INTERNET ADVERTISING AFTER *SORRELL V. IMS HEALTH*: A DISCUSSION ON DATA PRIVACY & THE FIRST AMENDMENT

INTRODUCTION

Over the past decade, ad-targeting technology has revolutionized Internet advertising and the monetization of online content. In 2011, Internet advertising revenues in the United States totaled $31.7 billion.[1] Display advertising on the Internet—the vast majority of which is "targeted" to consumers using various types of data and web analytics—accounted for 35%, or $11.1 billion, of total online advertising revenues.[2] At 22% year-over-year growth, online advertising revenues continue to grow at a phenomenal pace while advertising revenues from other sectors of the media economy, such as television, newspapers, and magazines, lag by comparison.[3] Much

---

1 INTERACTIVE ADVER. BUREAU, IAB INTERNET ADVERTISING REVENUE REPORT: 2011 FULL YEAR RESULTS 4 (Apr. 2012), *available at* http://www.iab.net/insights_research/industry_data_and_landscape/adrevenuereport.

2 *Id.* at 12.

3 "Internet advertising revenues for the full year of 2011 increased 22 percent over 2010." *Id.* at 4. Stuart Elliott, *Last Year Was a Good Year for Ad Spending, Report Finds*, MEDIA DECODER, N.Y. TIMES (Mar. 17, 2011, 8:00 AM), http://mediadecoder.blogs.nytimes.com/2011/03/17/last-year-was-a-good-year-for-ad-spending-report-finds ("'While television media have recouped their losses from the 2009 advertising downturn,' said Jon Swallen, senior vice president for research at the Kantar Media North America unit of Kantar Media, 'several other large

of this growth can be attributed to the emergence of sophisticated ad-targeting technology, which leverages data to increase the effectiveness and value of advertising on the Internet.

Unfortunately, targeted Internet advertising can present a threat to consumer privacy because it thrives on pervasive data collection methods that are not widely understood by the public. Data collection and use practices tend to occur seamlessly in a manner that is invisible to most consumers on the Internet.[4] As a result, "consumers often are unaware of when their data is being collected or for what purposes it will be used."[5] The general lack of clarity in many companies' privacy policies adds to this confusion.[6] In fact, survey data shows that consumers often express privacy preferences that run counter to their understanding of data collection and use practices.[7] To make matters worse, the threat to consumer privacy is aggravated by dubious, deceptive and otherwise questionable tactics employed by a handful of bad actors to collect and disseminate data about individuals without their knowledge or consent.[8] These concerns have prompted public interest advocacy groups and law enforcement agencies to investigate data collection methods associated with ad-targeting technology in recent years.[9]

There is no comprehensive federal law that governs consumer privacy on the Internet in the United States, but most experts agree that regulation is needed.[10] After repeated calls from public interest groups, legal scholars, and a handful of government agencies, legislative efforts to create a new regulatory framework are finally gaining ground.[11] However, a recent Supreme Court decision, *Sorrell v. IMS Health Inc.*, may call into question the constitutionality of pending legislation.[12]

In *Sorrell*, the Supreme Court held that a state statute restricting pharmaceutical marketers' access to and use of prescription data for advertising purposes violated the First Amendment.[13] At the highest level of abstraction, the *Sorrell* case was about the implementation of data in an advertising context. This led commentators to draw analogies between the statute in

---

segments are still 15 to 20 percent below their 2008 peak.'").

4 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 25 (Dec. 2010), *available at* www.ftc.gov/os/2010/12/101201privacyreport.pdf.

5 *Id.* at 25–26.

6 *Id.* at 26.

7 *See id.* at 25–26, 29–30.

8 For a series of articles and interactive features documenting the near-pervasive use of Internet-tracking technology and privacy implications for consumers, see *What They Know*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Mar. 30, 2012).

9 *See e.g.*, Press Release, U.S. Pub. Interest Research Grp., Consumer and Privacy Groups Warn Online Tracking at "Alarming Levels" (May 3, 2010), *available at* http://www.uspirg.org/news/usp/consumer-and-privacy-groups-warn-online-tracking-alarming-levels; *Consumer Privacy*, FTC BUREAU OF CONSUMER PROTECTION, http://business.ftc.gov/privacy-and-security/consumer-privacy (last visited Mar. 30, 2012).

10 *See* DEPT. OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY, (Dec. 2010), *available at* http://www.commerce.gov/node/12471; FTC, *supra* note 4.

11 *See infra* notes 93–107 and accompanying text.

12 Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

13 *Id.* at 2668–72.

Sorrell and efforts to regulate other types of data-driven advertising—particularly targeted Internet advertising.[14] As a result, speculation about *Sorrell*'s implications for targeted Internet advertising and its potential impact on legislative efforts proliferated from the day the complaint was filed in district court, and continued to grow as the case made its way to the Supreme Court.[15]

In the aftermath of the Supreme Court decision, commentators continue to disagree over the scope of *Sorrell* and its application to forthcoming consumer privacy legislation.[16] Some claim that *Sorrell* preempts the majority of current proposals to enact comprehensive consumer privacy legislation, while others argue that *Sorrell* was narrowly decided, and hinged upon issues that are not present in recent legislative proposals.

Given the centrality of targeted advertising to the Internet economy, it is no surprise that data miners, marketers, media companies, and other interested parties favor an interpretation of *Sorrell* that immunizes data-driven ad-targeting technologies from regulation; but such an interpretation distorts the Supreme Court's opinion at the expense of consumer privacy interests by treating the decision as a broad shield to regulation in all data-driven enterprises.

This Note examines the scope of *Sorrell v. IMS Health*, its potential impact on legislative efforts to enact comprehensive consumer privacy legislation, and its implications for targeted Internet advertising. Part I provides a general overview of ad-targeting technology, emphasizing the tension between its capacity to fuel economic growth and its tendency to neglect consumer privacy interests. Part II traces the development of growing public concern over consumer privacy, subsequent proposals to enact legislation, and the proliferation of widespread speculation about *Sorrell*'s impact upon such legislative reform. Part III goes beyond the hype around the case to provide a detailed analysis demonstrating why *Sorrell* does not preempt current legislative proposals to enact consumer privacy. Finally, this Note concludes that policymakers should embrace *Sorrell* as a blueprint for formulating regulations that strike an appropriate balance between freedom of expression and consumer privacy interests.

I. TARGETED ADVERTISEMENT: MONETIZING DATA ON THE INTERNET

Though ad-targeting technology is a relatively recent development in Internet advertising, the concept of "targeted" advertising is certainly not a new one. The practice of collecting data for the purpose of targeting advertising messages to specific audiences predates the advent of the Internet and web technologies.[17]

---

14 *See infra* Part II.
15 *Id*.
16 *Compare* Julin, *infra* note 157, *with CDT Statement on Supreme Court Decision in* Sorrell v. IMS Health, CENTER FOR DEMOCRACY AND TECHNOLOGY (June 23, 2011), https://www.cdt.org/pr_statement/cdt-statement-supreme-court-decision-sorrell-v-ims-health.
17 *See generally* Lawrence C. Lockley, *Notes on the History of Marketing Research,* J. MARKETING, Apr. 1950, at 733–36.

Marketers began to use research and data to tailor advertising messages and target appropriate audiences starting in the 1960s.[18] Viewed in this light, online ad-targeting is simply a new tool in the longstanding history of direct marketing.[19]

The term "ad-targeting," with respect to online advertising, is used in reference to a set of practices that make it possible for marketers to target specific consumers with advertising messages as they use the Internet.[20] This process involves three basic steps: collection, analysis, and implementation. First, data is collected from Internet users in order to identify characteristics that could be appealing to potential advertisers.[21] For example, information such as the region where a user lives, a user's occupation or income range, or the last three sites a user visited can be very useful information for an advertiser. Second, the data is analyzed so that it may be organized, segmented, and packaged with web inventory to be sold by publishers and other ad-supported websites.[22] This practice is commonly referred to as "data mining."[23] Finally, the data is used by ad-serving entities to target the appropriate users.[24] At this juncture, the previously collected data is layered against web traffic data in an online advertising operations system that delivers the advertisement to designated Internet users.[25] Not all targeting is the same. Advertisers, marketers, and publishers employ various types of targeting techniques to refine their audience. These methods vary in purpose, as well as how the relevant data is collected, organized, and implemented to reach the appropriate audience.

Demographic advertising employs static data that a user typically volunteers to a website. For example, when a customer clicks the link to register for the online edition of *The Wall Street Journal,* the customer is taken to a screen where she can voluntarily disclose personal information including her occupation, income, and interests. *The Wall Street Journal* subsequently uses this data to target relevant advertising to her. If she discloses her occupation as an attorney, she is much more likely to see advertisements for Westlaw

---

18 *A History of Success*, TNS GLOBAL MARKET RESEARCH, http://www.tnsglobal.com/tns/history (last visited Mar. 30, 2012) (explaining the creation of the five major market research companies from 1965 which later formed the basis of Taylor Nelson Sofres (TNS) group).

19 Direct marketing is a method of advertising that involves direct communication with customers via targeted email programs, traditional direct mail and telemarketing. *Direct Marketing,* OGILVY AND MATHER, http://www.ogilvy.com/Capabilities/Direct-Marketing.aspx (last visited Oct. 1, 2011).

20 *See The Tracking Ecosystem*, WALL ST. J., *available at* http://graphicsweb.wsj.com/documents/divSlider/ecosystems100730.html (last visited Mar. 30, 2012).

21 *See id.*

22 *See* Dave Williams, *Connecting the Data Dots on Facebook and Beyond*, ADAGE (Jan. 6, 2011), http://adage.com/article/digitalnext/marketers-facebook-audience-data/229244.

23 For an overview of commercial data-mining processes, see Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 71–81 (2003).

24 *The Tracking Ecosystem*, *supra* note 20; Doubleclick, a subsidiary of Google, is the most prominent ad serving business in the market. For more information, see *Doubleclick: The Technology Foundation for Advertising*, DOUBLECLICK, http://www.google.com/doubleclick/index.html (last visited Oct. 20, 2011).

25 *See The Tracking Ecosystem*, *supra* note 20.

products than someone who identifies themselves as an accountant. In this scenario, the use of demographic data for ad-targeting purposes seems to benefit all three parties involved—it benefits the advertiser by targeting only relevant audiences and thereby maximizing the efficiency of its campaign; it benefits the publisher by making its web inventory more appealing to advertisers; and finally, it benefits the customer by tailoring her advertising content to her professional interests.

However, not all data collection practices are so innocuous. Some websites require the disclosure of personal information in exchange for access to content, calling into question whether that information is disclosed on an entirely voluntarily basis. Moreover, data disclosed to one entity might later be shared with another entity or packaged and sold to several entities, unbeknownst to the user. In fact, some services even specialize in the niche business of collecting and aggregating such data from multiple websites, and selling it to marketers and ad-supported websites that use the data for ad-targeting purposes.[26]

Behavioral targeting differs from demographic targeting in that it uses dynamic data, which is typically derived from a user's online activities. "Behavioral advertising" is often mistakenly used as a blanket term to describe all forms of online ad-targeting. This fails to acknowledge the distinct data collection methods involved, which are critical to understanding how shifting legal standards might affect different types of online ad-targeting.

