YOU HAVE THE RIGHT TO BE DELETED: FIRST AMENDMENT CHALLENGES TO DATA BROKER DELETION LAWS

Molly Cinnamon*

Abstract

Most people are unaware that thousands of companies, of which they have never heard or interacted, profit off of their most sensitive personal data. Data brokers amass personal data from disparate sources, such as social media sites and credit reporting agencies, and sell the resulting individualized dossiers to anyone willing to pay. The resulting data can easily be weaponized to fuel fraud scams, harassment, and stalking. But in the absence of a federal privacy law, individuals in the United States have no legal means to request that data brokers delete their most sensitive data.

California's Delete Act, SB-362, passed in 2024, aims to solve this problem by requiring all data brokers to delete residents' data upon request. This Article treats California's Delete Act as prototypical legislation, as several other states are well-poised to pass similar laws as part of their privacy framework. But celebration may be premature. Well-funded litigants, including data brokers and trade associations, will likely argue that the Delete Act violates the First Amendment by limiting the sale of personal data. Prior interpretations of privacy laws by the Supreme Court indicate that the Delete Act could indeed be vulnerable to such challenges.

This Article anticipates those challenges and finds that legislation limiting data brokers' sale of personal data is constitutional under the First Amendment. Courts should maintain this understanding of the interaction between the First Amendment and privacy legislation, lest all regulations, especially in the digital age, be interpreted as constitutional violations. Privacy protections like the Delete Act can, and do, coexist with the Constitution's protection of free expression.

---

* J.D., Harvard Law School; B.A., Harvard University. I thank Professor Laura Weinrib (Harvard Law School) for her generous guidance in evolving my early ideas into this Article, and Dean Susannah Tobin (Harvard Law School) for her steadfast support of my writing and development as a scholar.

TABLE OF CONTENTS

INTRODUCTION

Every day, hour, and minute, Americans give up their most personal data for sale. Simply by using otherwise-free online services or even having their credit checked,[1] consumers relinquish control over their own data and kick off a chain of its sale. First, companies directly collect data about users' use of their services, creating metrics about their online behaviors and identities, and then sell it to data brokers. These data brokers further enrich this user data by integrating it with other sources, such as public records or even data from other data brokers, creating databases with the inferred habits, demographics, and identifiable information of individuals.[2] Finally, data brokers sell the data to anyone willing to pay, from digital advertisers to bad actors looking to carry out fraud schemes. In the absence of privacy legislation in the United States regulating these transactions, the data broker industry is now worth nearly $300 billion.[3] Most consumers have, at best, a faint awareness of their lack of privacy on the Internet, but the effects are palpable: a Google search of one's name results in numerous sites claiming to sell a dossier containing their preferences, history, and identity.

This data can be used in a range of benign to nefarious ways. Data about user attention may help advertising companies target ads or businesses implement differential pricing on their goods and services.[4] But a nefarious actor may use information about an individual's browsing and location data to dox, stalk, or harass them. For example, many data brokers buy and sell identifying information collected by credit bureaus, including an individual's name, date of

---

[1] *See* Joseph Cox, *The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15*, 404 MEDIA (Aug. 22, 2023, 8:34 AM), https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion [https://perma.cc/C7SY-2A9U] [hereinafter *The Secret Weapon Hackers Can Use*].

[2] *Id.*

[3] *See Data Broker Market Overview,* MKT. RSCH. FUTURE (2025), https://www.marketresearchfuture.com/reports/data-broker-market-11676 [https://perma.cc/H92Z-8P2B].

[4] *See* Bob Gellman, *Differential Pricing and Privacy: Good, Bad, or Otherwise?* (Mar. 11, 2014), https://www.bobgellman.com/rg-docs/RG-Differential%20Pricing-2014.pdf [https://perma.cc/8Y89-H3NL]; Jon Keegan & Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, THE MARKUP (June 8, 2023, 6:00 PM), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you [https://perma.cc/6CQN-P6VZ].

birth, addresses, Social Security Number, and telephone numbers; on underground forums, bad actors share this information about high-profile targets to coordinate in-person or online harassment.[5]

Efforts to reclaim one's digital identity are often futile. Attempting to scrub one's Internet presence is a Hydra-like problem: although some sites allow users to request removal of their data, these hundreds, if not thousands,[6] of data broker sites continuously repopulate their offerings by re-pulling their sources. In response to consumers' desire for privacy, a new industry has sprung up: for a subscription fee, content removal services, such as DeleteMe,[7] Aura,[8] and Optery,[9] claim to wipe your name from all data broker sites through continuous removal requests. Yet, with no law enforcing deletion, many data brokers simply ignore the removal requests altogether.

The California Delete Act, SB-362, which became effective on January 1, 2024, is the first law that aims to solve this problem. Amending California's comprehensive consumer privacy law, the California Consumer Privacy Act (CCPA),[10] the Delete Act creates a mechanism for California consumers to make a single request for all data brokers to delete data held about them.[11] Anticipating that data brokers will re-pull their sources, registered data brokers are required to recurringly delete data about that individual at least once every 45 days.[12] The Act is a necessary step to restoring a sense of control over one's own data.

While California is the first state to pass a sweeping data broker deletion law, other states are likely to follow suit. California has been a leader in privacy legislation since its 2018 passage of the CCPA, the first comprehensive consumer privacy state law.[13] As of early

---

[5] *See The Secret Weapon Hackers Can Use*, *supra* note 1.

[6] Eileen Guo, *What's next for our privacy?*, MIT TECH. REV. (Jan. 7, 2025), https://www.technologyreview.com/2025/01/07/1109301/privacy-protection-data-brokers-personal-information [https://perma.cc/9E9M-Y9L8] (noting that, as of 2025, reports estimate that 4,000 to 5,000 data brokers operate worldwide).

[7] DELETEME, https://joindeleteme.com [https://perma.cc/PB58-QCFQ].

[8] AURA, https://www.aura.com [https://perma.cc/47AE-J8GU].

[9] OPTERY, https://www.optery.com [https://perma.cc/CLA7-V4SA].

[10] CAL. CIV. CODE §§ 1798.100–199.100.

[11] CAL. CIV. CODE § 1798.99.86(d)(1).

[12] *Id.*

[13] *See Frequently Asked Questions*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/faq.html [https://perma.cc/YN6Y-3SS3].

2025, twenty states have passed parallel legislation.[14] Similarly, the Delete Act is likely to be mirrored elsewhere. Indeed, other states have already recognized the risk of the unfettered and untracked sale of residents' data. Vermont, Texas, and Oregon require data brokers to register with the state, with Vermont and Oregon also requiring publication of consumer opt-out options, where those exist.[15] Mandating deletion of residents' information is the next privacy protective measure. Federal action is not out of the question, either; in fact, California's Delete Act mirrors proposed bipartisan federal legislation, the Data Elimination and Limiting Extensive Tracking and Exchange (DELETE) Act.[16]

But celebrations over passage of California's Delete Act may soon be shrouded by legal challenges that would give other states pause in passing similar legislation. Potential discontents with the Act are likely to initiate litigation early into its existence in an effort to undermine the law before any parallel acts are adopted. And powerful plaintiffs such as NetChoice, the trade association that describes their goal as promoting free speech on the Internet,[17] may be eager to take up this cause. The stakes are high: if any legal challenges are successful, not only will California's Delete Act be struck down, but other similar state legislation will be stalled, and any possibility of a federal act requiring data broker deletion will be foreclosed.

In particular, laws regulating deletion of data broker data may be vulnerable to a First Amendment challenge. First Amendment doctrine is unsettled with regard to privacy legislation. In the 2011 Supreme Court case *Sorrell v. IMS Health Inc.*, the Court struck down Vermont legislation that limited the dissemination of prescription data as a content-based and speaker-based law that did not survive heightened scrutiny.[18] *Sorrell*'s holding resulted in some

---

[14] *See* C Kibby, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (last updated Feb. 10, 2025), https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/X4SY-UKNN] [hereinafter *U.S. State Privacy Legislation Tracker*].

[15] VT. STAT. ANN. tit. 9, § 2446 (2017); TEX. BUS. & COM. CODE ANN. § 509.005; OR. REV. STAT. § 646A.593(2)(a), (3)(c)(A)–(B).

[16] S. JUDICIARY COMM., REP. ON SB 362 (Becker), 2023–24 Reg. Sess., at 14 (Cal. 2023); *see also* DELETE Act, S. 3627, 117th Cong. (2022).

[17] *About Us*, NETCHOICE, https://netchoice.org [https://perma.cc/RNY7-NRKH] ("NetChoice works to make the Internet safe for free enterprise and free expression.").

[18] Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011).

scholars portending doom for all privacy legislation.[19] Such an extreme outcome has not yet occurred: as of 2025, the CCPA and eighteen other comprehensive state privacy statutes currently stand.[20] But *Sorrell* has encouraged questioning of privacy legislation on First Amendment grounds, with mixed success since 2011.[21] In fact, a recent district court opinion revived the power of *Sorrell* in striking down privacy legislation. In 2023, in *NetChoice, LLC v. Bonta*, a district court judge in the Northern District of California granted a preliminary injunction against the California Age-Appropriate Design Code Act (CAADCA), finding that privacy legislation to be an unconstitutional restraint on free speech.[22] The Ninth Circuit disagreed, finding that several of the provisions were not conclusively violative of the First Amendment to warrant a blanket preliminary injunction.[23] Further proceedings may clarify the law here, but the district court's interpretation of the law legitimized scholars' fears about the interaction between the First Amendment and privacy law. Supported by an expansive reading of the First Amendment backed by *Bonta*, *Sorrell*, and other cases, opponents of the Delete Act may be emboldened to oppose—and succeed in—striking down privacy legislation under the First Amendment.

This Article reviews potential First Amendment challenges to the California Delete Act and finds that regulation enabling deletion of data held by data brokers does not infringe upon free speech enshrined by the First Amendment. This Article treats the Delete Act as prototypical legislation and provides an analysis that can be widely applied to parallel legislation requiring deletion of data held by data brokers. In Part I, to ground the importance of the Delete Act in protecting consumer privacy, this Article will walk through the current lack of consumer privacy protections online, as well as the legal actors who are eager to preserve this state by challenging legislation like the Delete Act. Part II describes the interaction of the First Amendment and privacy legislation in scholarship and litigation, from *Sorrell* through *Bonta*. Finally, in Part III, this Article anticipates a challenge to the Delete Act or similar legislation under

---

[19] *See, e.g.*, Jane R. Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 109 (2014) (arguing that the sale of data is protected by a First Amendment right to create knowledge, and that protection of that right "will lead to some consequences that are difficult to accept[,] . . . [including] the leveling of popular consumer privacy laws.").

[20] *See U.S. State Privacy Legislation Tracker*, *supra* note 14.

[21] *See* G.S. Hans, *No Exit: Ten Years of 'Privacy vs. Speech' Post-Sorrell*, 65 WASH. U. J. OF L. & POL'Y 19, 20–21 (2021).

[22] NetChoice, LLC v. Bonta, 692 F. Supp. 3d 924, 936–937 (N.D. Cal. 2023), aff'd in part, vacated in part, 113 F.4th 1101 (9th Cir. 2024).

[23] NetChoice, LLC v. Bonta, 113 F.4th 1101, 1122 (9th Cir. 2024).

the First Amendment and analyzes the law in light of the key decision points made by *Sorrell* and *Bonta*. This Part emphasizes the nature of "deletion," pointing to analogous elements of statutes that were upheld in the face of First Amendment challenges. In anticipating First Amendment challenges and finding that the Act survives, this Article demonstrates that the Delete Act, and any parallel legislation, can successfully give consumers rights over their own data.

I. THE DELETE ACT AS A RESPONSE TO THE NEED FOR PRIVACY LEGISLATION

Today, consumers have no control over—let alone any idea about—the invasive degree to which data about them is bought and sold. The Delete Act is California's response to this sprawling market of personal data. To ground the need for such an Act, this Part reviews the lifecycle of the data market and the role of data brokers. Then, this Part describes privacy regulations targeting this data, including the Delete Act. Finally, this Part concludes with a review of the actors who are likely to bring challenges to the Delete Act or other similar legislation as an infringement of their free speech rights.

A. WHO OWNS DATA ABOUT YOU?

In the United States, individuals have no property rights in their own data, including data about their identity, address, or location patterns.[24] Thus, when an individual visits a website, signs up for a social media company, or applies for a loan or credit card,[25] they litter the Internet with digital breadcrumbs of personal data, over which they lack control or legal rights. Data brokers' integration of this data with other data sources only makes the information about an individual available online more precise and more invasive. Consumers should be concerned about the resulting data available about them: it can fuel targeted bouts of fraud or harassment. This Section will first walk through the data lifecycle that enables the amassing of individuals' personal data, then it will turn to the real harms of the unfettered use of this data.

