution or socialism, the Court held that much of this economic regulation violated the Fourteenth Amendment's Due Process Clause, infringing on the rights of workers and employers to what it called the 'liberty of contract.'").

law that seeks to mitigate consumers' vulnerability to cyberthreats may survive *Sorrell*, but it would require the Court to explicitly address a government interest that has yet to be tested. The best path forward for states seeking to legislate in the data privacy sphere is to empower the consumer. Providing consumers with a private right to opt-out of data collection they find objectionable would place a minimal burden on speech, and directly advance the goal of vindicating privacy in a digital landscape. The *Lochner* era was "inconsistent with the needs of a modern, industrial economy," and ended only after invalidating much of the New Deal legislation passed in response to the Great Depression.[250] State data privacy law, though severely limited by *Sorrell*, can foster progress before disaster strikes.

250. *Id.* at 1530.