Websites generate data for behavioral targeting by "tracking" users with cookies. A "cookie" is an identifying number assigned by a website to each user. Cookies enable websites to track and remember users' page visits, products stored in the user's cart, and other information such as an individual's username and billing address.[27] Data generated through the use of cookies is also frequently employed to generate inferences about a user's receptiveness to a particular advertising message based on that user's online behavior. Cookies can also be shared between sites and used to track users from site to site.[28] Cookies typically remain on a computer and continue to recognize a user's information until they are deleted from the user's browser.[29] The majority of people who use the Internet, however, do not have a good understanding of what a cookie is, when cookies might be added to their browsers, or how to remove them from their browsers, raising privacy issues.[30]

---

26 BlueKai and Interclick are examples.

27 Video: *A Guide to Cookies, What They Know*, WALL ST. J., http://online.wsj.com/video/how-advertisers-use-internet-cookies-to-track-you/92E525EB-9E4A-4399-817D-8C4E6EF68F93.html (last visited Oct. 1, 2011) (comparing behavioral targeting to getting "great customer service at a café where the barista remembers your name and your drink").

28 *See id*.

29 Though users can block or remove cookies from their browsers, "it is not possible to block all cookies without losing the ability to log into many sites and perform transactions with others." In addition, "Local Stored Objects" (also known as "Flash Cookies"), are more difficult to block or clear from one's browser. *Web Browsers,* ELECTRONIC FRONTIER FOUND., https://ssd.eff.org/tech/browsers (last visited Mar. 30, 2012).

30 *See* FTC, *supra* note 4, at 25–26.

Retargeting is a type of behavioral advertising that targets users based on previous Internet activity on an e-commerce site when it does not result in a sale.[31] When a user views a product on a website, and then leaves the website, marketers can target the user with ads that feature that very product for days that follow.[32] E-commerce websites employ retargeting technology because "it allows for incredibly efficient [advertising] to customers who might have been on the fence with a purchase."[33] Zappos.com's use of retargeting technology has risen to the level of Internet meme notoriety, with customers noting that shoes they view on the site subsequently follow them onto other sites for weeks.[34] Another popular type of targeting is location-based "geotargeting," which carves out its audience based on self-reported location data, Internet Protocol (IP) address location, or GPS data on a mobile device.[35] Geotargeting is especially popular with small businesses that only want to reach audiences within physical proximity, and larger businesses that want to tailor messages differently for various regional audiences.

Targeting technology significantly increases the efficiency and effectiveness of marketing campaigns for most advertisers, particularly when advertisers layer several types of targeting to reach their ideal audience. Indeed, advertisers often use demographic, behavioral, retargeting, and geotargeting in a single campaign.

More importantly, targeted advertising supports the economic vitality of digital publishers, content providers, and other ad-supported Internet businesses. The capacity for increased revenues associated with ad-targeting enables the provision of many Internet services at little or no cost to consumers. Online advertising inventory (i.e. advertising space on the Internet) is mostly sold on a "CPM" basis. A CPM is the unit used to describe the cost per one thousand impressions, or views, of an Internet advertisement.[36] With each layer of targeting, an online publisher typically charges a premium on top of its usual CPM price. For example, if the average CPM price on any given network is $10, and the network charges a 10% premium for each level targeting on its inventory, then adding five layers of targeting (e.g. age, gender, income, browsing history,

---

31 *How Retargeting Works,* ADROLL, http://www.adroll.com/retargeting (last visited Mar. 30, 2012).

32 Darryl Ohrt, *Does Re-Targeting Show a Lack of Respect for Our Customers?*, ADAGE (June 7, 2011), http://adage.com/article/small-agency-diary/happened-respect-customers/228031.

33 *Id.*

34 *See id*. *See also, e.g.*, Cynthia Weaver, *These Boots Are Made for… Following Me?,* YALELAWTECH BLOG (Nov. 7, 2010), http://www.yalelawtech.org/privacy-who-can-you-trust/these-boots-are-made-for-following-me; Miguel Helft & Tanzina Vega, *Retargeting Ads Follow Surfers to Other Sites,* N.Y. TIMES (Aug. 19, 2010), http://www.nytimes.com/2010/08/30/technology/30adstalk.html.

35 Note that geotargeting technology can be driven by location data that is derived from behavioral tracking, demographic surveying, or IP address information. On mobile devices, location data can also be derived from built-in GPS technology. *See generally How Does AdWords Know Where Geographically to Show My Keyword-Targeted Ads?,* GOOGLE, http://support.google.com/adwords/bin/answer.py?hl=en&answer=6401 (last visited Mar. 30, 2012).

36 Definition of "CPM," MARKETINGTERMS, VERSION 2, http://www.marketingterms.com/dictionary/cpm/ (last visited Apr. 1, 2012).

and location) would increase the CPM to $16.11.[37] If an advertiser wanted to buy 500,000 advertising impressions, adding these targeting premiums would increase the total cost of the inventory from $5,000 to $8,052, a 61% price increase. In short, targeting premiums enable many ad-supported Internet businesses to significantly increase the value of their online advertising inventory.

Apocalyptic headlines announcing the downfall of traditional news media are abundant.[38] The supposedly inevitable consequence of outdated business models disrupted by the advent of digital publishing, is driven by the seeming impossibility of sufficiently monetizing digital media platforms to make up for lost revenues from newspapers and other print media products. As newsstand and subscription revenues decline, media companies struggle to monetize digital media platforms through paid content models. This new and frustrating set of challenges is aggravated by the fact that online advertising inventory typically commands a significantly lower price than print. As publishers continue to face declining revenues, however, targeting technology enables content providers to maximize the value of Internet advertising inventory.[39] While online advertising has yet to fill the gap created by print-side losses for most traditional publishers, targeting technology provides an increasingly compelling model for generating replacement revenues.[40]

The emergence of targeting technology has not only impacted traditional publishers' migration to the digital medium; it has also become a crucial aspect of all ad-supported Internet business models.[41] Search companies and social networks are possibly even more dependent on the role of ad-targeting technology in boosting the value of their advertising inventory than traditional publishers. Therefore, the sustainability of digital publishing and other content providers' business models relies in part on sustaining the value attributed to online advertising inventory, which in turn is bolstered by targeting technology. As a result, many services that consumers have come to expect at no cost depend on revenues associated with data-driven ad-targeting technology.

The increasing monetary value of personal data provides an incentive for businesses to collect and maintain more records about individuals than ever before. However, these databases raise major privacy concerns for consumers whose interests are at odds with businesses that profit from the collection and aggregation of

---

37 $10 x 1.10^5 = $16.11

38 *See generally* Cliff Kuang, *Print Media Is Dying. Online Revenues Are Tiny. What if the Ads Are to Blame?,* FASTCOMPANY (July 8, 2009, 3:34 PM), http://www.fastcompany.com/blog/cliff-kuang/design-innovation/print-media-dying-online-revenues-are-tiny-what-if-ads-are-blame; Jeremy Mullman, *Biz Sections Dying Off for Lack of Ad Revenue*, ADAGE (Feb. 18, 2008) http://adage.com/article/mediaworks/biz-sections-dying-lack-ad-revenue/125145.

39 *See generally* Paul Farhi, *Online Salvation?*, AM. JOURNALISM REV., Dec. 2007/Jan. 2008, at 19, *available at* http://www.ajr.org/article.asp?id=4427.

40 *Id.*

41 Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, at W1, *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

personal information. In addition to tracking technology and traditional demographic data collection methods, records are created "from a variety of sources, including publicly available government records, human resource databases, promotional activities such as contests and mass mailings, and transactional data from noncash purchases, frequent shopper programs, and Internet and telephone use."[42] Through the repeated consolidation and analysis of otherwise disparate data sources, databases are created which contain strikingly detailed information about an individual, such as his or her social security number, health related information, finances, criminal records, lifestyle preferences, and more.[43] Professor Neil M. Richards explains that such activities raise at least four kinds of privacy concerns for individuals:

> First, databases can be used to process . . . potentially embarrassing or highly personal information . . . . Second, [databases] composed of nonsensitive information in such enormous quantities . . . constitute[] a highly detailed dossier of a person's entire existence. Third, the information contained in consumer profiles can be quite inaccurate. Finally, there are no meaningful legal requirements that personal information in consumer profiles be kept securely. If used improperly, the sheer level of detail contained in consumer profiles can facilitate crimes such as identity theft, stalking, or harassment.[44]

Richards also argues that the existence of massive privately owned databases "significantly raise[s] the stakes for government surveillance," noting that

> Governments have long used private records to spy upon their citizens—often with sinister consequences—and the availability of larger and more detailed private records about people makes such forms of surveillance easier for governments to engage in. Indeed, recent activities by the federal government to investigate and forestall terrorism have frequently relied on computerized private-sector customer records containing financial, airline passenger, and other data.[45]

According to Richards, the acquisition of databases from private industry by law enforcement agencies and other government entities is especially alarming because it enables them to side-step constitutional restrictions by outsourcing surveillance to private actors.[46]

Perhaps a more esoteric critique concerning the aggregation and use of personal data in targeted advertising campaigns centers on

---

42 Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1157 (2005).
43 *Id*. at 1157.
44 *Id*. at 1158 (citations omitted).
45 *Id*. at 1158–59 (citations omitted).
46 *Id*.

privacy concerns related to questions of personal autonomy, freedom from scrutiny or categorization, and similar values grounded in normative theories of social identity.[47] The dominant philosophical discourse on consumer privacy in legal academia seems driven in part by the notion that "[a] crucial aspect of the ability to engage in intellectual exploration is that it be both private and confidential."[48] Moreover, some scholars, such as Professors Daniel C. Howe and Helen Nissenbaum view tracking technology as a threat to egalitarianism and socioeconomic justice because it reduces individuals' agency in relationship to "social actors far more powerful than themselves on nearly every measurable dimension—including wealth, mastery over technology, and access to power."[49] Accordingly, numerous legal scholars support the development of privacy legislation that would "forbid data-processing practices that treat individuals as mere conglomerations of transactional data, or that rank people as prospective customers, tenants, neighbors, employees, or insureds based on their financial or genetic desirability."[50]

Public interest organizations also support legislative action, but typically agree that online ad-targeting has both advantages and downfalls. Consumer privacy advocates argue that certain data collection and targeting methods are predatory, particularly when advertisers seek to target users based on their specific vulnerabilities.[51] For example, the Centers for Disease Control and Prevention has called attention to how immersive advertising campaigns sponsored by "junk food" manufacturers target minors and contribute to the problem of childhood obesity.[52] Critics also argue that data collection practices rob individual users of the ability to control personal information and "reap the financial benefits of their own data while publishers, ad exchangers and information brokers . . . profitably cash in on this information."[53]

---

47 Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423 (2000). *See also, e.g.*, Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 739–41 (1999); Brett M. Frischmann, *Cultural Environment and* The Wealth of Networks, 74 U. CHI. L. REV. 1083, 1122 (2007); A. Michael Froomkin, *The Death of Privacy?,* 52 STAN. L. REV. 1461 (2000); Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 417–21 (2002); McClurg, *supra* note 23, at 126–27; James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 26 (2003); Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559 (1998); Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J. L. & TECH. 194 (2008); Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1290 (2005).