---

[24] *See* Carpenter v. United States, 585 U.S. 296, 398–402 (Gorsuch, J., dissenting) (suggesting that courts should grant individuals a property interest in personal data by considering their data an "effect" under the Fourth Amendment).

[25] *See The Secret Weapon Hackers Can Use*, supra note 1.

1. *The data lifecycle*

The data lifecycle is initiated by companies with whom consumers interact, or "first-party collectors." Companies collect data about users' usage of their apps, services, or devices, often making their offerings free in exchange for the ability to sell users' information to third parties as a revenue stream.[26] For example, a first-party collector that is a social media site may sell data about an individual's search terms, habits of usage, contacts in their social network, and geolocations from where they post. Buried in lengthy Terms of Service is permission for first-party collectors to collect, use, and sell users' data as they please. Yet over 90% of individuals do not read the lengthy and legalese-packed Terms of Service to which they agree.[27] Even for individuals who object to the Terms of Service, they have no negotiating power with the companies behind the services.[28] Today, it is practically necessary, personally and professionally, to have an online presence. But once users give up their data to first-party collectors, they unwittingly lose control over its future dissemination.

A third-party collector, also known as a data broker, is "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."[29] Upon purchasing first-party data, data brokers integrate it with data from disparate sources, creating detailed and invasive records about an individual's demographics, habits, and behaviors. For example, a data broker may purchase first-party data from a social media site about users' online interactions. The data broker can then integrate identifying information with financial transaction data and credit scores—acquired from another data broker—to create robust profiles of individuals' spending power. This new dataset can inform predictions about when an individual is most likely to purchase a high-ticket item. Even if the original dataset

---

[26] *See generally* JUSTIN SHERMAN, DUKE SANFORD CYBER POL'Y PROGRAM, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf [https://perma.cc/6C9L-5SWU].

[27] *See* Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements,* BUS. INSIDER (Nov. 15, 2017, 4:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/S6NV-8H35].

[28] *See id.*; *see generally* Aaron E. Ghirardelli, *Rules of Engagement in the Conflict Between Businesses and Consumers in Online Contracts*, 93 OR. L. REV. 719 (2015) (discussing Terms of Service as adhesion contracts with unconscionable terms).

[29] CAL. CIV. CODE § 1798.99.80(c).

is anonymized, integration with public records that include information such as names, addresses, contact information, and even social security numbers[30] can be used to re-identify individuals. This data can be sold to retailers to help inform differential pricing tactics. For instance, the cost of an airline ticket may be more expensive for an individual after they like a picture of a tropical beach.

The chain of integration continues on infinitely; other data brokers buy, filter, integrate, and resell this data, curating it for general or specific purposes for anyone willing to pay. The value—and invasiveness—of the datasets only increases with each integration, or each progression in the data lifecycle. And with machine learning, data brokers do not even need to own individuals' data to know personal information about them; probabilistic predictions from seemingly innocuous data can infer the behavior of individuals whose data is absent from their datasets.[31]

2. *Harmful uses of data broker data*

This data is readily available for sale. A quick search of an individual's name yields several websites selling personal information about them. The most established data brokers include Acxiom, Epsilon, Experian, and Equifax.[32] The latter two data brokers are major credit reporting agencies from whom brokering data serves as an additional revenue stream.[33] Most of these sites present as polished and professional; they suggest marketing and business-oriented uses of their data, and they require interested parties to make an account or speak to a representative to access the data.[34] But hundreds, if not thousands, of other data broker sites offer personal data with no barriers. For instance, USA People Search provides phone numbers, addresses, and relatives' information for

---

[30] *See* David S. Ardia, *Privacy and Court Records: Online Access and the Loss of Practical Obscurity*, 2017 U. ILL. L. REV. 1385, 1390 (2017).

[31] *See generally* Alicia Solow-Niederman, *Information Privacy and The Inference Economy*, 117 NW. U. L. REV. 357 (2022) (describing that today's individualized conceptions of privacy do not anticipate insights from machine learning, which create a new category of data: "information that might be about you.").

[32] *See* Margo Steines, *10 Top Data Broker Companies*, BUILT IN, https://builtin.com/articles/top-data-broker-companies [https://perma.cc/5XAH-T8DP].

[33] *See The Secret Weapon Hackers Can Use*, *supra* note 1.

[34] *See, e.g.*, ACXIOM, https://www.acxiom.com/ [https://perma.cc/PUN5-AYJ9].

free.[35] TruthFinder.com claims to have contact information, social media accounts, court records, details about assets, and photos.[36]

Data purchased from these data brokers can make for a powerful weapon. As just one example, this data can enable highly effective influence campaigns to drive the results of elections. When the Cambridge Analytica scandal broke in 2018, consumers were shocked to learn that seemingly innocuous data that they provided Facebook had been used to fuel election campaigns, including that of Donald Trump.[37] But Cambridge Analytica's data was made considerably more effective because it was integrated with data on United States consumers purchased from data brokers.[38] When combined with social media data, information available for purchase by data brokers created a powerful tool that enabled micro-targeting to influence individual voting behavior.[39] While the Federal Trade Commission (FTC) fined Facebook for failing to disclose the use of users' data for political purposes,[40] this enforcement action does not fix the underlying problem. As mentioned, Facebook and other sites can simply bury these disclosures in Terms of Service to which users blindly consent. Other campaigns of mass influence, by United States candidates or foreign adversaries, are all but certain.[41]

On an individual level, even data used for "advertising" can have nefarious uses. Uniquely identifiable data can arm bad actors with compromising information about individuals or high-value targets. For example, many data brokers segment populations based on details about individuals' race; health; psychological profiles, including medications they use; and financial circumstances, such as

---

[35] USA PEOPLE SEARCH, https://www.usa-people-search.com [https://perma.cc/342T-QYKA].

[36] TRUTHFINDER, https://www.truthfinder.com [https://perma.cc/HXU4-7LJK].

[37] *See* Margaret Hu, *Cambridge Analytica's Black Box*, BIG DATA & SOC'Y (Aug. 24, 2020), at 3, https://doi.org/10.1177/2053951720938091.

[38] *Id.* at 2.

[39] *Id.*

[40] *Id.*

[41] *See, e.g.,* Michael Kans, *Data Brokers and National Security*, LAWFARE (Apr. 29, 2021), https://www.lawfaremedia.org/article/data-brokers-and-national-security [https://perma.cc/25D4-7KFS] (discussing U.S. Intelligence admissions that China has collected, legally and illegally, large healthcare datasets from the U.S. and other nations "for purposes only it can control."); Alfred Ng, *Data broker offers access to voters likely to back Jan. 6 and right-wing militias*, POLITICO (Oct. 30, 2024), https://www.politico.com/news/2024/10/30/data-voters-political-violence-00186132 [https://perma.cc/7KP6-KVD3] (describing a data broker's sale of information about likely right-wing voters to U.S. Congress members and PACs in the runup to the 2024 Presidential election).

quantity of loans or debt.[42] Fraudsters engaged in identity theft or financial exploitation can leverage this data to manipulate their targets, gaining trust by referencing friends, family members, or personal habits.[43] The widespread availability of such information may help explain the rise in online scams targeting individuals aged 60 and over in recent years, resulting in losses exceeding $3.4 billion.[44]

The risks of data misuse go beyond financial fraud, extending into deeply personal and politically sensitive areas. One data broker claims to sell data on the comings and goings of visitors to abortion clinics.[45] Purchasers of this data can infer the identities of those seeking abortions, which, in the wake of *Dobbs v. Jackson Women's Health Organization*,[46] puts women from states with curtailed abortion rights at risk of retaliation or potential legal action.[47] To mitigate individual and societal risks, legislation must give data subjects rights to regain control over their own data.

B. ATTEMPTS TO CURB THE POWER OF DATA BROKERS

A historical lack of consumer privacy legislation has created a messy and unwieldy state of personal data in the United States. This regulatory vacuum has been exploited by thousands of data brokers to create a market worth nearly $300 billion.[48] Private companies and legislative efforts have attempted to answer consumers' demands for privacy in the face of this market.

---

[42] *See* Keegan & Eastwood, *supra* note 4 (describing a data broker's integration of nearly one-hundred different sources, many from other data brokers, to create a dataset segmenting individuals by race, political activity, and medical issues).

[43] As the California Senate Judiciary Committee pointed out in justifying the need for the Delete Act, "[e]lderly individuals are at a higher risk for scams, identity theft, and financial exploitation that rely on the collection and misuse of personal information." S. JUDICIARY COMM., REP. ON SB 362 (Becker), 2023–24 Reg. Sess., at 11 (Cal. 2023).

[44] *Elder Fraud, in Focus*, FBI (Apr. 30, 2024), https://www.fbi.gov/news/stories/elder-fraud-in-focus [https://perma.cc/3SZC-N2XC].

[45] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022, 12:46 PM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood [https://perma.cc/3DYK-Q9XP].

[46] Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022).

[47] Cox, *supra* note 45.

[48] *See* MARKET RESEARCH FUTURE, *supra* note 3.

1. *Market demand for a solution*

Some consumers, recognizing the discomfort of having their sensitive information available online, have sought solutions to reclaim a sense of privacy. Content removal services, such as DeleteMe,[49] Aura,[50] and Optery,[51] submit content removal requests to hundreds of data brokers on behalf of users. While users could submit individual removal requests themselves, manually scrubbing one's Internet presence is near-impossible because of the proliferation of data broker sites that frequently re-pull their upstream sources. These services operate on a subscription basis because they must recurringly send removal requests to account for the refreshing of data. Content removal services cost $90 to $200 per year, with prices varying based on the number of data brokers covered.[52]

Perhaps it is surprising that some data brokers even enable opt-out in the first place, given that their very existence is due to the lack of a stringent regulatory scheme. Although the United States lacks law requiring removal, many data brokers still fear legal backlash. For example, the expansive reach of the Federal Trade Commission Act (FTC Act), which bans "unfair or deceptive acts or practices in or affecting commerce," could potentially be enforced against the failure to offer an opt-out button.[53] Furthermore, if the data broker possesses data from people in the European Union, the data holder is required to follow the General Data Protection Regulation (GDPR), which requires enabling the subject of the data to request removal of their content.[54] Additionally, adding an opt-out or data correction form adds legitimacy to more polished data broker sites, reassuring customers that the data they are collecting is accurate. Still, in the absence of any directly applicable United States legislation, many data brokers simply ignore potential legal implications and do not offer an opt-out—or ignore opt-out requests. Thus, individuals who

---

[49] DELETEME, *supra* note 7.

[50] AURA, *supra* note 8

[51] OPTERY, *supra* note 9.

[52] *See* Charlie Osborne, *The Best Data Removal Services in 2025: Delete Yourself from the Internet*, ZDNET, https://www.zdnet.com/article/best-data-removal-services [https://perma.cc/Q2VF-TC9G].

[53] *See* 15 U.S.C. § 45(a)(1).

[54] Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 3(2), 7(3), 2016 O.J. (L 119) 1.

make every effort to wipe their online presence, including by using a content removal service, are often unable to do so completely.

2. *Attempted legislative solutions*

Without legal backing, content removal services can only partially solve the problem of unfettered personal data distribution online. Unfortunately, the United States altogether lacks federal consumer data privacy legislation that would give Americans control over their own data, no matter who is buying or selling it.[55] In 2022, Congress came close to passing comprehensive privacy legislation in the form of the bipartisan American Data Privacy and Protection Act, but the bill failed on questions of enforcement and preemption.[56] But efforts were revived in 2024, when a new bipartisan bill, the American Privacy Rights Act, stoked hope for the passage of a comprehensive federal privacy law.[57] But hope is a far cry from passage—as of early 2025, the bill is stalled in committee.[58]

Despite the absence of a comprehensive privacy law, Congress and federal agencies have recently turned a sharper eye to data brokers. On April 24, 2024, President Biden signed into law the "Protecting Americans' Data from Foreign Adversaries Act of 2024," limiting data brokers' ability to sell Americans' data to foreign adversaries.[59] And in September 2023, the Consumer Financial Protection Bureau (CFPB) initiated rulemaking that would

---

[55] *See* Müge Fazlioglu, *US Federal Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (last updated Aug. 2024), https://iapp.org/resources/article/us-federal-privacy-legislation-tracker [https://perma.cc/T8AL-7SPC] (discussing proposed federal privacy bills, none of which have been enacted by Congress).

[56] *See* Orion Donovan Smith, *McMorris Rodgers, House Democrats Back Compromise to Pass Historic Privacy Bill. But Will Cantwell let It Pass?*, THE SPOKESMAN-REV. (July 25, 2022), https://www.spokesman.com/stories/2022/jul/25/historic-data-privacy-law-could-be-within-reach-if [https://perma.cc/W8MT-M8WZ].

[57] *See* John Bailey, *American Privacy Rights Act of 2024: A Renewed Push for a Comprehensive National Privacy Framework*, AM. ENTER. INST. (Apr. 15, 2024), https://www.aei.org/technology-and-innovation/american-privacy-rights-act-of-2024-a-renewed-push-for-a-comprehensive-national-privacy-framework [https://perma.cc/93K6-SD97].

[58] *See* Joe Duball, *American Privacy Rights Act Markup Canceled, Next US House Steps Uncertain*, INT'L ASS'N OF PRIV. PROS. (June 27, 2024), https://iapp.org/news/a/american-privacy-rights-act-markup-canceled-next-us-house-steps-uncertai [https://perma.cc/F5FY-L2XS].

[59] *See* Making Emergency Supplemental Appropriations for the Fiscal Year ending September 30, 2024, and for Other Purposes, H.R. 815, 118th Cong. (2024) (containing the Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R. 7520, 118th Cong. (2024)).

subject more data brokers to the Fair Credit Reporting Act (FCRA), which requires covered businesses to enable consumers to dispute inaccuracies in consumer reports, which are then sold to data brokers.[60] Still, compared to countries with unified privacy legislation (such as the European Union's GDPR), the United States trails behind in establishing rights for citizens to manage their own data.

In the absence of federal momentum, twenty states have passed comprehensive consumer privacy laws, beginning with the California Consumer Privacy Act (CCPA) in 2018.[61] The CCPA gives California residents the right to know what data is being collected about them, the right to request deletion, and the right to opt out of the sale of their data.[62] However, the CCPA and other parallel state laws focus only on first-party data collection; meanwhile, third-party collectors like data brokers, who never interact with data subjects directly, are exempt from most privacy regulations.[63] Thus, under the CCPA, a California consumer who uses Facebook can request that Meta delete data about them, but they cannot make the same request of data brokers.[64]

The Delete Act fills this gap. The Act recognizes that data brokers have built businesses out of buying and selling personal data, yet data subjects have no legal recourse in ensuring their own data's

---

[60] *See Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices*, CONSUMER FIN. PROT. BUREAU (Aug. 15, 2023), https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices [https://perma.cc/Z6H7-LKVQ] [hereinafter *CFPB Remarks on Data Brokers*].

[61] *See U.S. State Privacy Legislation Tracker*, *supra* note 14.

[62] *See* California Consumer Privacy Act (CCPA), OFF. OF THE ATT'Y GEN., STATE OF CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa [https://perma.cc/EZ7K-NQB8].

[63] *See* SHERMAN, *supra* note 2626, at 2; *see also* S. JUDICIARY COMM., REP. ON SB 362 (Becker), 2023–24 Reg. Sess., at 11–12 (Cal. 2023).

[64] *See* S. JUDICIARY COMM., REP. ON SB 362 (Becker), 2023–24 Reg. Sess., at 17 (Cal. 2023) ("Though the California Consumer Privacy Act empowers individuals with a "Right to Delete" information from businesses that collect their personal information, that right is limited to that collected 'from the consumer.' Data brokers do not collect information from consumers directly, creating a loophole that leaves Californians unable to exercise this essential right and vulnerable to the risks associated with unauthorized collection, sale, and misuse.").

deletion or limited use.[65] The legislation amends the CCPA to create a single deletion mechanism in which California residents can request a one-time deletion of their data from registered data brokers.[66] Under the CCPA, these data brokers should have already registered with the state.[67] And under the Delete Act, they are required to "delete all personal information related to the consumers making the requests" at least once every 45 days,[68] with a fine of $200 per day for each act of noncompliance.[69]

The Delete Act is the first legislation of its kind. It gives consumers the right to stop the buying and selling of their own information by entities with whom they have never interacted. Given that Vermont, Texas, and Ohio have data broker registries as well, those states may not be far behind in passing similar legislation. And while a federal equivalent to California's Delete Act[70] is less likely to pass in a divided Congress, state initiatives may breathe new life into its support. However, excitement over the creation of a right of deletion from data brokers may be premature: First Amendment challenges are likely to arise from opponents of the legislation.

C. POTENTIAL CHALLENGERS TO DATA BROKER REGULATIONS

The Delete Act antagonizes several groups of well-resourced litigants. The Act impacts the core of data brokers' business models: compounded deletion requests undermine their source of revenue. Additionally, building out a deletion mechanism that meets the Act's specifications is a compliance burden. Data broker Experian lobbied for the passage of a bill that would amend the Delete Act by forcing consumers to verify each deletion request made to each data broker.[71] The amendment failed,[72] but had it passed, it would have rendered

---

[65] "Data brokers (generally businesses operating without any direct relationship with individual consumers), collect and sell this information without the knowledge of the individuals to whom the information relates. As an industry, data brokers have existed in the shadows and have largely been able to operate outside of any meaningful regulation, and until recently, public scrutiny." ASSEMB. COMM. ON PRIV. & CONSUMER PROT., REP. ON AB 1202 (Chau), 2018–2019 Reg. Sess., at 6 (Cal. 2019).

[66] CAL. CIV. CODE § 1798.99.86(a)(2).

[67] *Id.* § 1798.99.82(a).

[68] *Id.* § 1798.99.86(c)(1)(A).

[69] *Id.* § 1798.99.82(c)(1).

[70] *See* DELETE Act, S. 3627, 117th Cong. (2021).

[71] *See* S.B. 1076, 2023–2024 Reg. Sess. (Cal. 2024).

[72] The bill died when the first hearing, scheduled for April 23, 2024, was canceled at the request of the author. *See SB-1076 Data Brokers:*

the Delete Act useless in equalizing the balance of power between consumers and data brokers; it would negate the efficiency of a one-click deletion mechanism.

Trade associations whose businesses rely on data brokers are in vocal opposition to the Delete Act. Among others, the American Advertising Federation, the California Chamber of Commerce, and the Software & Information Industry Association (SIIA) opposed the bill when it was being debated in the California legislature.[73] Ironically, one ad firm, the Interpublic Group (IPG), considered using their consumer dossiers to create targeted ads aimed at California voters to mount an "opposition campaign" to the bill.[74] Notably, content removal services are not opposed to such deletion laws, which could replace their business model with a free government service. Because privacy laws have carve-outs for public records,[75] users will still pay for their deletion services—and some content removal services may be hoping to be contracted by the state to build this one-stop deletion mechanism.

Opponents are likely to frame the Delete Act as an infringement on data brokers' free speech rights by limiting what factual information they can store and share. Indeed, in 2019, Mayer Brown wrote a public memo on behalf of SIIA outlining why the CCPA was invalid under the First Amendment, claiming it restricted the dissemination of information.[76] As discussed in Part II, the CCPA was amended to quell SIIA's concerns, and their claims never amounted to litigation.[77] However, SIIA could very well repurpose these claims against the Delete Act.

NetChoice, a trade association focused on Internet free expression, is a likely foe of the Delete Act. Over the last few years, NetChoice has won First Amendment challenges against many

---

Accessible Deletion Mechanism, Results from *Bill History*, CAL. LEGIS. INFO., https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=202320240SB1076 [https://perma.cc/5ZCS-39K3].

[73] *See* S. JUDICIARY COMM., REP. ON SB 362 (Becker), 2023–2024 Reg. Sess., at 19 (Cal. 2023).

[74] *See* Alfred Ng, *Ad Firm Plans to Use People's Data in a Maneuver to Sink Data Privacy Bill*, POLITICO (Aug. 18, 2023, 2:04 PM), https://www.politico.com/news/2023/08/18/ad-giant-data-regulation-bill-00111849 [https://perma.cc/5DMA-6U2X].

[75] *See infra* Section III.A.

[76] Memorandum from Andrew J. Pincus, Mayer Brown, to Christopher Mohr, Gen. Couns., Software & Info. Indus. Ass'n 1 (Jan. 24, 2019), http://www.siia.net/Portals/0/pdf/Policy/Data%20Driven%20Innovation/Memo%20re%20CCPA.pdf [https://perma.cc/YJ4E-WPUY] [hereinafter Mayer Brown Memo].

[77] *See* discussion *infra* Section II.C.1.

Internet regulations on behalf of its members,[78] which include Meta, TikTok, and Google.[79] NetChoice's recent litigation, including *NetChoice v. Bonta*, indicates an appetite for challenging privacy laws.[80]

Major data brokers may well become members of the association, given their alignment with NetChoice's mission to "make the Internet safe for free enterprise and free expression."[81] Indeed, NetChoice has no dearth of funding to take up this cause: from 2020 to 2022, its revenue jumped from $3 million to $34 million.[82] Thus, it is only a matter of time before the Delete Act (or parallel legislation) is challenged by one of its many well-funded adversaries.

II. THE FIRST AMENDMENT AS A THREAT TO PRIVACY LEGISLATION

The roots of First Amendment challenges to privacy legislation are found in the Supreme Court's 2011 decision in *Sorrell v. IMS Health*.[83] To effectively highlight the core analytical decisions made by the Court in the majority opinion, this Part begins by reviewing the steps of a First Amendment analysis, as understood before *Sorrell*.

Speech, not conduct, is regulated under the First Amendment.[84] Thus, for the most part, if courts find that regulation targets conduct

---

[78] *See* Lily Jamali & Jesús Alvarado, *How NetChoice Became Big Tech's Ally against Social Media Regulation*, MARKETPLACE (Feb. 26, 2024), https://www.marketplace.org/shows/marketplace-tech/how-netchoice-became-big-techs-ally-against-social-media-regulation [https://perma.cc/A4E8-YAAY].

[79] *Id.*

[80] *See* NetChoice, LLC v. Bonta, 113 F.4th 1101 (9th Cir. 2024); *see also* NetChoice, LLC v. Reyes, 748 F. Supp. 3d 1105, 1111, 1114 (D. Utah 2024) (dismissing NetChoice's challenge to a state law limiting social media data collection for minors).

[81] *See Our Mission,* NETCHOICE, https://netchoice.org/about/#our-mission [https://perma.cc/U2PW-EA4T]. Additionally, NetChoice's cases are not limited to social media. *See* Chris Marchese, *Chamber of Commerce, NetChoice et al v. Franchot (Maryland),* NETCHOICE (Feb. 21, 2021), https://netchoice.org/chamber-of-commerce-netchoice-et-al-v-franchot [https://perma.cc/EF5C-YAPP].

[82] Issie Lapowsky, *The Same Big Tech Lobbying Firm is Behind the Two New Supreme Court Social Media Cases*, FAST CO. (Feb. 23, 2024), https://www.fastcompany.com/91034936/meet-netchoice-big-techs-legal-bulldog-at-the-center-of-two-major-supreme-court-cases [https://perma.cc/H78R-MH6B].

[83] Sorrell v. IMS Health, 564 U.S. 552 (2011).

[84] *See* Wisconsin v. Mitchell, 508 U.S. 476, 484 (1993).

and not speech, the law is considered outside of the reach of the First Amendment and is more likely to survive.[85] If the regulation does not turn on who is speaking or what is being expressed, it is content-neutral[86] and assessed by courts under intermediate scrutiny.[87] But if the regulation is content-, speaker-, or viewpoint-based, then courts will review it under strict scrutiny, and the law is unlikely to survive.[88] The Supreme Court is more forgiving of restrictions on commercial speech. Even though commercial speech regulations are often content-based, they are typically assessed using the *Central Hudson* intermediate scrutiny test: whether the regulation is no more extensive than necessary to serve a substantial government interest.[89] Thus, a law has a better chance of survival if it is content-neutral or commercial.

In *Sorrell*, the Supreme Court held for the first time that data privacy legislation can be struck down under the First Amendment.[90] To uphold privacy laws in the face of such First Amendment challenges, the analytical choices made by Justice Kennedy's majority in *Sorrell*, as well as follow-on cases, must be understood.

A. THE SUCCESSFUL FIRST AMENDMENT CHALLENGE IN SORRELL V. IMS HEALTH, INC.

In *Sorrell*, a data broker successfully challenged privacy legislation under the First Amendment. Vermont's Prescription Confidentiality Law prohibited pharmacies, health insurers, and similar parties from selling prescriber-identifying information.[91] The law prohibited the data's use for marketing but allowed it for other

---

[85] *But see* United States v. O'Brien, 391 U.S. 367, 376 (1968) (holding that some types of conduct are symbolic, and thus warrant First Amendment protection).

[86] *See* Reed v. Town of Gilbert, 576 U.S. 155, 164 (2015).

[87] *See* City of Austin v. Reagan Nat'l Advert. of Austin, LLC, 596 U.S. 61, 76 (2022).