48 Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 419 (2008).

49 Daniel C. Howe and Helen Nissenbaum, *TrackMeNot: Resisting Surveillance in Web Search,* in LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY, AND IDENTITY IN A NETWORKED SOCIETY, 431 (Ian Kerr, Valerie Steeves, and Carole Lucock, eds., 2009).

50 *Cohen, supra* note 47, at 1424.

51 Press Release, Fed'n of State Pub. Interest Research Grps., Consumer and Privacy Groups Urge Congress to Enact Consumer Privacy Guarantees (Sept. 1, 2009), *available at* http://www.uspirg.org/news/usp/consumer-and-privacy-groups-urge-congress-enact-consumer-privacy-guarantees.

52 *Legal and Policy Resources on Public Health "Winnable Battles,"* CENTER FOR DISEASE CONTROL AND PREVENTION, http://www2.cdc.gov/phlp/winnable/Advertising_Children.asp (last updated Dec. 20, 2010).

53 Grant Gross, *Privacy Groups File FTC Complaint on Behavioral Advertising*, PC WORLD (Apr. 8, 2010, 11:20 AM),

In the United States, there is no single comprehensive consumer privacy law that applies to online data collection or targeted advertising on the Internet. Information privacy law "consists of a hodgepodge of constitutional protections, federal and state statutory provisions, common law rules, and so on."[54] Private actions attempting to expand the breadth of existing federal statutes such as the Electronic Communications Privacy Act (ECPA),[55] the Computer Fraud and Abuse Act (CFAA),[56] and the Children's Online Privacy Protection Act (COPPA)[57] have largely failed to remedy

---

http://www.pcworld.com/article/193789/privacy_groups_file_ftc_complaint_on_behavioral_advertising.html (citing a complaint filed with the FTC on behalf of the Center for Digital Democracy (CDD), U.S. PIRG and the World Privacy Forum). *See also Should You Sell Your Digital Privacy?*, HARV. BUS. SCH. (Aug. 25, 2003), http://hbswk.hbs.edu/item/3636.html; Leena Rao, *Personal Raises $7M from Steve Case and Others to Help Consumers Protect Their Digital Data*, TECHCRUNCH (Jan. 6, 2011), http://techcrunch.com/2011/01/06/personal-raises-7m-from-steve-case-and-others-to-help-consumers-protect-their-digital-data (describing Personal, a new service that "empower[s] consumers to become gatekeepers of their information" and have sole ownership rights to control, share, and sell their personal data).

54 PATRICIA L. BELLIA, PAUL SCHIFF BERMAN, BRETT M. FRISCHMANN, DAVID G. POST, CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE, 625 (4th ed. 2011). Note, however, that certain industry-specific federal laws exist to protect individuals' privacy with respect to health care or personal financial information. *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 100 Stat. 2548 (2006) (codified in scattered sections of 5, 18, 29, and 42 U.S.C.); Right to Financial Privacy Act, 12 U.S.C § 3401–3422 (2006).

55 18 U.S.C. §§ 2510–2522 (1986). ECPA was enacted to prevent law enforcement agencies from performing unlawful interceptions of emerging electronic communications services. Whether ECPA is effective in reaching its intended goal is a worthy inquiry of its own, but its shortcomings as a tool for advancing consumer privacy are even more apparent. ECPA prohibits "any person" from intercepting electronic communications, but creates a significant statutory exception where parties to a communication have provided consent for a website to access their personal information. This "consent exception" has shaped the inquiry in consumer privacy suits brought under ECPA by plaintiffs who claim that ad-targeting practices unlawfully intercepted their private electronic communication, resulting in dismissals where consent was demonstrated "through evidence of appropriate notice and disclosure to users through service terms or privacy policies." Eric C. Bosset, Simon J. Frankel, Mali B. Friedman, Stephen P. Satterfield, *Private Actions Challenging Online Data Collection Practices Are Increasing: Assessing the Legal Landscape*, 23 INTELL. PROP. & TECH. L.J. 3, 4 (2011). *See also In re* Pharmatrak, Inc., 329 F.3d 9, 19 (1st Cir. 2003) (holding that secretly intercepting and accessing personal information through use of "cookies" was not found to violate ECPA because one of the parties to the communication "gave consent" to the interception). ECPA also creates exceptions for interceptions occurring in the ordinary course of business and as necessary, incident to rendering services. Taken together, these exceptions foreclose liability under ECPA "for behavioral advertising of the kind that [many ad companies] practice[]." Bosset et al., *supra* note 55, at 4.

56 18 U.S.C. § 1030 (West, Westlaw through 2008 amendments). CFAA was intended to address the problem of computer hacking by non-government actors by penalizing unauthorized access. "Private persons who can show 'damage or loss' from [the] prohibited conduct may sue for civil damages," but those plaintiffs are likely to face difficulty in "making the required showing of tangible damage or economic loss associated with the alleged intrusion." Bosset et al., *supra* note 55 at 5. Thus, CFAA appears to be no more useful than ECPA in the realm of consumer privacy.

57 15 U.S.C. §§ 6501–6506 (2006). Unlike ECPA and CFAA, which were never intended as consumer privacy protections, COPPA was specifically designed as a consumer privacy protection for children under the age of thirteen. COPPA requires websites directed towards children to provide detailed notice of its data policies and "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children." *Id.* § 6502(b)(1)(A)(ii). The statute further prohibits websites from "conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity." *Id.* § 6502(b)(1)(C). Finally, COPPA requires children's websites to establish and maintain "procedures to protect the confidentiality, security, and integrity of personal information collected from children." *Id.* § 6502(b)(1)(D). While COPPA speaks directly to privacy advocates' concerns, its major limitation is that the consumer protections it affords extend only to Internet users below the age of thirteen. *Id.* § 6501(1).

alleged privacy harms related to data collection and targeting technologies.[58] Without a comprehensive federal statutory framework, consumer privacy is largely left to self-regulation. The Federal Trade Commission (FTC) publishes "Fair Information Practice Principles" (FIPPs), to guide the industry on the importance of "transparency, consumer autonomy, and accountability,"[59] but it also emphasizes the limitations of self-regulation, and the supports the call-to-action for comprehensive legislation from Congress.[60]

The absence of regulatory guidelines has a negative impact on industry as well as consumers, since the resulting uncertainty is a constant source of anxiety for marketers, publishers, and other ad-supported Internet businesses. Comprehensive privacy legislation would provide much needed clarity and eliminate confusion for many U.S. companies, yet the supposed tension between regulation and economic growth has caused legislators to approach reform with utmost caution. Although politicians want to advance consumer privacy interests, they are hesitant to do so because regulatory efforts are often misconstrued as a threat to innovation, particularly in a weak economy. Nevertheless, the collective call for legislative action from legal scholars, public interest organizations, and government agencies seems to have finally catalyzed progress towards a comprehensive consumer privacy framework in Congress over the past year.[61] According to some commentators, however, the Supreme Court's First Amendment ruling in *Sorrell v. IMS Health* threatens to preempt such forthcoming legislation.

II. *SORRELL V. IMS HEALTH*: THE CONSTITUTIONAL RIGHT TO . . . AD TARGET?

A. *The Controversy over Data Privacy and the First Amendment*

The statute at issue in *Sorrell* initially seemed to have a relatively a narrow application—it restricted a specific set of marketing tactics employed by pharmaceutical companies and their advertising partners in three New England states. However, the case quickly came to represent much larger issues, as it raised broader questions about how the First Amendment may limit a wide range of information regulations.

1. The Vermont Statute

Many pharmacies keep detailed records of their customers' prescription information, including the prescribing doctor's name

---

58 *See generally* Bosset et al., *supra* note 55, at 5.
59 FTC, *supra* note 4, at 6.
60 *Id.* at 8 ("In 2000, the Commission reported to Congress that, although there had been improvement in industry self-regulatory efforts to develop and post privacy policies online, only about one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security."). *See also Fair Information Practice Principles*, FED. TRADE COMMISSION, *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last updated June. 25, 2007).
61 *See infra* notes 93–107.

and the patient's age, gender, and health conditions.[62] Pharmacies collect this data for every prescription, and sell it to pharmaceutical information-research and marketing companies that combine that information with other data, such as the American Medical Association's (AMA) membership database, which includes doctors' specialties and contact information.[63] This process enables the maker of a new drug to target specific doctors who treat patients with the corresponding health condition "and lavish that physician with attention and gifts in an effort to get them to switch [to] . . . more expensive, newer drugs that are no-more effective and generally less safe than older, established choices."[64]

In 2007, the Vermont legislature became concerned that highly sophisticated pharmaceutical marketing campaigns were influencing doctors to make decisions based on incomplete and biased information.[65] Legislators found that these targeted campaigns increased the overall cost of healthcare by encouraging excessive reliance on brand-name drugs, without comparing less costly generic alternatives.[66]

In order to address the perceived negative impact on the state's public health goals, the Vermont legislature passed the Prescription Confidentiality Law.[67] The statute prohibited pharmacies, health insurers, and other healthcare intermediaries from selling, disclosing, or using prescriber-identifying information without consent from the prescribing doctor.[68] However, the statute provided limited exceptions for certain purposes such as transferring information for health care research purposes, transmitting prescriptions between pharmacies, and targeting public health communications about treatment options, safety notices, and clinical trials.[69] In essence, the statute made it unlawful for pharmaceutical marketers to access or use a doctor's prescription information without that doctor's consent. Similar legislation had already been enacted in New Hampshire[70] and Maine.[71]

---

62 Ano Lobb, *Darkside of Health Data*, JUSTMEANS (Nov. 12, 2009, 9:40 AM), http://www.justmeans.com/Darkside-of-health-data/5224.html.

63 *Id.*

64 *Id.*

65 "[T]he 'goals of marketing programs are often in conflict with the goals of the state' and that the 'marketplace for ideas on medicine safety and effectiveness is frequently one-sided in that brand-name companies invest in expensive pharmaceutical marketing campaigns to doctors.' [18 V.S.A. § 4631 (2007),] §§ 1(3), (4). Detailing, in the legislature's view, caused doctors to make decisions based on 'incomplete and biased information.' § 1(4)." Sorrell v. IMS Health, Inc., 131 S. Ct. 2653, 2661 (2011) (citing legislative findings from Vermont's Prescription Confidentiality Law).

66 *Id.*

67 18 V.S.A. § 4631, *invalidated by Sorrell*, 131 S. Ct. 2653.

68 *Id.*

69 *Id.*

70 New Hampshire's Prescription Information Law, which became effective on June 30, 2006, prohibited the "transmission or use of both patient-identifiable data and prescriber-identifiable data for certain commercial purposes." IMS Health Inc. v. Ayotte, 490 F. Supp. 2d 163, 170 (D.N.H. 2007) *rev'd and vacated,* 550 F.3d 42 (1st Cir. 2008) *abrogated by Sorrell* 131 S. Ct. 2653.