[88] *See* Lamb's Chapel v. Ctr. Moriches Union Free Sch. Dist., 508 U.S. 384, 394 (1993) ("[T]he First Amendment forbids the government to regulate speech in ways that favor some viewpoints or ideas at the expense of others.") (citing City Council of L.A. v. Taxpayers for Vincent, 466 U.S. 789, 804 (1984)); *see also Reed*, 576 U.S. at 165 (holding that content-based laws receive strict scrutiny).

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

[90] Sorrell v. IMS Health, 564 U.S. 552, 579–80 (2011); *see* Hans, *supra* note 21, at 22–25 (describing decades of debates over free speech and privacy rights leading to the *Sorrell* majority opinion).

[91] *Sorrell*, 564 U.S. at 558–60.

purposes, such as "health care research."[92] IMS Health, a data broker buying and selling this data, challenged the law, claiming that it created an unconstitutional "restriction on truthful speech by information providers . . . and pharmaceutical companies on matters of public concern."[93] The Supreme Court agreed and found that the law did not pass intermediate scrutiny, striking down the law as a violation of the First Amendment.[94]

In its First Amendment analysis of the Vermont law, Justice Kennedy's majority opinion made several determinations that have impacted the assessment of privacy legislation after *Sorrell*. This section will analyze them in turn.

1. *Finding that the law impacts speech, not conduct*

Sorrell found that the sale, transfer, and use of data is speech and not conduct.[95] Relying on First Amendment cases about the regulation of the media, the Court found that "[a]n individual's right to speak is implicated when information he or she possesses is subjected to 'restraints on the way the information might be used' or disseminated."[96] The Court recognized that prescriber-identifying data is a form of factual information: "there is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes."[97] Under this argument, consumer data is First Amendment-protected speech. This statement, however, is dicta. Although this dicta was overlooked even by the dissent,[98] it has sparked varied interpretations of *Sorrell* that portend different fates for privacy legislations' constitutionality. If the dicta became a holding, then all privacy legislation would be analyzed as a restriction of speech, as such laws inherently limit the dissemination of information about individuals.

---

[92] *Id.*

[93] Brief for the Respondents at 6, *Sorrell*, 564 U.S. 552 (No. 10-779).

[94] *Sorrell*, 564 U.S. at 580.

[95] *Id*. at 570.

[96] *Id.* at 568 (quoting Seattle Times Co. v. Rhinehart, 467 U.S. 20, 32 (1984)); *see also* Bartnicki v. Vopper, 532 U.S. 514, 527–28 (2001) (finding that the publication of lawfully obtained truthful information on matters of public importance must be permissible under the First Amendment, absent "a need . . . of the highest order.").

[97] *Sorrell*, 564 U.S. at 570.

[98] *Id.* at 580–603 (Breyer, J., dissenting); Hans, *supra* note 21, at 25 n.30.

2. *Finding that the law is content-, speaker-, and viewpoint-based*

The Court found that Vermont's law was content-based because it prohibited the sale of data "subject to exceptions based in large part on the content of a purchaser's speech."[99] Those who wished to use the data for "educational communications" or "health care research" could purchase it, and those who wanted to use the data for marketing could not.[100] To the Court, this distinction was effectively a content preference.[101]

The Court found that the law was speaker-based because it disfavored pharmaceutical manufacturers, while allowing others, such as academic organizations or researchers, to use prescriber-identifying information.[102] The opinion looked to Vermont's legislative history, which illustrated that lawmakers' "express purpose . . . [was] to diminish the effectiveness of marketing by manufacturers of brand-name drugs."[103] Because the legislature explicitly disfavored certain speakers and their messages, the Court found that, in practice, the law was also viewpoint discriminatory.[104] A state "may not burden the speech of others in order to tilt public debate in a preferred direction."[105] Many commentators argue that the law's narrow exclusion of speakers, paired with the clear bias in the legislative history, was the fatal flaw of the statute, and that otherwise, it would have been upheld.[106]

3. *Applying "heightened scrutiny"*

The Court avoided a determination of whether the speech at issue was commercial and, thus, the *Central Hudson* intermediate scrutiny test should apply.[107] Instead, it explained that "[t]he First Amendment requires *heightened scrutiny* whenever the government creates 'a regulation of speech because of disagreement with the

---

[99] *Sorrell*, 564 U.S. at 564.

[100] *Id.*

[101] *Id.* at 564–565.

[102] *Id.*

[103] *Id.* at 565.

[104] *Id.*

[105] *Id.* at 578-79.

[106] *See, e.g.*, Agatha M. Cole, Note, *Internet Advertising After Sorrell V. IMS Health: A Discussion on Data Privacy & The First Amendment*, 30 CARDOZO ARTS & ENT. L.J. 283, 307 (2012) ("[T]he Court's reasoning suggests that a blanket restriction . . . would trigger a lower standard of scrutiny").

[107] *See Sorrell*, 564 U.S. at 583 (referencing Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980)).

message it conveys.'"[108] The Court did not further define the term "heightened scrutiny," but suggested it was something greater than intermediate scrutiny.[109] Still, to demonstrate that the law failed even a lower standard of scrutiny, the Court proceeded with an intermediate scrutiny analysis.[110] This choice created confusion about whether the *Central Hudson* commercial speech test was upheld after *Sorrell*.[111] Litigants and courts wondered: after *Sorrell*, are content-based laws regulating commercial speech assessed under strict scrutiny, intermediate scrutiny, or this new, undefined level of "heightened" scrutiny? This distinction matters: laws are far more likely to survive under intermediate scrutiny.

4. *Finding the statute was not appropriately drawn*

For a law to survive intermediate scrutiny under the *Central Hudson* commercial test, the court must find that the speech at issue concerns lawful activity and is not misleading, the asserted government interest is substantial, the regulation directly advances the government interest asserted, and the regulation is no more extensive than is necessary to serve that interest.[112] The Court in *Sorrell* found that the statute was not drawn to serve the privacy interest advanced by Vermont because it enabled a limitless set of speakers, excluding those engaged in marketing, to disseminate prescriber-identifying information.[113] The Court suggested that the law would have survived intermediate scrutiny if Vermont "advanced its asserted privacy interest by allowing the information's

---

[108] *Sorrell*, 564 U.S. at 566 (citing Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989)) (emphasis added).

[109] *Sorrell*, 564 U.S. at 571–72 (distinguishing the standard "commercial speech inquiry" from a "stricter form of judicial scrutiny").

[110] *Id.*

[111] *See* Ira Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861, 934 (2014) (describing that despite rejecting intermediate scrutiny as the appropriate standard of review, the Court decided the case by applying the *Central Hudson* test to the law at issue). *Compare* Bambauer, *supra* note 19, at 105 (following *Sorrell*, describing that "[d]ata disseminated in an advertisement . . . will receive the lesser protections afforded to commercial speech under the Central Hudson test just like any other advertising speech."), *with* Hans, *supra* note 21, at 29 (discussing the Court's unhappiness with the *Central Hudson* commercial speech test as evinced in Matal v. Tam, 582 U.S. 218 (2017)).

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

[113] *Sorrell*, 564 U.S. at 572–73.

sale or disclosure in only a few narrow and well-justified circumstances."[114]

5. *Justice Breyer's dissent*

In the dissent, joined by Justices Ginsburg and Kagan, Justice Breyer evaluated the Vermont law as a restriction on commercial speech and found that it passed intermediate scrutiny.[115] He evinced a general skepticism of the practice of buying and selling data, suggesting generosity at his application of even intermediate scrutiny: "the Court has found that 'sales practices' that are 'misleading, deceptive, or aggressive' lack the protection of even this 'intermediate' standard."[116] The dissent found that the intermediate scrutiny standard was met because privacy is a substantial state interest[117] which was advanced by the law because it preserved patient confidentiality: an established norm.[118] As to the legislative history that the majority found to be evidence of viewpoint discrimination, Breyer suggested that it evinced an effort to protect the public health, which falls within the state's police powers.[119]

In response to the majority's suggestion of applying "heightened scrutiny," Breyer warned of the risk of returning to the *Lochner* era: if the Court reviews all regulations through a strict scrutiny lens, then almost all regulatory programs will be struck down, as they are often speaker-based.[120] His dissent predicted the weaponization of the

---

[114] *Id.* at 573.

[115] *Id.* at 581 (Breyer, J., dissenting).

[116] *Id.* at 583–84 (quoting 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 501 (1996)).

[117] *Sorrell*, 564 U.S. at 596 ("[T]his Court has affirmed the importance of maintaining 'privacy' as an important public policy goal—even in respect to information already disclosed to the public for particular purposes (but not others)."); *see also* Dep't of Just. v. Reps. Comm. for Freedom of Press, 489 U.S. 749, 762–771 (1989) (exempting the disclosure of an FBI rap sheet from a Freedom of Information Act request because it would constitute an unwarranted invasion of personal privacy).

[118] *Sorrell*, 564 U.S. at 598 (Breyer, J., dissenting).

[119] *Id.* at 596–97.

[120] *See id.* at 585. Courts rarely find that a law passes strict scrutiny, either because the law is not narrowly tailored, or the government interest is deemed not compelling enough. Rare exceptions include Holder v. Humanitarian L. Project, 561 U.S. 1 (2010), in which the Court found that national security interests were compelling enough to uphold a law that criminalized providing terrorist groups material support in the form of speech, and Williams-Yulee v. Florida Bar, 575 U.S. 433, in which the Court found that the interest in preserving public confidence in the judiciary was compelling enough to uphold a law that prohibited judicial candidates from personally soliciting campaign funds.

Sorrell opinion to undercut privacy legislation under the justification of protecting freedom of speech.

B. SORRELL'S IMPACT ON PRIVACY LEGISLATION

Sorrell left open many questions debated by legal scholars. Scholars debated the influence of the "data is speech" dicta,[121] whether the *Central Hudson* test still applied to regulations of commercial speech,[122] and, in turn, whether most privacy legislation constituted a violation of the First Amendment. While some scholars have portended doom for privacy legislation following *Sorrell*, lower courts tell a different story—*Sorrell* has, for the most part, been read as limited to its facts.

1. *Academic response to Sorrell*

Even before *Sorrell*, some legal scholars suggested that privacy legislation is incompatible with the First Amendment. Eleven years before *Sorrell*, legal scholar Eugene Volokh framed data privacy laws as "a right to stop people from speaking about you."[123] This framing begs the question: to Volokh, information privacy laws are unlikely to pass a First Amendment strict scrutiny test.[124] Volokh argues that broadening First Amendment exceptions to uphold privacy laws will have unintended consequences, such as creating property rights in pure facts, undermining copyright laws, and limiting the dissemination of factual, time-sensitive news.[125] Thus, he "reluctantly oppose[s]" data privacy laws.[126]

---

[121] *Compare* Bambauer, *supra* note 19, at 63 (arguing that data is speech), *with* Rubinstein, *supra* note 111, at 934–35 (arguing that Kennedy's "data is speech" dicta should be read narrowly).

[122] *Compare* Ashutosh Bhagwat, *Sorrell v. IMS Health: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 858 (2012) (finding that "the Court blurred the distinction between strict and intermediate scrutiny," suggesting a reconsideration of the commercial speech doctrine), *with* Bastian Shah, *Commercial Free Speech Constraints on Data Privacy Statutes After Sorrell v. IMS Health*, 54 COLUM. J.L. & SOC. PROBS. 93, 109 (2020) (arguing that *Sorrell* did not change the commercial speech doctrine, as "heightened scrutiny" is synonymous with "intermediate scrutiny").

[123] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You*, 52 STAN. L. REV. 1049, 1049 (2000).

[124] *See id.* at 1106–07 (Volokh contests the idea that privacy is a compelling government interest, suggesting that it undermines other Constitutional rights, such as the right to free speech).

[125] *See id.* at 1078–80.

[126] *Id.* at 1053.

In the aftermath of *Sorrell*, multiple scholars echoed Volokh's ideas, reading the majority's opinion broadly. In 2012, one legal scholar published an article interpreting *Sorrell*'s dicta as a holding, calling well-established privacy-preserving laws like HIPAA into question.[127] In the same year, another scholar argued that *Sorrell*'s holding indicates that the sale of information is not commercial speech.[128] Thus, because the government's interests are not compelling enough to pass strict scrutiny, laws regulating the sale of data should be struck down. To get out of this "doctrinal box," he suggested that courts consider distinguishing factual speech and "cultural, political, and more generally idea-focused speech."[129]

But other scholars encouraged a narrow reading of *Sorrell*. Multiple scholars looked past the "data is speech" dicta[130] and identified *Sorrell*'s holding as the striking down of a content-based and speaker-based restriction on speech.[131] They argued that if the Vermont law had been crafted for uniform application, instead of exclusively banning marketing or pharmaceutical companies, then it would have been constitutional.[132] In contrast to scholars' questioning of the constitutionality of HIPAA, one scholar pointed out that despite HIPAA's singling out of marketing as a nonpermissive use of health data, HIPAA lacks the "pointedly discriminatory goal and impact of Vermont's data-mining law," and is thus viewpoint-neutral.[133] Finally, these scholars read "heightened

---

[127] Bambauer, *supra* note 19, at 96, 114 (suggesting that HIPAA's limitation on data sharing due to privacy concerns undermines effective research and thus is not properly tailored); *see also* David R. Morantz, *HIPAA's Headaches: A Call for A First Amendment Exception to the Newly Enacted Health Care Privacy Rules*, 53 U. KAN. L. REV. 479 (2005) (arguing that HIPAA's protection of key health information of public concern is in conflict with the First Amendment). Despite scholars questioning its constitutionality, HIPAA's privacy provisions have not been formally challenged under the First Amendment.

[128] Bhagwat, *supra* note 122, at 866, 872 ("For example, do individuals truly have a compelling interest in maintaining the privacy of their browsing habits, since they share those habits freely with myriad websites, and few individuals take steps to prevent those websites from tracking their clicks?") (emphasis removed).

[129] *Id.* at 856, 877.

[130] *See* Rubinstein, *supra* note 111, at 934–35.

[131] *See* Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1519 (2015); *see also* Cole, *supra* note 106, at 307.

[132] *See* Richards, *supra* note 131, at 1519; *see also* Cole, *supra* note 106, at 307.

[133] *See* Beverly Cohen, *Regulating Data Mining Post-Sorrell: Using HIPAA to Restrict Marketing Uses of Patients' Private Medical Information*, 47 WAKE FOREST L. REV. 1141, 1179 (2012).

scrutiny" as applying only to content-based commercial restrictions, preserving the *Central Hudson* intermediate scrutiny test for content-neutral laws.[134] These assessments of the *Sorrell* holding suggest that the case does not threaten future privacy legislation.

2. *Lower court application of Sorrell*

Until 2023, fears about *Sorrell* being used as a weapon to strike down data privacy legislation were largely unproven. Over the decade since *Sorrell*, laws that limited data sharing were challenged under the First Amendment and routinely upheld by lower courts.[135] Data privacy laws upheld against the backdrop of *Sorrell* include: the Fair Credit Reporting Act (FCRA), which restricts consumer reporting agencies from reporting any "adverse items of information" about a consumer;[136] the Video Privacy Protection Act (VPPA), which limits distributors of prerecorded media from disclosing consumer information to third parties;[137] Michigan's equivalent to the VPPA for video rental stores, the Video Rental Privacy Act (VRPA);[138] Maine's Act to Protect the Privacy of Online Customer Information, which requires ISPs to obtain approval from customers before selling their data;[139] and Illinois' Biometric Information Privacy Act (BIPA), which prohibits collecting biometric data without subject consent.[140] This section will analyze the common findings of courts in evaluating these laws after *Sorrell*.

a. Some content- or speaker-based distinctions are permissible.

Lower courts did not find that data privacy laws' content- or speaker-based distinctions doomed them to strict or heightened

---

[134] *See* Shah, *supra* note 122, at 109; *see also* Cole, supra note 106, at 308.

[135] *See* Zachary Shapiro, *Data Protection in The Digital Economy: Legislating in Light of Sorrell v. IMS Health Inc*, 63 B.C. L. Rev. 2007, 2038–41 (describing that privacy laws challenged post-*Sorrell*, such as in Boelter v. Hearst Communications, Inc., 192 F. Supp. 3d 427 (S.D.N.Y. 2016), have survived because courts continue to analyze them using the *Central Hudson* commercial speech test).

[136] King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303, 304 (E.D. Pa. 2012).

[137] Saunders v. Hearst Television, Inc., 711 F. Supp. 3d 24, 33 (D. Mass. 2024).

[138] Boelter v. Hearst Commc'ns, Inc., 192 F. Supp. 3d 427, 451 (S.D.N.Y. 2016).

[139] ACA Connects v. Frey, 471 F. Supp. 3d 318, 318 (D. Me. 2020).

[140] Am. Civ. Liberties Union v. Clearview AI, Inc., No. 20 CH 4353, 2021 WL 4164452, at *1 (Ill. Cir. Ct. Aug. 27, 2021).

scrutiny. The courts emphasized an inherent difference from *Sorrell*: these laws were not viewpoint discriminatory.[141] They lacked Vermont's incriminating legislative history—which lower courts emphasized as evidence of a bias animating content- and speaker-based restrictions—justifying heightened scrutiny under *Sorrell*.[142] As one lower court interpreted *Sorrell*, "[s]peaker-based distinctions should lead to strict scrutiny only if those exemptions are hiding content- or viewpoint-based preferences."[143] Thus, in the absence of discriminatory intent, data privacy laws can be evaluated under intermediate scrutiny.

In some cases, courts overlooked content- and speaker-based distinctions incidental to these laws, as opposed to purposeful distinctions created to silence certain types of speech or speakers.

For instance, in evaluating whether Illinois' BIPA is content-based, the court found that in specifically limiting biometric information, the law limits *media*, not content.[144] By contrast, "[i]f BIPA regulated, say, capture of faceprints of people yelling but not faceprints of people smiling, that would be a content-based distinction. BIPA does nothing of the sort."[145] As for speaker-based restrictions, some courts were more forgiving if the distinction targeted the speaker holding the majority of the data. For example, although Michigan's VRPA is speaker-based—prohibiting video-rental businesses from sharing customer-identifying data—the court found that it "restricts, indiscriminately, the group of individuals most likely to reveal consumer identifying information" and for that reason, among others, did not merit strict scrutiny.[146] The law in *Sorrell* allowed the sharing of data, but restricted it in narrow circumstances; by contrast, the VRPA restricts the sharing of data, and only allows it in narrow circumstances, which the *Sorrell* majority suggested was a more permissible construction of a data privacy statute.[147]

---

[141] *See King*, 903 F. Supp. 2d at 308–09; *see also Clearview AI*, 2021 WL 4164452 at *8 (referencing Sorrell, 564 U.S. at 571–72).

[142] *See King*, 903 F. Supp. 2d at 309 (quoting Sorrell v. IMS Health, 564 U.S. 552, 566 (2011)) ("It is true that content-based restrictions on protected expression are sometimes permissible . . . . Here, however, Vermont has not shown that its law has a neutral justification.").

[143] *Clearview AI*, 2021 WL 4164452 at *8.

[144] *Id.* at *7.

[145] *Id.*

[146] Boelter v. Hearst Commc'ns, Inc., 192 F. Supp. 3d 427, 446–47 (S.D.N.Y. 2016).

[147] *Id.* at 450; *see supra* Section II.A.4.

b. Data privacy laws regulate commercial speech.

Almost all courts have affirmed that *Central Hudson* is good law after *Sorrell*, applying the commercial speech standard regardless of whether the law at issue is content- or speaker-based.[148] Most lower courts found that laws regulating the buying and selling of data regulate commercial speech.[149] Commercial speech is that which "propos[es] a commercial transaction, which occurs in an area traditionally subject to government regulation."[150] The buying and selling of data does not cleanly align with this definition, compared to, for example, advertising. However, lower courts have found that—because the buying and selling of consumer data is profit-generating for businesses and facilitates follow-on commercial transactions—the disclosure of consumer data is an economic act.[151] Thus, a law regulating the selling of data by data brokers should be considered a regulation of commercial speech.

For regulations of commercial speech, courts apply intermediate scrutiny. Thus, such commercial privacy regulations should dodge strict scrutiny and have a far greater chance at surviving constitutional challenges than laws regulating non-commercial speech.

---

[148] *See, e.g.*, ACA Connects v. Frey, 471 F. Supp. 3d 318, 327 (D. Me. 2020); *Boelter*, 192 F. Supp. 3d at 447 n.10 (finding that, even if commercial speech is content-based, it should be assessed under intermediate scrutiny because the Supreme Court's ruling in Reed v. Town of Gilbert, 576 U.S. 166 (2015), which held that content-based restrictions should be assessed under strict scrutiny, did not change decades of commercial speech precedent).

[149] *See ACA Connects*, 471 F. Supp. 3d at 326–27; *Boelter*, 192 F. Supp. 3d at 445–46; Saunders v. Hearst Television, Inc., 711 F. Supp. 3d 24, 33 (D. Mass. 2024). Am. Civ. Liberties Union v. Clearview AI, Inc., No. 20 CH 4353, 2021 WL 4164452, at *7 (Ill. Cir. Ct. Aug. 27, 2021) (finding that BIPA "is subject to intermediate scrutiny because it is a content-neutral regulation that only incidentally burdens speech."). For more discussion of courts' consideration of consumer reports as commercial speech as determined in King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303, 309–12 (E.D. Pa. 2012), see Section III.B.1.iii.

[150] Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557, 562 (1980).

[151] *See Boelter*, 192 F. Supp. 3d at 445; *see also Saunders*, 711 F. Supp. 3d 24, 33 n.8 (The VPPA regulates speech "'solely motivated by the desire for profit,' which 'is a force less likely to be deterred than others,' further counseling in favor of the application of intermediate scrutiny." (citing Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 762 (1985))).

c. The laws pass intermediate scrutiny.

In evaluating intermediate scrutiny, courts found that consumer privacy is a substantial government interest.[152] Other adjacent concerns were also permissible: BIPA was justified as responding to concerns about "the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded."[153]

Courts found an appropriate fit between the government's interests and laws limiting data sharing. Even if data is available in other databases, such as public records, laws limiting data disclosures are appropriate means to protect consumer privacy. Otherwise, "[s]uch a 'cramped notion of personal privacy' ignores an individual's interest in maintaining the 'practical obscurity' of cumulative, indexed, computerized data."[154]

Thus, in practice, *Sorrell*'s holding did not undermine the constitutionality of laws limiting the sharing of consumer data. But *Sorrell* is still very much good law, and opponents of privacy legislation rely on it in an effort to strike down regulations.[155] Litigants have good reason to think that a broad reading of *Sorrell* would be appealing to courts in the wake of major decisions by the Supreme Court. In recent years, the Supreme Court has expanded the definition of "content-based laws"[156] and expressed dissatisfaction with the *Central Hudson* commercial speech test.[157] These decisions suggest an openness, if not an eagerness, to evaluating privacy

---

[152] *See Boelter*, 192 F. Supp. 3d at 447–48 ("The Michigan Legislature's stated interest in enacting the VRPA is the protection of consumer privacy. . . . This constitutes a substantial state interest." (citing Trans Union Corp. v. F.T.C. ("Trans Union I"), 245 F.3d 809, 818 (D.C. Cir. 2001) (finding that the state's interest in protecting "the consumer's right to privacy . . . is substantial"))).

[153] *Clearview AI*, 2021 WL 4164452 at *8.

[154] *King*, 903 F. Supp. 2d at 311–12 (citing U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press, 489 U.S. 749, 763 (1989)).

[155] *See* Hans, *supra* note 21, 36–37 (recounting the plaintiff's attempt to use *Sorrell* to convince the court to review the privacy regulation at issue under strict scrutiny in the case of *Clearview AI*, 2021 WL 4164452).

[156] *See generally* Reed v. Town of Gilbert, 576 U.S. 155 (2015) (expanding the notion of content-based laws by holding that laws are content-based if they require the viewer to look at content in order to determine if it is subject to regulation).

[157] *See* Hans, *supra* note 21, at 28–29 (discussing the Supreme Court's longstanding unhappiness with the *Central Hudson* test, most recently culminating in a fractured opinion in Matal v. Tam, 582 U.S. 218, 245 (2017), in which the Justices could not align on whether a commercial or non-commercial speech standard applied to the law at issue).

legislation under strict or heightened scrutiny.[158] Indeed, recent challenges to laws limiting data sharing have demonstrated an appetite to revive the broad reading of *Sorrell* that threatens privacy legislation.

C. REVIVAL OF FIRST AMENDMENT CHALLENGES TO PRIVACY LEGISLATION

As the Court expands First Amendment jurisprudence and more states pass comprehensive privacy legislation, new constitutional challenges have attempted to clarify and expand *Sorrell*'s impact.[159]

1. *Considering the CCPA as a restriction on free speech*

After the CCPA, California's comprehensive privacy legislation, was passed in 2018, the Software and Information Industry Association (SIIA) argued that the CCPA violated the First Amendment by restricting the dissemination of information, including by allowing consumers to stop first-party sale of their personal data.[160]

SIIA argued that the sale of consumer data is not in the "nature of advertising" and is thus not commercial speech.[161] Likely anticipating extension of the CCPA to regulate data brokers, SIIA's memo argues: "For example, a business that publishes and sells information for use by other businesses is producing an information-based product, but that speech is not in the nature of advertising and does not qualify as 'commercial speech.'"[162] Thus, according to the memo, the CCPA should be evaluated under strict scrutiny.[163]

---

[158] *See* Hans, *supra* note 21, at 27–30.