71

> On June 29, 2007, state of Maine Governor John E. Baldacci signed into law L.D. 4, 'An Act to Amend the Prescription Privacy Law' . . . allow[ing] Maine prescribers to

2. First Amendment Challenge and Legislative Action

Several healthcare data analytics companies[72] and trade groups representing the country's leading pharmaceutical research and biotechnology companies[73] challenged the laws in all three states, seeking declaratory and injunctive relief under the theory that these statutes violated their First Amendment rights.[74] The first suit was brought against the New Hampshire statute, which was struck down on First Amendment grounds.[75] Six months later, a District Court in Maine granted a preliminary injunction precluding enforcement of its law on similar reasoning.[76] Maine and New Hampshire both appealed to the United States Court of Appeals for the First Circuit.

By the time the First Circuit heard oral arguments,[77] concern about the potential impact of this case had spread well beyond Maine and New Hampshire. Although the statutes in all three states were originally intended to reach only prescription data uses by pharmaceutical companies in off-line marketing campaigns, they quickly began to signify much more. Many believed that the outcome of these cases loomed large on the future of consumer data privacy and online advertising. Several public interest advocacy groups, including the American Association of Retired Persons (AARP), the National Physicians Alliance, and the Electronic Privacy Information Center (EPIC), filed briefs in support of New Hampshire's attorney general.[78] Briefs were also filed by lobbying organizations and corporate interest advocacy groups in support of the plaintiffs.[79]

> "opt-out," in other words, to demand confidentiality by preventing pharmaceutical companies from using their individualized prescribing information to market them or others. The Law [did] not directly affect [prescription drug information intermediaries' ("PDIIs")] ability to purchase pharmacy information or to use that information for purposes other than marketing. If prescribers opt-out, however, the Law forbids carriers, pharmacies, or PDIIs from selling or using their information for marketing[.]

IMS Health Corp. v. Rowe, 532 F. Supp. 2d 153, 165 (D. Me. 2007), *abrogated by Sorrell*, 131 S. Ct. 2653.

72 Including IMS Health, Inc., Verispan, L.L.C., and Source Healthcare Analytics, Inc., a subsidiary of Wolters Kluwer, Health Inc.

73 Represented by the Pharmaceutical Research and Manufacturers of America (PhRMA). Headquartered in Washington, D.C., PhRMA represents the country's leading pharmaceutical research and biotechnology companies, which are devoted to inventing medicines that allow patients to live longer, healthier and more productive lives. PhRMA companies are leading the way in the search for new cures. PhRMA members alone invested an estimated $49.4 billion in 2010 in discovering and developing new medicines. Industry-wide research and investment reached a record $67.4 billion in 2010.

About PhRMA, PHRMA, http://www.phrma.org/about/phrma (last visited Mar. 31, 2012). The PhRMA membership roster includes most global pharmaceutical companies. *Member Companies*, PHRMA, http://www.phrma.org/about/member-companies (last visited Mar. 31, 2012).

74 *Ayotte*, 490 F. Supp. 2d 163; *Rowe*, 532 F. Supp. 2d 153; and IMS Health, Inc. v. Sorrell, 631 F. Supp. 2d 434 (D. Vt. 2009).

75 *Ayotte*, 490 F. Supp. 2d at 170.

76 *Rowe*, 532 F. Supp. 2d at 157.

77 Oral arguments were heard on Jan. 9, 2008.

78 American Association of Retired Persons, Community Catalyst, National Legislative Association on Prescription Drug Prices, National Physicians Alliance, New Hampshire Medical Society, Prescription Policy Choices, and the Electronic Privacy Information Center filed amici curiae in support of the Attorney General's position.

79 EHealth Initiative, National Alliance for Health Information Technology, Surescripts,

The First Circuit Court of Appeals reversed and vacated the New Hampshire District Court decision, finding that the New Hampshire law was a legitimate commercial regulation that placed a restriction on conduct, not speech.[80] A few months later, the Vermont statute was also upheld on different grounds.[81] The Vermont District Court found that the statute did in fact place a restriction on speech,[82] but that the law withstood intermediate scrutiny because it was narrowly tailored to support the state's substantial interest in cost containment and other public health goals.[83]

Shortly after the First Circuit decision, speculation about the potential impact of the ruling on commercial data privacy beyond the pharmaceutical context began to spread like wildfire in the advertising community. The Association of National Advertisers rallied support against the First Circuit decision, claiming the issue transcended prescription drugs, and asking the Supreme Court to review the decision.[84] Publishers and advertisers worried that the ruling would "affect[] virtually any business that uses information about consumer buying behavior to guide its sales strategies."[85] In addition, they were fearful that the ruling would "embolden other states to restrict the collection and trade of consumer data," potentially limiting "a range of activities, from producing targeted Web advertising to screening job applicants for criminal behavior."[86]

Over forty briefs were filed in support of IMS Health's Supreme Court bid following the First Circuit's decision, but the Court denied certiorari.[87] The First Circuit reaffirmed its position by overturning the injunction against the Maine statute as well.[88] The issue seemed settled, yet the fight was not over.

Two years after the First Circuit's ruling on the New Hampshire statute, the Second Circuit Court of Appeals reversed and vacated the Vermont District Court decision, holding the Vermont Prescription Confidentiality Law unconstitutional.[89] Whereas the First Circuit had characterized prescription data as "a mere 'commodity' with no greater entitlement to First Amendment protection than 'beef jerky' . . . the [Second Circuit] concluded that a prohibition on the sale of prescriber-identifying information [was] a content-based rule akin to a ban on the sale of cookbooks, laboratory results, or train

---

National Association of Chain Drug Stores, the Washington Legal Foundation, Coalition for Healthcare Communications, and Wolters Kluwer Health, Inc. filed amici curiae in support of the plaintiffs.

80 *Ayotte*, 550 F.3d at 45.

81 *See* IMS Health v. Sorrell, 631 F. Supp. 2d 434, 440 (D. Vt. 2009).

82 *Id.* at 445–47.

83 *Id.* at 449–55.

84 Arlene Weintraub, *The Fight over Drug Data Mining,* BLOOMBERG BUSINESSWEEK (June 10, 2009, 4:56 PM), http://www.businessweek.com/magazine/content/09_25/b4136000501366.htm.

85 *Id.*

86 *Id.*

87 *Id.*; IMS Health, Inc. v. Ayotte, 129 S. Ct. 2864 (2009) (denying Petition for Writ of Certiorari to the United States Court of Appeals for the First Circuit).

88 *See* IMS Health, Inc. v. Mills, 616 F.3d 7 (1st Cir. 2010).

89 *See* IMS Health, Inc. v. Sorrell, 631 F. Supp. 2d 434 (D. Vt. 2009).

schedules."[90] The Circuit split was largely attributable to disagreement over this issue.[91] The Vermont Attorney General petitioned for a writ of certiorari to review the judgment. On January 7, 2011, the Supreme Court granted certiorari to resolve the split between the First and Second Circuits.[92]

Meanwhile, Congress and the executive branch embarked on a campaign to enact comprehensive privacy legislation in response to concerns over data collection and targeted practices involved in Internet advertising. In March 2011, the Obama administration called upon Congress to enact comprehensive consumer privacy legislation.[93] In a hearing before the Senate Committee on Commerce, Science, and Transportation, the Assistant Secretary for Communications and Information at the Department of Commerce stated the Administration's view that "the U.S. consumer data privacy framework [would] benefit from legislation to establish a clearer set of rules . . . while preserving the innovation and free flow of information that are hallmarks of the Internet."[94] The administration also provided substantive recommendations for a new federal privacy law, recommending flexible and well tailored legislation that would "set forth baseline consumer data privacy protections" in a consumer privacy bill of rights, and "provide the FTC with the authority to enforce" those protections.[95]

One month later, Senators John Kerry and John McCain made a bipartisan proposal for exactly this type of framework in the Commercial Privacy Bill of Rights Act of 2011 (CPBRA).[96] The legislation outlines three fundamental consumer privacy rights and prompts the FTC to initiate rulemaking proceedings requiring entities that collect, use, transfer, or store large amounts of personal data about individuals for extended time periods to adjust their privacy policies to conform with those rights.[97] More specifically, CPBRA establishes the right to security and accountability,[98] the right to notice and individual participation,[99] and rights relating to

---

90 Sorrell v. IMS Health, Inc., 131 S. Ct. 2653, 2666 (2011) (quoting IMS Health Inc. v. Ayotte, 550 F.3d 42, 53 (1st Cir. 2008)).

91 *Sorrell*, 131 S. Ct. at 2666.

92 Sorrell v. IMS Health, Inc., 131 S.Ct. 857 (2011) (granting petition for writ of certiorari to the United States Court of Appeals for the Second Circuit granted).

93 See testimony of Lawrence E. Strickling, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration, *Before the S. Comm. on Commerce, Science, and Transportation,* 112th Cong. (Mar. 16, 2011). (Testimony of Lawrence E. Strickling, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration).

94 *Id.*

95 *Id.*

96 S. 799, 112th Cong. (2011).

97 CPBRA applies to entities that collect, use, transfer, or store personally identifiable information concerning more than 5,000 individuals during any consecutive twelve-month period. *Id.* § 401.

98 CPBRA requires companies to protect information from data breaches, embrace "privacy by design," and respond to requests for information from individuals about how their personal data is collected, used, transferred, or stored. *Id.* §§ 101–103.

99 CPBRA reaffirms a company's obligation to provide "clear, concise, and timely notice to individuals" about its data practices, including any subsequent changes in its privacy policy; ensures notice requirements cannot be circumvented through data transfers to third parties, by prohibiting them from using data in any manner not specifically authorized; mandates a "clear

data minimization, constraints on distribution, and data integrity as fundamental principles of consumer privacy.[100] CPBRA entrusts the FTC and state attorneys general with enforcement authority, but does not provide any private right of action.[101] It also eases the burden of compliance and limits the scope of liability by establishing a safe harbor program to be administered by nongovernmental organizations.[102]

The administration's call for legislation also prompted the introduction of the Personal Data Privacy and Security Act[103] and the Do Not Track Online Act in the Senate.[104] In addition, at least four other comprehensive privacy bills are currently being considered in the House of Representatives, which would help define and promote consumer rights with respect to personal data in the Internet advertising context.[105]

As the date for oral arguments came near, speculation about *Sorrell*'s impact on Internet advertising continued to grow. The Coalition for Healthcare Communication called the case "a game changer" for data-driven businesses, advertising agencies, publishers and other media companies.[106] "If IMS loses because the Court considers these activities unworthy of First Amendment protections, 'the assaults on data gathering and use in marketing will proliferate . . . [and t]he ensuing legal actions will not just be about IMS data, but all marketing uses of data, which would be a huge blow," explained one commentator.[107]

Sixteen *amicus curiae* briefs were filed in support of IMS Health, three of which were filed by interested parties whose primary concern had little to do with prescription information or the pharmaceutical industry.[108] A leading group of publishers and journalists including Bloomberg, McGraw-Hill, Hearst Corporation, and the Associated Press, filed a brief contending that both of the lower courts had "failed to adequately understand, define and protect

---

and conspicuous mechanism" for users who wish to opt-out from being tracked altogether, or to prevent the use of their data by third parties; requires companies that store such information to provide individuals with access to data collected about them and the ability to correct data to improve its accuracy. *Id.* §§ 201–202.