[159] *Cf. id.* at 20 (describing post-*Sorrell* cases that have provided clarity on how the Court may analyze privacy legislation).

[160] *See* Mayer Brown Memo, *supra* note 76, at 1, 4. Although SIIA was the recipient of this memo written by attorneys at Mayer Brown (including Eugene Volokh), the views espoused have been echoed by SIIA's President and thus can be assumed to be SIIA's own. For instance, in a 2020 press release, SIIA's President described the CCPA as containing "fatal First Amendment flaws." Press Release, Software & Info. Indus. Ass'n, CCPA Reguls. Create a Gordian Knot: Either Comply with the Unconstitutional Restrictions or Risk Expensive Enf't Actions, Says SIIA (Jun. 3, 2020), https://www.siia.net/ccpa-regulations-create-a-gordian-knot-either-comply-with-the-unconstitutional-restrictions-or-risk-expensive-enforcement-actions-says-siia/ [https://perma.cc/GA6V-8Z7E].

[161] *See* Mayer Brown Memo, *supra* note 76, at 5.

[162] *Id.*

[163] *Id.* at 6.

SIIA also argued that the CCPA is content- and speaker-discriminatory. The memo argues that the enforcement of consumers' opt-out rights is content-based: when the CCPA prohibits the sale of an opted-out individual's data, they foreclose all forums for disseminating this information.[164] Because the law in application limits speech about a specific person, it is content-based. Additionally, the CCPA is speaker-based because it "selectively burdens the speech of a subset of businesses that maintain and sell personal information."[165] If adopted, these positions would require courts to evaluate all data privacy laws under strict scrutiny, harkening back to Breyer's warning of a return to the *Lochner* era in the *Sorrell* dissent.[166] Indeed, the memo proceeds to argue that the CCPA fails strict scrutiny: "[t]he government cannot defend a speech restriction 'by merely asserting a broad interest in privacy.'"[167]

SIIA never litigated these issues. Most of their discontent hinged on the CCPA's carveout for "publicly available information" (PAI), which it alleged was vaguely defined.[168] The state legislature addressed this concern with an amendment in 2019.[169] The amendment staved off a legal challenge of the CCPA—for now. But the arguments raised by SIIA apply beyond PAI and the CCPA; they could easily be repurposed to challenge legislation like the Delete Act.

---

[164] *Id.* at 12.

[165] *Id.* at 11–12 (citing CAL. CIV. CODE § 1798.140(c)).

[166] Sorrell v. IMS Health, Inc., 564 U.S. 552, 585 (2011) (Breyer, J., dissenting).

[167] *See* Mayer Brown Memo, *supra* note 76, at 6 (citing U.S. West, Inc. v. Fed. Commc'n Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999)).

[168] Mayer Brown Memo, *supra* note 76, at 9–10.

[169] The original statute limited the sale of public government records when doing so would "not [be] compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained" without providing guidance for how to assess compatibility of purpose. CAL. CIV. CODE § 1798.140(o)(2) (2018) (amended 2024). In 2019, the legislature narrowed the definition of PAI by removing the language about uses for compatible purposes. It was also expanded to encompass "information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media" and "information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience." CAL. CIV. CODE § 1798.140(v)(1)(2) (2024). *See also infra* Section III.A.

2. *Reviving a broad reading of Sorrell in NetChoice v. Bonta*

Concerns about the reach of *Sorrell* were fully revived in late 2023, when a district court granted a preliminary injunction against enforcement of the California Age-Appropriate Design Code Act (CAADCA).[170] Among other requirements, CAADCA prohibits for-profit entities from collecting, selling, sharing, or retaining data about individuals under 18.[171] NetChoice argued that these requirements violate the First Amendment by limiting the speech of businesses.[172] The court applied *Sorrell*, stating that under its precedent, because CAADCA "restricts the 'availability and use' of information by some speakers but not others, and for some purposes but not others, [it] is a regulation of protected expression."[173] Proceeding through a First Amendment analysis, the court found that CAADCA is an unconstitutional restriction on speech.[174]

For the aspects of CAADCA's coverage that prohibited the sale of personal information, the court determined that a commercial speech test applied.[175] The opinion struggled with this determination and left room for second-guessing at later stages of the proceedings.[176] The court did not conduct a content-based analysis, finding that the *Central Hudson* test applies regardless.[177] However, the court did find CAADCA was speaker-based because it created restrictions on for-profit companies, but not governmental or non-profit entities.[178]

Nonetheless, the court found that CAADCA's restriction on collecting, selling, sharing, and retaining children's data failed intermediate scrutiny because it was not drawn to serve the stated privacy interest.[179] The court acknowledged the importance of the state's interest in protecting minors from harmful content and that the excessive collection of children's data results in harmful ad-targeting.[180] But, in limiting data collection altogether, the court

---

[170] *See* NetChoice, LLC v. Bonta, 692 F. Supp. 3d 924, 966 (N.D. Cal. 2023), aff'd in part, vacated in part, 113 F.4th 1101 (9th Cir. 2024).

[171] *Id.* at 942.

[172] *Id.*

[173] *Id.* at 944.

[174] *Id.*

[175] *Id*. at 947 (citing Hunt v. City of Los Angeles, 638 F.3d 703, 715–16 (9th Cir. 2011) (finding speech commercial because it was "directed to their products and why a consumer should buy them" and not "inextricably intertwined" with non-commercial speech)).

[176] *See Bonta*, 692 F. Supp. 3d. at 947.

[177] *Id.* at 946–48.

[178] *Id.* at 946.

[179] *Id.* at 957.

[180] *Id.* at 956.

found that CAADCA is over-expansive because it restricts neutral or beneficial content targeted to minors.[181] Thus, because the law failed intermediate scrutiny, the court enforced a preliminary injunction against CAADCA.[182]

In August 2024, the Ninth Circuit overturned the lower court, finding that only one of the provisions of the CAADCA, related to compelled speech, was likely facially unconstitutional under the First Amendment.[183] The others—including the provision limiting the collection and sale of data—require further proceedings, and the Ninth Circuit vacated the preliminary injunction for those portions of the Act.[184] Although the Ninth Circuit's ruling somewhat cabined the expansive reading of *Sorrell* employed by the lower court, only further litigation will reveal courts' assessments of the interaction between privacy legislation and the First Amendment. Still, the *Bonta* decision demonstrates the power of using *Sorrell* to threaten privacy legislation. That result is likely to embolden litigants—NetChoice among them—who hope to bring similar claims to preliminarily enjoin or strike down other privacy legislation, such as the Delete Act.

III. UPHOLDING LAWS REQUIRING DELETION IN THE FACE OF A FIRST AMENDMENT CHALLENGE

Despite scholarly and judicial questioning of whether data privacy laws limit lawful speech, laws requiring the deletion of consumers' data are constitutional under the First Amendment. Since *Sorrell*, most courts have found that privacy legislation receives, and passes, intermediate scrutiny. As this section lays out, the Delete Act can and should receive similar treatment.

After examining the text of the Delete Act, this Part conducts a First Amendment analysis by looking to post-*Sorrell* jurisprudence. Jurisprudence, in addition to healthy First Amendment policy, suggests that the Delete Act and parallel legislation will survive in the face of constitutional challenges. If courts rule that the Delete Act unconstitutionally restricts free speech, they will dangerously expand the scope of the First Amendment and significantly weaken the government's ability to protect citizens' data. The First

---

[181] *Id.* at 957.

[182] *See Bonta*, 692 F. Supp. 3d. at 957..

[183] NetChoice, LLC v. Bonta, 113 F.4th 1101, 1125 (9th Cir. 2024).

[184] *See id.* at 1123 (finding that the district court inadvertently converted NetChoice's facial challenge into an as applied challenge by focusing on social media companies; the record must be developed further to assess the validity of a facial challenge).

Amendment would become a sword to undermine the protection of citizens, not a shield to protect their free discourse.

A. THE TEXT OF THE DELETE ACT

The Delete Act requires the California Privacy Protection Agency (CPPA) to create a one-click deletion mechanism that enables residents to delete their data on registered data brokers' sites. The Delete Act defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."[185] The main provision providing legal force behind deletion reads:

> (1) Beginning August 1, 2026, after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section, the data broker *shall delete all personal information of the consumer at least once every 45 days* pursuant to this section . . .
>
> (2) Beginning August 1, 2026, after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section, *the data broker shall not sell or share new personal information of the consumer . . .*[186]

The Act contains exceptions to this provision. Most notably, data brokers are not required to delete PAI, or data that "is lawfully made available from federal, state, or local government records."[187] Additionally, data brokers are not required to comply with a deletion request if it is necessary for them to maintain the consumer's personal information in order to "[e]xercise free speech, [or] ensure the right of another consumer to exercise that consumer's right of free speech."[188] This exception was likely drafted to avoid litigation about the constitutionality of the statute under the First Amendment. But because the statute does not clarify the boundaries of "free speech"—the very issue discussed in this article—constitutional challenges are likely to arise regardless.

Because the issue of deletion has not been squarely litigated, a First Amendment analysis must rely on a close analogy: laws that limit the sharing of data. Laws that require data brokers to delete data

---

[185] CAL. CIV. CODE § 1798.99.80(c).
[186] CAL. CIV. CODE § 1798.99.86(d) (emphasis added).
[187] CAL. CIV. CODE § 1798.140(v)(2)(B)(i)(I).
[188] CAL. CIV. CODE § 1798.105(d)(4).

functionally limit the sharing of that data; data cannot be shared if it no longer exists in a data broker's database. Just as laws limiting data sharing have been considered a regulation of protected expression,[189] so too would laws requiring deletion of data. Thus, the following Section leans heavily on First Amendment jurisprudence in the lower courts that address regulations of data sharing. Of course, these opinions are not binding for a court evaluating the Delete Act, but they are instructive in developing a common interpretation of data privacy laws.

B. FIRST AMENDMENT ANALYSIS

This Section analyzes the Delete Act's constitutionality under the First Amendment, addressing the key points made by *Sorrell* and the district court in *Bonta*.[190] Although this Section specifically analyzes the Delete Act, its findings can be extrapolated to parallel laws in other states or at the federal level.

This analysis is premised on the assumption that, after *Sorrell*, a court would likely find the Delete Act regulates speech, not conduct.[191] Given that the First Amendment applies, the next step is determining the nature of the speech at issue, which determines the level of scrutiny a court applies. As this Section discusses, the lower courts' assessments of the nature of speech involved in the buying and selling of data indicates that the Delete Act regulates commercial speech. Additionally, the Delete Act's structure—against the backdrop of the CCPA and its carve-out for PAI—render the regulation content-, speaker-, and viewpoint-neutral. Given the nature of the speech at issue in the Delete Act, courts should analyze the legislation under intermediate scrutiny, or at least something less restrictive than strict scrutiny. And the Delete Act should pass intermediate scrutiny: the government has several substantial interests in regulating the retention of its citizens' data, and the Act itself is no more extensive than necessary to serve those interests.

---

[189] *See, e.g.*, NetChoice, LLC v. Bonta, 692 F. Supp. 3d 924, 944 (N.D. Cal. 2023), aff'd in part, vacated in part, 113 F.4th 1101 (9th Cir. 2024) (citing Sorrell v. IMS Health, Inc., 564 U.S. 552, 571 (2011)) (describing that a regulation that "restricts the 'availability and use' of information by some speakers but not others, and for some purposes but not for others, is a regulation of protected expression."); *supra* Section II.A.

[190] *See supra* Part III.

[191] *Sorrell*, 564 U.S. at 570 (finding that the sale, transfer, and use of data is speech and not conduct).

1. *Finding intermediate scrutiny applies based on the nature of the speech at issue.*

The level of scrutiny a court applies to a law depends on how it categorizes the speech the law regulates. While the Ninth Circuit and district court in *Bonta* assumed that commercial speech receives intermediate scrutiny,[192] a strict reading of *Sorrell* leaves room for interpretation. Post-*Sorrell*, other courts have grappled with a lack of clarity about whether heightened or intermediate scrutiny applies if a law regulating commercial speech is content- or speaker-based.[193] For this reason, scholars suggest that for a privacy law to be upheld in the wake of *Sorrell*, it must be content-, speaker-, and viewpoint-neutral.[194] Indeed, the Delete Act meets this requirement as it is a regulation of commercial speech and it is content-, speaker-, and viewpoint-neutral.

A court may be further compelled to conclude that intermediate scrutiny applies by looking to courts' treatment of the FCRA, which limits the data made available in credit reports. As this Section lays out, data brokers and credit reporting agencies sell the same data, and thus, parallel degrees of scrutiny should apply.

a. Courts will likely find that the sale of data is commercial speech, but the Delete Act could strengthen its language to lead to this conclusion.