100 CPBRA seeks to address further consumer interest in data minimization, constraints on distribution, and data integrity by imposing restraints on the extent of data collection practices and the length of time that data may be retained to only that which is "reasonably necessary"; prohibits careless and irresponsible data sharing practices; requires companies to implement procedures intended to ensure accuracy of data. *Id.* §§ 301–303.

101 S. 799, §§ 402–403, 406.

102 *Id.* § 501.

103 Personal Data Privacy and Security Act, S. 1151, 112th Cong. (2011).

104 Do Not Track Online Act, S. 913, 112th Cong. (2011).

105 Do Not Track Kids Act, H.R. 1895, 112th Cong. (2011); Consumer Privacy Protection Act, H.R. 1528, 112th Cong. (2011); Global Online Freedom Act, H.R. 3605, 112th Cong. (2011); Do Not Track Me Online Act, H.R. 654, 112th Cong, (2011); Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (BEST PRACTICES) Act, H.R. 611, 112th Cong. (2011).

106 Gretchen Parisi, *Update: Supreme Court Finds Rx Data Use Ban Violates the First Amendment,* COALITION FOR HEALTHCARE COMMUNICATION (Apr. 20, 2011), http://www.cohealthcom.org/2011/04/20/why-the-supreme-court-oral-arguments-in-sorrell-v-ims-matter-to-patients-clients-and-health-marketing-agencies.

107 *Id.*

108 *See infra* notes 109–112 and accompanying text.

First Amendment rights to gather, publish and report on computerized data and the important information and analysis that is based on such data."[109] Trade groups representing large advertising agencies, database publishers, and marketing intelligence groups filed another brief, arguing that database publishing should receive the highest level of First Amendment protection, regardless of its purpose, since "databases are comprised of facts," and the "publication of truthful information is essential to a democratic society."[110] Several advertising associations also filed briefs, emphasizing the centrality of data to the economy and advertising businesses in particular, that "rely upon the protections of the First Amendment every day in conducting their businesses nationwide."[111]

Numerous public interest organizations, physicians groups, state governments, and the United States Solicitor General sided with the state of Vermont.[112] The Electronic Frontier Foundation (EFF), Public Citizen, and EPIC in particular, tended to frame the issue as implicating major information privacy rights in the digital era.[113] However, other organizations, such as the Center for Democracy and Technology (CDT), were cautious about framing the case in this manner, explaining that because *Sorrell* was limited to the narrow issue of de-identified prescription data in the context of pharmaceutical marketing, it would not have a negative general impact on other privacy considerations, so long as the respondents

---

109 Brief for Bloomberg L.P., The McGraw-Hill Companies, Inc., et al., as Amici Curiae Supporting Respondents at 3–4, Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011) (No. 10–779), 2011 WL 1253925.

110 Brief for American Business Media, The Coalition for Healthcare Communication, The Consumer Data Industry Association, Corelogic, The National Association of Professional Background Screeners, and Reed Elsevier Inc. as Amici Curiae Supporting Respondents at 4, *Sorrell*, 131 S. Ct. 2653 (No. 10–779), 2011 WL 1253921.

111 Brief for Association of National Advertisers, Inc., American Advertising Federation, and American Association of Advertising Agencies as Amici Curiae Supporting Respondents at 28, *Sorrell*, 131 U.S. 2653 (No. 10–779), 2011 WL 1253920.

112 *See, e.g.*, Brief of Amicus Curiae Electronic Frontier Foundation in Support of Petitioners, *Sorrell*, (No. 10–779), 2011 WL 757416; Brief of AARP and the National Legislative Association on Prescription Drug Prices as Amici Curiae in Support of Petitioners, *Sorrell*, 131 S. Ct. 2653 (No. 10–779), 2011 WL 771333; Brief of Amici Curiae AFSCME District Council 37, Health Care for All, and Community Catalyst in Support of Petitioners, *Sorrell*, 131 S. Ct. 2653 (No. 10–779), 2011 WL 805234; Brief of Amicus Curiae Association of American Physicians & Surgeons in Support of Petitioners, *Sorrell*, 131 S. Ct. 2653 (No. 10–779), 2011 WL 741929; Brief of Amici Curiae Public Citizen, the Center for Science in the Public Interest, Consumer Action, Public Good, U.S. PIRG, and New Hampshire PIRG in Support of Petitioners, *Sorrell*, 131 S. Ct. 2653 (No. 10–779), 2011 WL 757415; Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Legal Scholars and Technical Experts in Support of the Petitioners, *Sorrell*, 131 S. Ct. 2653 (No. 10–779), 2011 WL 719646; Brief for the United States as Amicus Curiae Supporting Petitioners, *Sorrell*, 131 S. Ct. 2653 (No. 10–779), 2011 WL 719647; Brief for the States of Illinois, Alabama, Arizona, Arkansas, California, Colorado, Delaware, Georgia, Hawaii, Idaho, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Minnesota, Mississippi, Montana, Nevada, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Washington, and West Virginia and the District of Columbia as Amici Curiae in Support of Petitioners, *Sorrell*, 131 S. Ct. 2653 (No. 10–779), 2011 WL 771332.

113 *See generally* Press Release, Public Citizen, Public Citizen Files Suit to Obtain Information Gathered Under Vermont's Pharmaceutical Marketing Disclosure Law (Aug. 29, 2005), *available at* http://www.citizen.org/pressroom/pressroomredirect.cfm?ID=2036; *Sorrell v. IMS Health*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/cases/sorrell-v-ims-health (last visited Dec. 15, 2011); *Sorrell v. IMS Health*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/ims_sorrell/#state (last visited Mar. 31, 2012).

and amici did not bring them out.[114] CDT did not file an amicus brief, but issued a memo warning that consumer privacy could actually be harmed if the Court were to accept some of the claims made in briefs supporting the Vermont statute.[115] "Sorrell v. IMS Health is not about privacy in the way that defenders of the Vermont law claim," explained the CDT memo.[116] CDT further cautioned that a broad ruling might negatively impact privacy, and "could derail other very timely initiatives."[117]

Following oral arguments, but before the case was decided, CDT issued another statement anticipating the ruling and its potentially "far-reaching privacy implications."[118] "We are facing an important moment in the effort to secure comprehensive personal information privacy protections for consumers," explained CDT's health privacy expert, Deven McGraw, "[and] that effort would be upended if the Court were to find in this case that corporate First Amendment rights trump privacy protections."[119] McGraw noted however, that the Court could avoid the "confrontation between corporate First Amendment rights and privacy" altogether by deciding the case "on the narrow basis of whether the statute inappropriately discriminate[d] against particular types of speech or speakers."[120] And that is just what the Court did.

B. *The Supreme Court Decision*

Today the Supreme Court has overturned a sensible Vermont law that sought to protect [medical privacy]. This divided ruling is a win for data miners and large corporations and a loss for those of us who care about privacy . . . . [The] decision is another example of this Court using the First Amendment as a tool to bolster the rights of big business at the expense of individual Americans . . . . State legislatures should be allowed to protect their citizens' privacy rights over corporate interests in profits.

–Senator Patrick Leahy[121]

In a 6-3 decision, the Supreme Court held that the Prescription Confidentiality Law imposed an unconstitutional burden on protected speech under the First Amendment.[122]

---

114 *See Memo on Sorrell v. IMS Health, Inc: Supreme Court Case Requires Nuanced Understanding of Privacy*, CENTER FOR DEMOCRACY AND TECH. (Mar. 22, 2011), *available at* http://www.cdt.org/paper/memo-sorrell-v-ims-health-inc-supreme-court-case-requires-nuanced-understanding-privacy.

115 *Id.* at 5.

116 *Id.*

117 *Id.*

118 Deven McGraw, *Sorrell v IMS Health Has Far-Reaching Privacy Implications*, CENTER FOR DEMOCRACY AND TECHN. (May 6, 2011), http://www.cdt.org/blogs/deven-mcgraw/sorrell-v-ims-health-has-far-reaching-privacy-implications.

119 *Id.*

120 *Id.*

121 Press Release, Senator Patrick Leahy, Comment of Senator Patrick Leahy on Supreme Court Decision in *Sorrell v. IMS Health Inc*. (June 23, 2011), *available at* http://leahy.senate.gov/press/press_releases/release/?id=4a16ce1b-1710-44b7-9b6d-ac723ad6bdce.

122 Sorrell v. IMS Health, Inc., 131 S. Ct. 2653 (2011).

The Court refused to adopt the First Circuit's characterization of the statute as mere commercial regulation, stating that "the creation and dissemination of information are speech within the meaning of the First Amendment," and rejecting arguments that the sale, transfer, or use of prescriber-identifying data constituted conduct rather than speech.[123]

Having determined that such uses of data constitute speech, the majority found that allowing pharmacies to sell information "to private or academic researchers . . . but not . . . to pharmaceutical marketers," imposed a content and speaker-based restriction on speech.[124] The majority reasoned that because marketing is "speech with a particular content," restricting access to data for marketing purposes amounts to content-based discrimination.[125] The Court further noted that the legislature had designed the statute with an express purpose to target marketers' and pharmaceutical companies' speech for "disfavored treatment," going "beyond mere content discrimination, to actual viewpoint discrimination."[126]

In finding that the statute constituted viewpoint discrimination, the Court emphasized that the "First Amendment requires heightened scrutiny whenever the government creates 'a regulation of speech'" which imposes a "content-based burden on protected expression" because it disagrees with the message it conveys.[127] Therefore, in order to overcome "the targeted, content-based burden . . . on protected expression," the state would have to show that "the statute directly advance[d] a substantial governmental interest and that the measure [was] drawn to achieve that interest."[128]

The Court held that the Prescription Confidentiality Law could not overcome heightened scrutiny. Vermont's Attorney General[129] argued that the statute was necessary "to protect medical privacy, including physician confidentiality, avoidance of harassment, and the integrity of the doctor-patient relationship."[130] Vermont also defended its law on the basis that it was "integral to the achievement of policy objectives—namely, improved public health and reduced healthcare costs."[131] But the Court rejected these arguments, holding that neither justification warranted the content-based restrictions and viewpoint discrimination imposed by the statute.[132]

Justice Breyer's dissent ultimately sided with the First Circuit Court of Appeals in reasoning that the statute was a reasonable effort to regulate commercial activity that did not impose any