The Delete Act limits a proposed commercial transaction for the sale of individuals' data and thus regulates commercial speech. Both pre- and post-*Sorrell*, courts have routinely agreed that the speech at issue for laws regulating the collection and sharing of data is commercial.[195] Even the district court in *Bonta*, which preliminarily

---

[192] *See Bonta,* 692 F. Supp. 3d at 941; *Bonta*, 113 F.4th at 1113.

[193] *Supra* Section II.B.

[194] *See, e.g.*, Rubinstein, *supra* note 111, at 935 ("[P]rivacy laws restricting the sale and marketing use of personal information may survive even heightened scrutiny under Sorrell provided they (1) avoid content or viewpoint discrimination by not singling out particular uses or particular groups as being subject to certain restrictions while exempting others or otherwise tilting the public debate, (2) identify a substantial government interest, and (3) use narrowly tailored means to protect privacy."); Shah, *supra* note 122, at 114.

[195] For pre-*Sorrell* cases on this issue, *see* U.S. West, Inc. v. Fed. Commc'n Comm'n, 182 F.3d 1224, 1233 n.4 (10th Cir. 1999) (determining that telephone companies' use of customer information for marketing purposes was commercial speech); Trans Union Corp. v. Fed. Trade Comm'n, 267 F.3d 1138, 1141 (D.C. Cir. 2001) (determining the consumer

enjoined the CAADCA, recognized that the Act's regulation of the sale of children's personal information likely constituted a regulation of commercial speech.[196]

The Ninth Circuit's review of the district court's opinion in *Bonta* does not undermine this argument, but it resurfaces a narrow definition of commercial speech. The appellate court only looked to CAADCA's provision compelling covered businesses to prepare a Data Protection Impact Assessment (DPIA) to identify risks of "material detriment to children."[197] Whereas the district court analyzed all of the provisions under intermediate scrutiny, the Ninth Circuit fixated on the fact that the DPIA did "more than propose a commercial transaction," to find that the DPIA provision was not a regulation of commercial speech.[198] Although the court was not addressing the provisions of CAADCA limiting availability and use of data, their narrow framing of commercial speech may revive arguments that call for a strict reading of commercial speech. Indeed, in arguing against the constitutionality of the CCPA, the SIIA memo maintained that the sale of data is the production of an information-based product, not speech in the "nature of advertising," and thus is not commercial speech.[199] While the view espoused in the SIIA memo has yet to prevail in court as applied to regulations limiting the availability and use of data, its adoption would likely be existential for the Delete Act. If the Delete Act is viewed as regulating non-commercial speech, it is more likely to receive strict scrutiny and not survive a constitutional challenge.[200]

---

reports constitute commercial speech). For post-*Sorrell* cases on this issue, *see* Sosa v. Onfido, Inc., 600 F. Supp. 3d 859, 881 (determining that BIPA's restriction on the collection of biometric information without users' consent was the regulation of commercial speech); *see also* King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303, 309–12 (E.D. Pa. 2012) (determining the consumer reports constitute commercial speech).

[196] *Bonta*, 692 F. Supp. at 947 ("The Court notes that some sections of the CAADCA, such as those prohibiting the sale of personal information . . . may well be analyzed as regulating only commercial speech.").

[197] *Bonta*, 113 F.4th at 1108.

[198] *Id.* at 1119 (quoting Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 66 (1983)).

[199] *See* Mayer Brown Memo, *supra* note 76, at 5–6.

[200] *Bonta*, 113 F.4th at 1119 (For all other commercial speech, courts must apply a form of intermediate scrutiny by asking "whether the asserted governmental interest is substantial," "whether the regulation directly advances the governmental interest asserted," and "whether [the law] is not more extensive than is necessary to serve that interest." (quoting Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980)).

To shore up the Delete Act against such a challenge, legislators may consider amending the Act to clarify that deletion means that the data broker cannot propose a sale of consumer data. This would more squarely define the speech at issue as speech that "does no more than propose a commercial transaction,"[201] guiding courts to find that the speech is commercial.

b. Courts are likely to find that the Delete Act is content-, speaker-, and viewpoint-neutral because of the Act's structure.

Based on legal assessments of other laws regulating the sale of data, courts are likely to find that the Delete Act is content-neutral. Just as BIPA's regulation of biometric data was content-neutral, so too is the Delete Act's regulation of third-party consumer data.[202] The law only limits a *type* of data, not the content of that data. By contrast, if the Delete Act only required deletion of data containing certain content, such as that of low-income populations, it would be content-based.[203]

The Delete Act is speaker-neutral due to two elements of its structure: first, the exception for PAI, and second, its backdrop of the CCPA. Legislators designed this exception for PAI in both the CCPA and the Delete Act in order to avoid running afoul of the First Amendment. Government records receive a special status because, by definition, they are public. Thus, without an exception in the Delete Act, anyone *but* data brokers could freely share information from public government records. Data brokers would be singled out as a class of speakers who could not sell this data. Before the exception was included, the SIIA memo raised this concern as a reason why the CCPA should be evaluated under strict scrutiny.[204] But with the included exception of PAI, the legislation remains speaker-neutral.

Furthermore, the Delete Act is speaker-neutral because, together with the CCPA, the requirement to delete data covers all entities that can buy or sell consumer data. The CCPA gives consumers the right to delete their data from first-party collectors, businesses with whom the consumer has a direct relationship,[205] and the Delete Act gives consumers the right to delete their data from third-party collectors,

---

[201] *Bonta*, 113 F.4th at 1119.

[202] *See* Am. Civ. Liberties Union v. Clearview AI, Inc., No. 20 CH 4353, 2021 WL 4164452, at *7 (Ill. Cir. Ct. Aug. 27, 2021).

[203] The *Clearview* court suggested that BIPA would be content-based if it limited its application to certain kinds of faceprints, such as those of people yelling or smiling. 2021 WL 4164452, at *7.

[204] *See* Mayer Brown Memo, *supra* note 76, at 4–6.

[205] CAL. CIV. CODE § 1798.105(a).

businesses with whom the consumer does not have a direct relationship.[206] The laws work in tandem to create a complete regulatory scheme that limits access to consumers' data by *all* parties. Neither first-party nor third-party businesses are singled out.

Lastly, courts will likely find that the Delete Act is viewpoint-neutral. First, unlike in *Sorrell*, its legislative history indicates no effort to craft the Act to "tilt public debate in a preferred direction."[207] Second, it is evenhanded in its application, unlike *Sorrell* and *Bonta*. In *Sorrell*, the Vermont law prevented pharmaceutical manufacturers from purchasing prescriber-identifying information but enabled academics or nonprofits to use that same data.[208] In *Bonta*, the CAADCA prevented for-profit entities from selling or purchasing children's data, but not governmental or nonprofit entities.[209] In both cases, the courts found that the uneven application of the law, without clear rationale, indicated a viewpoint preference. The Delete Act's even-handed deletion requirement, for first and third-party businesses alike, is purposefully distinct from the laws in *Sorrell* and *Bonta*.

Given this design, courts are likely to find the Delete Act to be content-, speaker-, and viewpoint-neutral. Thus, because of the nature of the speech at issue, courts should review the Act with a lesser degree of scrutiny.

c. Treatment of laws regulating deletion should parallel laws regulating consumer reports.

The Delete Act should receive intermediate scrutiny not only because it is a content-neutral regulation of commercial speech, but also because its treatment should mirror that of regulations of consumer reporting agencies. Consumer reporting agencies are analogous to data brokers; they both collect information about consumers and sell that data to other businesses.[210] But because they specifically amass credit and financial information, consumer reporting agencies operate under a regulatory structure governed by

---

[206] CAL. CIV. CODE § 1798.99.86(c)(1); *see also* CAL. CIV. CODE § 1798.99.80(c) (defining data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship").

[207] Sorrell v. IMS Health, Inc., 564 U.S. 552, 578–88 (2011).

[208] *See id.* at 564.

[209] *See* NetChoice, LLC v. Bonta, 692 F. Supp. 3d 924, 944–46 (N.D. Cal. 2023).

[210] *See List of consumer reporting companies*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/consumer-reporting-companies/companies-list/ [https://perma.cc/9KEZ-VUTV].

the FCRA and enforced by the FTC.[211] When the FCRA has been challenged under the First Amendment, courts have repeatedly assessed the law under intermediate scrutiny.[212]

Both before and after *Sorrell*, courts have upheld the statute's limits on disclosures of consumer reports, finding they survive intermediate scrutiny.[213] Consumer reporting agencies challenged these restrictions under the First Amendment, concerned about the impact to their businesses.[214] In the 2001 case *Trans Union Corp. v. F.T.C.*, the D.C. Circuit upheld the FCRA's limitation on the sale of consumer reports to marketers.[215] In the 2012 case *King v. Gen. Info. Servs., Inc.*, a district court upheld FCRA's requirement that consumer reports exclude "adverse items of information" from seven years or earlier.[216]

In both cases, the courts evaluated the respective sections of the FCRA under intermediate scrutiny. But they grappled with applying a lower degree of scrutiny for factual speech; just months before *Trans Union*, the Court had upheld the ability of newspapers to publish factual information, even if it was originally illegally obtained.[217] To distinguish the consumer report context from that of newspapers, the *Trans Union* court established a distinction of public versus private speech.[218] The opinion described that "[p]rivacy-based restrictions on the publication of truthful information" will be struck down when the speech at issue is a "matter of public concern."[219] By contrast, consumer reports warrant less rigorous First Amendment protection because their speech is of "purely private concern": according to the court, factual information generated by consumer reports is shared only between the consumer reporting agencies and

---

[211] Most data brokers are currently not covered by the FCRA because they sell data that is not just for the purpose of evaluating consumer credit information. *See* 15 U.S.C. § 1681(f).

[212] Trans Union Corp. v. Fed. Trade Comm'n, 267 F.3d 1138, 1143–44 (D.C. Cir. 2001); King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303, 310–13 (E.D. Pa. 2012).

[213] *See* cases cited *supra* note 12 (finding in both cases that the FCRA's restrictions on the dissemination of consumer reports withstand First Amendment challenges).

[214] *Trans Union*, 267 F.3d at 1140; *King*, 903 F. Supp. 2d at 304–05.

[215] Trans Union I, 245 F.3d 809, 812 (D.C. Cir. 2001). The consumer reporting agency Trans Union sold consumers' data to marketers such that they could target them "by mail or telephone to offer them goods and services."

[216] *King*, 903 F. Supp. 2d at 304.

[217] *See* Bartnicki v. Vopper, 532 U.S. 514, 526–27 (2001).

[218] *See Trans Union*, 267 F.3d at 1141–42.

[219] *Id.* at 1140–41 (citing Pet. at 5–6).

their customers for the purpose of making business decisions.[220] *King* agreed that consumer reports are private speech: "consumer reports are made available to the paying subscriber only. As such, the private nature of these consumer reports does not significantly contribute to public dialogue."[221]

In recent years, this justification has become a fiction. Credit bureaus, including Trans Union, can sell "credit headers," or a subset of a full credit report, to third parties without triggering the FCRA.[222] This credit header information includes all information about a consumer, such as their name, current and prior addresses, social security number, and telephone number, other than from whom they have borrowed money. [223] Many data brokers purchase credit header information. For instance, Immigration and Customs Enforcement (ICE) uses similar data that flows through Equifax, and then is sold to data brokers, in order to better identify individuals.[224]

Ironically, in *Trans Union*, the court emphasized that Trans Union's restrictions preventing customers from broadly sharing consumer reports made that data "private speech."[225] Yet today, Trans Union is one of the credit reporting agencies selling credit headers.[226] Any assumption that consumer reports exist only between consumer reporting agencies and their purchasers is no longer accurate. Functionally, the distinction between credit reporting agencies and data brokers has collapsed.[227] Thus, courts should apply the same level of scrutiny to laws regulating consumer reporting agencies as laws limiting data brokers.

---

[220] *Id.* at 1140 ("In *Dun & Bradstreet,* the Supreme Court held that a consumer reporting agency's wholly false credit report warranted only qualified constitutional protection because the report 'concern[ed] no public issue.'" (citing Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 762 (1985))).

[221] *King*, 903 F. Supp. 2d at 307.

[222] *See The Secret Weapon Hackers Can Use*, *supra* note 1.

[223] *Id.*

[224] *Id.*

[225] *See Trans Union*, 267 F.3d at 1141–42 (determining that Trans Union's marketing lists generated from consumer reports concern are "private speech" in part because "Trans Union's target marketing lists interest only Trans Union and its target marketing customers, and Trans Union sells its lists for one-time use, prohibiting purchasers from disseminating the data.").