---

123 *Id.* at 2667.
124 *Id.* at 2662–63.
125 *Id.* at 2663.
126 *Id.* at 2663.
127 *Id.* at 2664 (2011) (citing Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989), Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 418 (1993), and Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 658 (1994)).
128 *Sorrell,* 131 S. Ct. at 2667.
129 William H. Sorrell is the Attorney General for the state of Vermont.
130 *Sorrell,* 131 S. Ct. at 2668.
131 *Id.*
132 *Id.*

significant burden on free speech.[133] The dissent emphasized that the Court had never before found that the First Amendment prohibits government from restricting the use of information gathering pursuant to a regulatory mandate, nor had it ever previously applied any form of heightened scrutiny in a similar case.[134] The dissent further noted that the majority's decision represented a troubling shift in preference for judicial decision-making over democratic decision-making, departing from a longstanding trend of deference as to similar regulatory measures since the New Deal.[135]

III. *SORRELL*'S POTENTIAL IMPACT ON INTERNET ADVERTISING REGULATION

Speculation about *Sorrell*'s application to Internet advertising intensified after the Supreme Court issued its decision. The opinion was understood by many as "showing sympathy toward targeted marketing."[136] Internet libertarians heralded *Sorrell* as "a major victory for commercial free speech rights," hypothesizing that the ruling would preempt forthcoming privacy legislation.[137] Marketers welcomed the possibility that targeted marketing could in some situations enjoy First Amendment protection.[138] "[T]he decision enables us to use the First Amendment to defend innovative and effective marketing of all types, including [the use of data and data analytics] in the digital space," explained one such commentator.[139]

In spite of widespread speculation about *Sorrell*'s impact on Internet advertising and digital privacy, the majority seemed to indicate that its decision was narrow and left much to be resolved.[140] The Court prudently acknowledged that technology's capacity "to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."[141] In light of this disclaimer, *Sorrell* is probably not quite the shield that marketers are hoping for with respect to privacy regulations and targeted advertising.

---

133 *Compare Sorrell*, 131 S. Ct. at 2677 (Breyer, J., dissenting), *with* IMS Health Inc. v. Ayotte, 490 F. Supp. 2d 163, 170 (D.N.H. 2007) *rev'd and vacated,* 550 F.3d 42 (1st Cir. 2008), *abrogated by* Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

134 *Sorrell*, 131 S. Ct. at 2677 (Breyer, J., dissenting).

135 *Id.* at 2685 (Breyer, J., dissenting) ("[This decision] reawakens *Lochner*'s pre-New Deal threat of substituting judicial for democratic decisionmaking where ordinary economic regulation is at issue.").

136 Bruce L. McDonald, *Does the Supreme Court's* Sorrell *Decision Threaten Privacy?,* WILEY REIN LLP (July 2011), http://www.wileyrein.com/publications.cfm?sp=articles&id=7222.

137 *Sorrell: The Supreme Court Confronts Free Speech, Marketing & Privacy,* TECHFREEDOM (July 19, 2011), http://techfreedom.org/event/sorrell-supreme-court-confronts-free-speech-marketing-privacy.

138 "As a result of this Supreme Court decision, clients, publishers and agencies are in a much better position today to oppose restrictions on marketing and marketing analytics when imposed by all governments, including states, the Congress, the FTC and the FDA." John Kamp, Sorrell v. IMS*: What Marketing Professionals Need to Know,* COALITION FOR HEALTHCARE COMMS. (July 18, 2011, 2:59 PM), http://www.cohealthcom.org/2011/07/18/sorrell-v-ims-what-marketing-professionals-need-to-know.

139 *Id.*

140 *Sorrell*, 131 S. Ct. at 2672.

141 *Id.*

The *Sorrell* decision is certainly remarkable in the way that it describes data as speech, and the scope of that particular finding will inevitably become a considerable question for both lower courts and policymakers. However, this aspect of the decision cannot be isolated and read separately from the rest of the opinion to frame it as a First Amendment shield to any and all regulations involving data. To that end, the Court's content and viewpoint discrimination analysis offers a more comprehensive framework for assessing the constitutionality of any particular restriction on data under the First Amendment. The majority's latter analysis preserves policymakers' ability to adopt regulations that would protect consumer privacy interests without violating the First Amendment, and supports the conclusion that recent legislative proposals to implement new consumer privacy regulations will very likely escape *Sorrell*'s narrow reach.

A. *The Limited Scope of Sorrell*

1. Data as Speech

The Court's declaration that "the creation and dissemination of information" constitutes speech under the First Amendment is an interesting aspect of the opinion regarding its applicability to commercial data privacy and information law.[142] As contemplated by the dissent, an overbroad interpretation of that language could open a "Pandora's Box of First Amendment challenges to many ordinary regulatory practices that may only incidentally affect [speech]."[143] Indeed, the broadest interpretation of the majority's language would be to understand it as meaning that all data is speech. Yet treating all data as speech seems overbroad and highly problematic. While the Court's language is undoubtedly broad, such an interpretation would position *Sorrell* as a de facto challenge to any ordinary regulation of information-based goods, leading to absurd results and undesirable consequences. For example, countless areas of statutory and common law that impose content-based restrictions on information, such as securities regulation, intellectual property and antitrust law, the Uniform Commercial Code, and the Federal Rules of Evidence would trigger heightened First Amendment scrutiny under such a simplistic understanding of *Sorrell*.[144]

Therefore, the task at hand is developing a nuanced understanding of the Court's reasoning that reflects its true intentions and yields more favorable results. Thankfully, the rest of the opinion tempers the majority's uncharacteristically broad language with respect to the First Amendment boundary.

In spite of its seemingly unequivocal language, *Sorrell* does not expand the scope of First Amendment protection to data in and of

---

142 *Id.* at 2667.
143 *Id.* at 2685 (Breyer, J., dissenting).
144 *See, e.g.*, Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1768 (2004); Richards, *supra* note 42, at 1171.

itself, irrespective of context. In fact, the opinion renders the conceptual distinction between commodity, conduct, content, and expression somewhat obsolete. The Court's seemingly broad characterization of data as speech hinges not on some arbitrary categorical classification of data as either speech or commodity, but on the expressive role of prescription data in a marketing context.[145] In other words, the protected speech at issue in *Sorrell* is not prescription data in and of itself, but the marketing purpose that it serves.[146] Justice Kennedy's suggestion that the case could be resolved similarly even if prescriber-identifying data had been designated a commodity rather than speech further supports the conclusion that, notwithstanding the Court's radical dicta characterizing the creation and dissemination of information as speech, *Sorrell* does not inherently expand the scope of First Amendment protection to all activities involving the use, collection, sale, or transfer of data.[147]

Moreover, the Court's implication that data constitutes speech contradicts its later reasoning that compares the Vermont statute to a law prohibiting trade magazines from purchasing or using ink.[148] In this analogy, the Court positioned data as the metaphorical ink—a commodity. According to the Court's logic then, data, like ink, is also a commodity, subject to reasonable regulations that may incidentally restrict speech. However, such restrictions violate the First Amendment if the intended use for such data is the creation of protected expression, such as marketing or journalism.

This is not the first case to consider the First Amendment status of otherwise non-expressive information as speech when that information is used to support the function of expression. In *Universal City Studios, Inc. v. Corley*, the Second Circuit contemplated the scope of First Amendment protection for computer code, and resolved to treat code as "combining nonspeech and speech elements."[149] Having found that the code supported expressive purposes, the court upheld the content-neutral regulation because it supported a substantial government interest.[150] The *Corley* opinion is consistent with an interpretation of *Sorrell* that determines whether data is First Amendment speech on the basis of whether the data is being used to directly support an expressive function. *Corley* also demonstrates that "classifying the target of governmental regulatory action as 'speech,' . . . implicates the protections of the First Amendment . . . [but] does not immunize the activity from governmental regulation."[151]

The relationship between ad-targeting technology and data is

---

145 *Sorrell*, 131 S. Ct. at 2664–67.
146 *Id.*
147 *See id.* at 2667 ("[T]his case can be resolved even assuming, as the State argues, that prescriber-identifying information is a mere commodity.").
148 *Id.*
149 Universal City Studios, Inc. v. Corley, 273 F.3d 429, 451 (2d Cir. 2001).
150 *Id.*
151 BELLIA ET AL., *supra* note 54, at 530 (4th ed. 2011).

similar to the relationship between computer programs and code. Both encompass processes that are simultaneously functional and expressive such that the two concepts merge entirely. Under the majority's reasoning in *Sorrell*, the creation and dissemination of data through tracking and targeting technologies could easily be characterized interchangeably as speech or conduct in the vast majority of circumstances. The distinction between restrictions based on whether the primary affect impacts speech, conduct, or commodity traditionally plays a significant role in First Amendment jurisprudence, but data, code, and other types of information that are not independently expressive require a renewed approach to assessing the First Amendment boundary. Advertising may require an even more nuanced analysis because it also tends to conflate distinction between commercial speech and commerce in and of itself. Of course, this complicates the task of isolating speech from conduct in First Amendment analysis, but does not render it impossible, as indicated by the *Corley* decision. *Sorrell* does not provide a bright-line rule to assess the scope of First Amendment protection applicable to data. Rather, the opinion reveals a majority that is more likely to engage in a nuanced analysis that places more emphasis on context than medium.

2. Content and Viewpoint Discrimination

The Court effectively sidesteps the issue of whether targeted pharmaceutical marketing should be characterized as commercial or political speech in *Sorrell*. Instead, the Court finds that the exception allowing pharmacies to sell information to academic or research institutions, but not to pharmaceutical marketers, is a content and speaker-based restriction on speech, warranting heightened scrutiny irrespective of its classification.[152] The extent to which *Sorrell* hinges on Vermont's statutory exception is largely determinative of its scope and application to Internet advertising. If the Court's analysis relies on that exception, then privacy regulations that are content and viewpoint neutral presumably escape *Sorrell*'s reach. This aspect of the Court's reasoning suggests that a blanket restriction on the sale of prescription data, prohibiting sales to anyone for any purpose, would trigger a lower standard of scrutiny.

Under the Court's reasoning in *Sorrell*, a neutral statute would certainly not trigger strict scrutiny. However, the majority's apparent resistance to traditional categories of First Amendment scrutiny leaves open the question of whether otherwise neutral regulations would be subject to rational basis review or intermediate scrutiny.[153] While it is unclear exactly how *Sorrell*'s "heightened

---

152 *Sorrell,* 131 S. Ct. at 2657.

153 The majority's application of "heightened scrutiny" falls outside of the three traditionally recognized categories of First Amendment scrutiny (rational basis review, intermediate scrutiny, and strict scrutiny). Other aspects of the opinion seem to imply that the Court's analysis resembles the intermediate scrutiny standard more closely than strict scrutiny standard. "Heightened scrutiny" is either another term for intermediate scrutiny, or an independent

scrutiny" standard compares to the three generally recognized levels of scrutiny belonging to First Amendment jurisprudence (rational basis review, intermediate scrutiny, and strict scrutiny), the Supreme Court has consistently held that regulations on speech which discriminate against speakers based upon the content of their speech are subject to strict scrutiny review.[154] "Heightened scrutiny" thus remains a somewhat ambiguous standard that includes anything more stringent than rational basis review. Yet the Court's articulation of its standard in assessing Vermont's ability to demonstrate "a substantial governmental interest" and to show "that the measure is drawn to achieve that interest," cites several intermediate scrutiny cases, suggesting that "heightened scrutiny" is ostensibly more akin to intermediate scrutiny than strict scrutiny.[155] If *Sorrell*'s heightened scrutiny standard is in fact comparable to intermediate scrutiny, then it follows that other discriminatory regulations would also trigger intermediate scrutiny. It can thus be inferred that a content and viewpoint neutral data privacy regulation would trigger a lower standard than intermediate scrutiny. Therefore, the Court's analysis is consistent with the continued review of content and viewpoint neutral regulations, including several of the proposed consumer privacy bills, under rational basis scrutiny.

On rational basis review, a statute or regulation "comes before the Court bearing a strong presumption of validity, and those attacking its rationality have the burden to negate every conceivable basis that might support it."[156] If the Vermont statute at issue in *Sorrell* had been content and viewpoint neutral, its designated purpose to put generic drugs on a level playing field with brand name drugs and lower the cost of government subsidized health care for the purpose of satisfying public health objectives would almost certainly have survived rational basis review. Similarly then, privacy legislation that does not single out particular uses of data and does not identify specific groups as being subject to certain restrictions while exempting others, should pass constitutional muster under the Court's reasoning in *Sorrell*. Congress could theoretically ban behavioral tracking altogether without violating the First Amendment under *Sorrell*'s reasoning (unless the prohibition applied

---

standard which is more stringent that intermediate scrutiny, but less stringent than strict scrutiny. Witt v. Dept. of the Air Force, 527 F.3d 806 (9th Cir. 2008). Justice Kennedy's articulation of the test in *Sorrell* ("the State must show at least that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest") seems to indicate that its use of "heightened scrutiny" is more akin to the intermediate scrutiny standard. *Sorrell*, 131 S. Ct. at 2667–68.

154 *See e.g.*, Ysursa v. Pocatello Educ. Ass'n, 555 U.S. 353 (2009); Legal Services Corp. v. Velazquez, 531 U.S. 533 (2001); U.S. v. Playboy Entm't Grp., Inc., 529 U.S. 803 (2000); Police Dept. of Chi. v. Mosley, 408 U.S. 92 (1972); Turner Broadcasting System, Inc. v. F.C.C., 512 U.S. 622 (1994); R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).

155 *Sorrell*, 131 S. Ct. at 2667–68 (citing Board of Trustees of State Univ. of N.Y. v. Fox, 492 U.S. 469, 480–81 (1989), and Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980)). The opinion also cites City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410 (1993) and 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484 (1996), both of which are widely cited as "intermediate scrutiny" cases as well. JEFFREY M. SHAMAN, CONSTITUTIONAL INTERPRETATION: ILLUSION AND REALITY 100–02 (2000) (providing a comprehensive history of intermediate scrutiny).

156 F.C.C. v. Beach Commc'ns, Inc., 508 U.S. 307, 307 (1993).

only to specific groups or provided exceptions for certain types of uses). It is improbable, of course, that Congress would consider such drastic measures since the negative economic impact on Internet businesses and innovation of such a plan would drastically outweigh any information privacy benefit to consumers. It is increasingly likely, however, that a framework restricting specific practices and giving legal force to consumer privacy guidelines (requiring consent, for example) will be implemented.

B. *Application to Current Legislative Proposals*

Several months after the decision was published, Thomas R. Julin, the attorney who represented IMS Health before the Supreme Court, published an article assessing *Sorrell*'s potential impact on forthcoming consumer privacy legislation.[157] Julin claimed that recent legislative proposals to implement a comprehensive consumer privacy framework—which he collectively (and erroneously) refers to as "Do Not Track Acts"—were based on similarly lackluster justifications to those that were offered to support the Vermont statute.[158] Then, without further analysis, without addressing how such laws would impose unconstitutional restrictions on speech, and without contemplating whether such proposals contain content or viewpoint discrimination, Julin concluded that any legislative proposals embodying Do Not Track principles would surely be subject to the same fate as the Vermont statute under *Sorrell*.[159]

Like much of the earlier speculation about *Sorrell*'s scope and application, Julin's analysis with respect to recent legislative proposals is conclusory and misguided. To begin with, *Sorrell* does not address data collection, which is the primary concern in many of the current legislative proposals. Thus, *Sorrell* probably does not extend to regulations that impose restrictions on data collection without touching upon how that data is used. More importantly, according to the Court's analysis, the act of collecting data can only be characterized as speech to the extent that it directly supports an expressive function—otherwise, it can just as easily be characterized as non-expressive conduct, which is not protected by the First Amendment.[160] Therefore, data privacy regulations that concern only non-expressive aspects of the ad-targeting process would also escape a First Amendment challenge under *Sorrell*. Furthermore, a regulation would have to contain viewpoint or content discrimination to warrant the heightened scrutiny standard applied in *Sorrell*. As a result, a blanket restriction on unauthorized data transactions, containing no exceptions for certain entities or purposes, would presumably trigger only rational basis scrutiny, even

---

157 Thomas R. Julin, Sorrell v. IMS Health *May Doom Federal Do Not Track Acts,* 10 PRIV. & SEC. L. REP. 25 (2011), *available at* http://www.huntonprivacyblog.com/tag/thomas-julin.

158 *See* sources cited *supra* notes 96, 104, 105, *infra* notes 163, 164; Julin, *supra* note 157 (referring to these bills collectively as the "Do Not Track Acts" although a handful of them do not touch upon online tracking).

159 *See* Julin, *supra* note 157.

160 *Id.*

if it was directly related to an expressive function; and the Court would surely recognize the legitimacy of consumer privacy interests associated with legislative proposals of the Do Not Track variety (most of which regulate data collection irrespective of who is collecting the data or what they intend to do with it) under rational basis review. Finally, even if such a statute were to trigger heightened scrutiny, *Sorrell* does not foreclose the possibility that the Court would recognize a substantial government interest in protecting consumer privacy.

Speculation that *Sorrell* preempts the majority of consumer privacy bills currently before Congress requires a series of unwarranted assumptions about the substance of those proposals which Julin and other commentators fail to even consider. According to *Sorrell*, consumer privacy legislation could be deemed unconstitutional if (1) it imposes restrictions on expressive uses of data (i.e. it burdens protected speech); (2) its restrictions discriminate against speakers based upon the content of their speech; and (3) the burden placed on protected expression by the statute cannot be justified by the government's asserted interest in privacy or the statute is not narrowly tailored to advance the public interest in privacy on the Internet.[161] Consumer privacy bills currently before Congress simply do not contain the same defects as Vermont's Prescription Confidentiality law. The following charts summarize the Supreme Court's Analysis of the Vermont Prescription Confidentiality Law in *Sorrell* and apply its analysis to consumer privacy bills currently before Congress:

TABLE 1: Supreme Court's Analysis of Vermont Prescription Confidentiality Law in *Sorrell v. IMS Health*[162]

Title	Restriction on Expressive Use of Data	Content Discrimination	Viewpoint Discrimination
Vermont Prescription Confidentiality Law	Prohibits selling, disclosure, or use of prescription data without consent from the prescribing doctor.	Prohibition extends only to data used for "marketing purposes"; creates an exception for educational and other uses	Affects pharmaceutical companies, marketers, and data miners disproportionately

161 *See generally id.*
162 Sorrell v. IMS Health, Inc., 131 S. Ct. 2653 (2011).

TABLE 2: Application of *Sorrell* to Privacy Legislation Currently Before Congress [163]

Title	Restriction on Expressive Use of Data	Content Discrimination	Viewpoint Discrimination
Personal Data Privacy and Security Act	*NONE: impacts how data is collected, maintained, and stored, but not how it is used*	*NONE: Does not specify content (applies equally to all uses of data)*	Applies to "data brokers"
Do Not Track Online Act	*NONE: impacts only how data is collected, not how it is used*	*NONE: Does not specify content (applies equally to all uses of data)*	Applies to online service providers, including providers of mobile applications and services
Consumer Privacy Protection Act	Prohibits sale or disclosure of data collected about an individual where that individual has indicated preference to have their personal data precluded from such uses (depends on whether sale and disclosure are "expressive" uses of data)	*NONE: Does not specify content (applies equally to sale and disclosure of data for any purpose)*	*NONE: Does not target a particular group of speakers; one could argue that it disproportionately impacts data miners, but provisions would affect companies that only incidentally collect or aggregate data in the same way*
Commercial Privacy Bill of Rights	Prohibits any unauthorized use of data collected about an individual without that individual's consent (captures expressive and non-expressive uses)	Prohibition extends to "any use," including but not limited to "behavioral advertising or marketing," BUT creates exceptions for purposes of providing services requested by that individual, fraud prevention and detection, or to provide for a secure physical or virtual environment	Does not target a particular group of speakers since it applies to "all entities," yet could impact marketers and data miners disproportionately in its application
Do Not Track Me Online Act	Prohibits use of data pertaining to an individual that has elected to opt-out pursuant to mandatory opt-out provision (captures both expressive and non-expressive uses)	Does not specify content (applies equally to all uses of data), BUT gives FTC authority to exempt certain uses from regulation	Does not target a particular group of speakers, yet could impact marketers and data miners disproportionately in its application
BEST PRACTICES Act	Prohibits any unauthorized use of non-public data collected about an individual without that individual's consent (captures expressive and non-expressive uses)	Does not specify content (applies equally to all uses of data), BUT creates exceptions for purposes of providing services, fraud prevention and detection, emergencies and legitimate government request	Does not target a particular group of speakers, yet could impact marketers and data miners disproportionately in its application
Do Not Track Kids Act	Prohibits use and disclosure of data collected from known minors (captures both expressive and non-expressive uses)	Prohibition extends only to data used for "targeted marketing purposes"	Affects children's websites and marketers disproportionately

Applying the Court's reasoning in *Sorrell* to current legislative proposals, two of the bills in question—the Personal Privacy and Security Data Act and the Do Not Track Online Act[164]—would not

[163] Personal Data Privacy and Security Act, S. 1151, 112th Cong. (2011); Do Not Track Online Act, S. 913, 112th Cong, (2011); Consumer Privacy Protection Act, H.R. 1528, 112th Cong. (2011); Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. (2011); Do Not Track Me Online Act, H.R. 654, 112th Cong, (2011); Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (BEST PRACTICES) Act, H.R. 611, 112th Cong. (2011); Do Not Track Kids Act, H.R. 1895, 112th Cong. (2011).