[226] *See The Secret Weapon Hackers Can Use*, *supra* note 1.

[227] The CFPB has recognized this collapse. They are considering rulemaking that would fold some data brokers under the definition of consumer reporting agency, forcing compliance to the FCRA. *See CFPB Remarks on Data Brokers*, *supra* note 60.

Applying the same level of scrutiny to the sale of data by consumer reporting agencies and data brokers yields two potential outcomes. First, a court could update the meaning of "private speech," as used in *Trans Union*, to reflect the modern era. If "public" data is limited to PAI, which is generated by public government records,[228] then all other forms of data are "private" speech and not a matter of public concern. In other First Amendment contexts, courts have protected the privacy interests of factual speech, even if disclosure would be in the public interest. In 2021, in *Americans for Prosperity v. Bonta*, the Supreme Court struck down a California law requiring tax-exempt charities to disclose the names and addresses of their biggest donors, finding that it violated the First Amendment by chilling donors' association rights.[229] The Court wrote that "[e]very demand that might chill association . . . fails exacting scrutiny."[230] As *Americans for Prosperity* recognized, privacy, even at the expense of disclosing factual information, is critical to enable free association. Freely available invasive data about consumers, which can include details about the medication they take or their sexual preferences,[231] presents a similar, if not more immediate, risk of chilling association. Although *Americans for Prosperity* examined regulation of nonprofits, and the Delete Act targets commercial relationships, courts should carry the same reasoning from the compelled disclosure context to the data privacy context for consistency's sake. Just like the FCRA, the Delete Act should be considered a regulation of private speech, and intermediate scrutiny should apply.

Alternatively, a court could find that all data handed over to companies by consumers is "public." In turn, courts would likely find that any restrictions on most consumer data limits speech and thus likely constitute a First Amendment violation. This would invite constitutional challenges to decades-old privacy laws like the FCRA and HIPAA.[232] To maintain consistency in First Amendment jurisprudence and avoid the erosion of decades-old laws regulating data on and offline, courts should find that consumer data, whether sold by consumer reporting agencies or data brokers, is private speech, and thus, intermediate scrutiny applies.[233]

---

[228] *See* CAL. CIV. CODE § 1798.140(v)(2).

[229] *See* Ams. for Prosperity Found. v. Bonta, 594 U.S. 595, 615, 618 (2021).

[230] *Id.* at 615.

[231] *See supra* Section I.A.2.

[232] *See* Bambauer, *supra* note 19, at 61.

[233] *See* Bhagwat, *supra* note 122, at 874–77 (arguing that to get out of the "doctrinal box" in which all data privacy regulations are struck down,

2. *Applying intermediate scrutiny*

Courts are likely to find that the Delete Act passes intermediate scrutiny because it is no more extensive than necessary to serve a substantial governmental interest. [234] In writing the Act, the California legislature explicitly identified several interests, including consumer privacy and protection against fraud, that other courts have identified as "substantial." As this Section describes, courts are likely to recognize other governmental interests in the law's passage, including the strengthening of national security. Finally, the opt-in structure of the deletion mechanism renders the Delete Act no more extensive than necessary to serve these substantial interests.

a. The government has several substantial interests in regulating data brokers' data deletion.

Courts have repeatedly recognized several of the government interests advanced by the Delete Act as substantial. First, the California legislature explicitly aimed to advance consumer privacy in passing the Act.[235] Several courts have found privacy to be a substantial government interest.[236] Indeed, even the *Sorrell* majority recognized the criticality of privacy in a digital age: "The capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."[237] In particular, the Delete Act's authors recognized the particular privacy invasion that occurs when an individual has no direct relationship with a company, yet they can buy and sell data about them.[238] In legislative history, lawmakers explained that the Delete Act patches a hole in the CCPA that prevents data subjects from exercising their right to delete against

---

courts need to recognize that "factual speech requires a distinct analytical approach different from the traditional protections provided to cultural, political, and more generally idea-focused speech").

[234] *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N. Y., 447 U.S. 557, 566.

[235] *See* S. JUDICIARY COMM., REP. ON SB 362 (Becker), 2023–24 Reg. Sess., at 7–8 (Cal. 2023).

[236] *See, e.g.*, Trans Union I, 245 F.3d 809, 818 (D.C. Cir. 2001) (finding "no doubt" that the government's interest in protecting "the consumer's right to privacy . . . is substantial"); Sosa v. Onfido, Inc., 600 F. Supp. 3d 859, 882 (N.D. Ill. 2022) (finding that "Illinois has a substantial interest in protecting consumers, and more specifically, protecting their privacy in and control over their biometric data").

[237] Sorrell v. IMS Health Inc., 564 U.S. 552, 579 (2011).

[238] *See* S. JUDICIARY COMM., REP. ON SB 362 (Becker), 2023–24 Reg. Sess., at 1 (Cal. 2023).

data brokers.[239] Legislators described that this gap "leaves Californians unable to exercise this essential right and vulnerable to the risks associated with unauthorized collection, sale, and misuse."[240] The Delete Act directly advances the government interest in privacy by allowing consumers to limit their online personal information.[241]

Additionally, the Delete Act's authors explicitly recognized another interest—protecting against the downstream harms of a lack of digital privacy.[242] This includes harassment, discrimination, identity theft, financial exploitation, among others.[243] Limiting one's personal data online alleviates this risk. Similarly, Illinois' BIPA was upheld because the enacting legislature found that compromised biometric data puts an individual at risk for identity theft, and the statute alleviated this harm by reducing the sharing of such information.[244]

The government has another substantial interest in regulating data brokers, even if not explicitly identified by the Delete Act or its legislative history. Laws regulating digital privacy help protect national security. The unfettered buying and selling of personal information pose not only a personal privacy risk but also a national security risk. Data about biometrics, geolocation, search history, and demographics enable adversaries to plot targeted attacks against the United States and its people. For instance, terrorists can purchase aggregated geolocation data to determine the most common public transportation routes at rush hour, allowing them to plan an attack to maximize devastation. Sensitive data is already available to adversaries—as one report concluded, military personnel records sold by data brokers could be used to blackmail senior military leaders over threatened public dissemination of private health information.[245]

If California legislators had identified this interest in their framing of the Delete Act, they would have found a loophole to the First Amendment challenges discussed in this article. Even if a court

---

[239] *Id.* at 17.

[240] *Id.*

[241] *See Sosa*, 600 F. Supp. 3d at 882–83 ("For [the 'directly advances'] prong to be met, the harms identified by Illinois must be real and the restriction at issue must in fact 'alleviate them to a material degree.'" (quoting Fla. Bar v. Went for It, Inc., 515 U.S. 618, 625–226 (1995))).

[242] *See* S. JUDICIARY COMM., REP. ON SB 362 (Becker), 2023–24 Reg. Sess., at 11 (Cal. 2023).

[243] *Id.*

[244] *See Sosa*, 600 F. Supp. 3d at 884 (finding that BIPA's limit of the collection and sharing of biometric information was no more extensive than necessary to serve the substantial governmental interest of privacy).

[245] *See* Sherman, *supra* note 2626, at 11.

determines that the legislation should be evaluated under strict scrutiny, rendering it unlikely to survive, the Supreme Court has recognized the government's national security as an interest so compelling that a law designed to that end is more likely to be upheld. For example, in *Holder v. Humanitarian Law Project*, the Court upheld a law limiting forms of speech to terrorist groups because of the government's national security interest.[246] If the Delete Act is amended to capture this intent, it would likely survive an analysis of any scrutiny.

However, this strategy bears risk for the long-term sanctity of the First Amendment. It opens the door for limiting speech under the justification of "national security," which can take on a shifting definition. But in addition to other arguments, framing privacy laws as national security tools is a powerful lens by which to motivate courts to uphold laws requiring data broker deletion. It is just one of many substantial government interests for which the Delete Act should be upheld.

b. The Delete Act passes intermediate scrutiny because it is no more extensive than necessary to serve these government interests.

Compared to the structure of other privacy laws, courts will likely find that the design of the Delete Act's deletion mechanism minimizes the restriction of protected speech. The Act's opt-out scheme is less restrictive of protected speech than opt–in consent schemes upheld after *Sorrell*. If the Delete Act was opt-in, California consumers would have to visit the deletion portal to affirmatively express that they consent to data brokers selling their data; by contrast, the Act requires consumers to visit the site to request removal of their data. Because opt–in schemes require explicit agreement from users for information to be shared, they are more restrictive of the dissemination of consumers' data.

Nonetheless, lower courts have upheld multiple data sharing laws that require opt–in consent: the U.S. District Court of the Southern District of New York upheld the VRPA, which only allowed the disclosure of consumer-identifying video rental information with consent;[247] the Circuit Court of Illinois found that BIPA's requirement of opt-in consent was a reasonable solution to

---

[246] Holder v. Humanitarian L. Project, 561 U.S. 1, 33–34 (2010). In fact, the Court sidestepped a strict scrutiny analysis because the "evaluation of the facts by the Executive, like Congress's assessment, is entitled to deference" on the issue of national security.

[247] Boelter v. Hearst Commc'ns, Inc., 192 F. Supp. 3d 427, 449 (S.D.N.Y. 2016).

"return control over citizens' biometrics";[248] and the U.S. District Court of the District of Maine upheld a state privacy law that prohibits providers of broadband Internet access from sharing customers' data unless the customer expressly consents.[249] By contrast, CAADCA, the law at issue in *Bonta*, features no opt–in or opt–out provision.[250] It is an even more restrictive approach to speech, limiting companies from collecting or sharing data about children with no user-determined exception. Although not explicitly stated, perhaps this design choice animated the *Bonta* court's finding that this CAADCA provision failed intermediate scrutiny.[251] Thus, laws that call for an opt-out scheme, like the Delete Act and the CCPA,[252] are likely to be upheld, as they are less restrictive by avoiding a blanket-ban on speech.

Looking to jurisprudence following *Sorrell*, courts are likely to find that the Delete Act is a content–neutral regulation of commercial speech that passes intermediate scrutiny. Thus, the Delete Act and any parallel legislation modeled after it are likely to be upheld under the First Amendment. As laid out in this Section, if courts find otherwise, they risk harming fundamental applications of First Amendment law that have enabled decades–old laws to exist. The result would weaponize the First Amendment to attack individual privacy on and offline, rather than deploy it to protect freedom of association and expression.

CONCLUSION

Despite concerns generated by *Sorrell* and *Bonta*, not all privacy legislation is doomed to unconstitutionality. Indeed, as this Article demonstrates, the Delete Act and other laws requiring deletion of consumer data by third parties are likely constitutional under the First Amendment.

This outcome is not only jurisprudentially required, but it is also called for by potential downstream effects of striking down such legislation. Striking down the Delete Act would be a jurisprudential

---

[248] Am. Civ. Liberties Union v. Clearview AI, Inc., No. 20 CH 4353, 2021 WL 4164452, at *9 (Ill. Cir. Ct. Aug. 27, 2021).

[249] ACA Connects v. Frey, 471 F. Supp. 3d 318, 322, 331 (D. Me. 2020).

[250] Cal. Age-Appropriate Code Design Act, 2020 Cal. Stat. ch. 320, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273 [https://perma.cc/8N88-4KJW].

[251] *See* NetChoice, LLC v. Bonta, 692 F. Supp. 3d 924, 961 (N.D. Cal. 2023), aff'd in part, vacated in part, 113 F.4th 1101 (9th Cir. 2024).

[252] CAL. CIV. CODE § 1798.120(a). The CCPA possesses an opt-out scheme requiring first-party collectors to comply when consumers ask them to stop sharing their data.

shot across the bow of a return to the *Lochner* era[253]—this time, digital.[254] All privacy legislation, from the CCPA to HIPAA to the FCRA, would be evaluated under strict scrutiny. In removing legislation regulating the buying and selling of personal data, courts would be instructing consumers that they have only one opportunity to protect their data—refusing the Terms of Service at the site of first-party collection. But in the absence of government regulations, failure to sign Terms of Service may mean a user cannot use the service at all. Yet these services are required to be participants in modern life.

The stakes are high. Failure to uphold legislation like the Delete Act would fundamentally weaken the position of individuals in protecting their data privacy, communicating that the United States does not uphold privacy as a valuable interest. As outlined in this Article, defenders of the Delete Act have a strong argument that the required deletion of data broker data indeed comports with the First Amendment in strengthening consumers' online protections. Such legislation is necessary to restore a sense of ownership over one's own digital identity, demonstrating that in the United States, you do indeed have the right to be deleted.

---

[253] Sorrell v. IMS Health Inc., 564 U.S. 552, 602–603 (2011) (Breyer, J., dissenting).

[254] *See* Richards, *supra* note 131, at 1529–31.