[164] Personal Privacy and Security Data Act, S. 1151; Do-Not Track Online Act, S. 913.

even be subject to First Amendment scrutiny because they do not impose restrictions on expressive uses of data. *Sorrell* broadly characterized the creation and dissemination of information as speech for First Amendment purposes, but the majority's analysis clearly indicated that data regulations are only deemed to impose a restriction on speech to the extent that they limit the ways in which that data may be used.[165] Here, the regulations only restrict the ways in which data is collected or gathered—not the way that data is subsequently used. As a result, *Sorrell* does not apply to those statutes. The Consumer Privacy Protection Act, on the other hand, could be said to impose restrictions on speech since it affects the actual sale and disclosure of data rather than just regulating ways in which such data is collected. Nevertheless, the Consumer Privacy Protection Act escapes *Sorrell* because it does not constitute content or viewpoint discrimination.[166] While the other statutes could be found at least somewhat discriminatory because they provide certain exceptions or have disproportionate affects on certain speakers, the Consumer Privacy Protection Act applies broadly across the board to any entity that sells or discloses data pertaining to an individual.[167] *Sorrell*'s application to the Commercial Privacy Bill of Rights Act, the Do Not Track Me Online Act, the BEST PRACTICES Act, and the Do Not Track Kids Act by contrast, require a slightly more nuanced analysis.[168]

1. The Commercial Privacy Bill of Rights Act

The CPBRA is the most important of all proposed legislation because its structure is consistent with the Obama administration's renewed call for Congressional action on consumer privacy. In February 2012, the White House released a second report on consumer privacy, seeking the enactment and codification of a Consumer Privacy Bill of Rights.[169] The report endorses a rights-based approach to consumer privacy legislation, and signals the probable introduction of additional legislative proposals. While the CPBRA precedes the White House report, its construction parallels the framework articulated by the administration, and provides insight into the potential construction of future legislative proposals likely to gain wider support in Congress.

CPBRA prohibits any unauthorized use of data collected about an individual without that individual's consent.[170] The consent requirement extends to both expressive and non-expressive uses of

---

165 *Sorrell*, 131 S. Ct. at 2657, 64-67. *See also* "Data as Speech" *infra* Part III.A.1.

166 *See supra* Table 2 (noting that the Consumer Privacy Protection Act does not specify a particular type of content or group of speakers as the target of its restrictions on data uses). The bill's provisions apply to *any* entity that "collects (by any means, through any medium), sells, discloses for consideration, or uses personally identifiable information of more than 5,000 consumers during any consecutive 12-month period." H.R. 1528, § 3.

167 *Id.*

168 Commercial Privacy Bill of Rights Act, S. 799; Do Not Track Me Online Act, H.R. 654; BEST PRACTICES Act, H.R. 611; Do Not Track Kids Act, H.R. 1895.

169 WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

170 Commercial Privacy Bill of Rights Act , S. 799, 112th Cong. (2011).

an individual's data, meaning that CPBRA's constitutionality under *Sorrell* could hinge on whether its restrictions discriminate against speakers based upon the content of their speech.

Unlike the Vermont Prescription Confidentiality Law, which specifically imposed its restrictions on marketing, CPBRA does not explicitly target a particular type of content. However, CPBRA, like the Vermont statute, does exempt certain specified uses from its restrictions. CPBRA creates exceptions to its consent requirement where an entity's purpose in using the data is to provide the individual in question with services that individual has requested.[171] The statute also provides an exception for purposes related to fraud prevention and cybersecurity.[172] Yet these exceptions are fundamentally different from those the Court took issue with in *Sorrell*. Vermont's exception allowing prescription data to be used for public health or educational purposes, while restricting its use for marketing purposes, was considered particularly offensive because its effect rose to the level of viewpoint discrimination—it created a situation where a pharmaceutical company might be barred from using prescription data to promote a new drug, while a nonprofit public health organization would be allowed to access the same data for the purpose of creating public health communications promoting the use of the generic competitor to that very drug.[173] The CPBRA exceptions, by contrast, do not rise to the level of viewpoint discrimination as they merely serve to facilitate service providers' operations where an individual has already provided implied consent. Any individual who knowingly provides information to an Internet service likely expects that the same information can be used to fulfill a request he or she makes of that same service. In addition, it is difficult to imagine a scenario in which an individual would object to the same data being used pursuant to his or her interest in fraud prevention and cybersecurity with respect to that service. In other words, the exceptions are justifiable because any user's intent in providing information to an online service embodies an implied consent to use the information for those purposes.

Opponents of CPBRA could still argue that the statute has a discriminatory effect in spite of its otherwise neutral application. Marketers could argue, for example, that although the consent requirement applies to all entities alike, individuals are less likely to consent to marketing uses, and so the statute disproportionately affects marketers in its application. While plausible, this line of reasoning is a distant divergence from the viewpoint analysis in *Sorrell*.

Assuming *arguendo* that CPBRA were found to impose content and speaker based restrictions on speech, it would also be more likely to overcome even heightened scrutiny on the merits of its justification. Vermont's Prescription Confidentiality law was

---

171 *Id.* § 202.
172 *Id.*
173 *Sorrell*, 131 S. Ct. at 2662–63.

designed to level the playing field for all participants, but essentially picked winners by giving advantage to one group. Its purported interest in doing so was to protect medical privacy and reduce healthcare costs by attempting to put generic drugs on a level playing field with name-brand pharmaceuticals.[174] The Court rejected these justifications, in part, because they found the statute was not drawn to support its objectives.[175] CPBRA is designed to protect individual's right to and interest in personal privacy on the Internet, with the goal of fostering trust in the treatment of that information to support the development of Internet commerce.[176] Because CPBRA establishes a direct relationship between a widely recognized harm (unauthorized and negligent data practices) and provides a narrow and specific remedy (requiring consent, accountability, and strict adherence to principles that acknowledge and respect individual's rights on the Internet), it would be very difficult to argue that the bill does not support its stated objectives under any standard of First Amendment scrutiny.[177]

2. The Do Not Track Me Online Act and The BEST PRACTICES Act

The Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, or the "BEST PRACTICES" Act, and the Do Not Track Me Online Act are very similar to CPBRA for First Amendment purposes, and would probably surpass constitutional muster under *Sorrell* for the same reasons. The BEST PRACTICES Act, like CPBRA, prohibits unauthorized use of data collected about an individual without that individual's consent, and has almost identical exceptions.[178] The Do Not Track Me Online Act requires covered entities to provide an opt-out mechanism, allowing individuals to "effectively and easily prohibit the collection or use" of their personal data.[179] One possibly significant difference with respect to the Do Not Track Me Online Act, however, is that it entrusts the FTC with authority to create exceptions to the applicability of its regulations.[180] Accordingly, the constitutionality of FTC regulations created pursuant to this law would depend in part on the nature of those exceptions, and their impact on the relative neutrality of that statute's application.

3. The Do Not Track Kids Act

The Do Not Track Kids Act[181] amends the Children's Online Privacy Protection Act (COPPA)[182] to extend, enhance, and revise

174 *Sorrell*, 131 U.S. at 2668.
175 *Id.*
176 S. 799.
177 S. 799.
178 H.R. 654, 112th Cong. (2011).
179 *Id.* § 3.
180 *Id.*
181 H.R. 1895, 112th Cong. (2011).
182 15 U.S.C. §§ 6501–6506 (2006).

the provisions relating to parental control over the collection, use, and disclosure of personal information of children.[183] The bill disproportionately affects children's websites, arguably constituting viewpoint discrimination under the criteria set forth in *Sorrell*. However, the bill would most likely overcome even the strictest standard of scrutiny because it supports parental rights, which the Court has repeatedly held to be more important than other fundamental liberty interests.[184] Therefore, the Do Not Track Kids Act would also likely withstand a First Amendment challenge under *Sorrell* and other First Amendment precedent.

CONCLUSION

The tension between regulatory efforts and freedom of expression with respect to targeted advertising is just one example of the increasing politicization of Internet policy, which is beholden by ideological warfare between Internet libertarians and those who favor a regulatory framework.[185] The former group appropriated *Sorrell* as a poster-child for its First Amendment assault on regulatory efforts related to data and the Internet.

Sorrell initially sparked considerable intrigue and controversy, but its application to forthcoming regulations is actually quite limited. At first glance, it seemed as though *Sorrell* could have preempted any and all regulations restricting the use of data-driven ad-targeting techniques. But the majority's reasoning clearly indicates that *Sorrell*'s capacity to preempt regulatory efforts is limited to statutes that impose content and speaker based restrictions on expressive uses of data. A thorough analysis of the decision reveals that *Sorrell* leaves much flexibility for policymakers to craft baseline consumer privacy legislation.

Legislators and policymakers should attempt to understand *Sorrell* as a blueprint for legislation. The decision ultimately provides a clear test to determine when data should be treated as speech and when restrictions on its use will be subject to a heightened level of scrutiny under the First Amendment. *Sorrell* does not preempt forthcoming consumer privacy legislation, but merely

---

183 H.R. 1895, 112th Cong. (2011).

184 "The law has traditionally recognized that parents are uniquely situated to raise their children, which necessarily entails protecting their children from certain risks . . . . The extent to which a child's name is disclosed and publicly disseminated on the Internet is another risk over which parents maintain responsibility and control." Sec. Indus. & Fin. Mkts. Ass'n v. Garfield, 469 F. Supp. 2d 25, 36–37 (D. Conn. 2007) (citing Pierce v. Soc'y of Sisters, 268 U.S. 510, 534–35 (1925) (the "liberty of parents and guardians" includes the right "to direct the upbringing and education of children under their control"); United States v. Myers, 426 F.3d 117, 125 (2d Cir. 2005) ("[T]he fundamental right of parents to make decisions concerning the care, custody, and control of their children [is] perhaps the oldest of the fundamental liberty interests recognized by" the Supreme Court.); Wilkinson *ex rel.* Wilkinson v. Russell, 182 F.3d 89, 104 (2d Cir. 1999) ("[P]arents enjoy a constitutionally protected interest in their family integrity . . . ."); Fay v. S. Colonie Cent. Sch. Dist., 802 F.2d 21, 26 (2d Cir. 1986) ("[A] parent has a fundamental interest in his child's upbringing.")).

185 *See generally, e.g.*, Aaron Burstein et. al., *Foreword: The Rise of Internet Interest Group Politics*, 19 BERKELEY TECH. L.J. 1 (2004); Marci A. Hamilton, *The Distant Drumbeat: Why the Law Still Matters in the Information Era*, 20 CARDOZO ARTS & ENT. L.J. 259 (2002); Bradford L. Smith, *the Third Industrial Revolution: Policymaking for the Internet,* 3 Colum. Sci. & Tech. L. Rev. 1, 32–76 (2001).

forces lawmakers and regulators to be more creative in drafting laws that do not favor certain content or speakers over others. Therefore, consumer privacy advocates and their allies should embrace *Sorrell* to the extent that it provides them with a guide for enacting a framework that will pass Constitutional muster.

Agatha M. Cole[*]

[*] Executive Editor, CARDOZO ARTS & ENT. L.J. (Volume 31), J.D. Candidate, Class of 2013, Benjamin N. Cardozo School of Law; B.A., *cum laude*, New York University, Class of 2008. Many thanks to Professor Brett Frischmann, Professor Felix Wu, Aaron Burstein, and the editorial staff of the *Cardozo Arts & Entertainment Law Journal* for their expertise, advice, and encouragement in writing this Note. Thank you also to my friends and family, and especially to my mother, Tatine Darker, for being an endless source of support and inspiration.