William & Mary Law Review

Volume 56 | Issue 4 Article 12

Why Data Privacy Law Is (Mostly) Constitutional

Neil M. Richards

WHY DATA PRIVACY LAW IS (MOSTLY) CONSTITUTIONAL

NEIL M. RICHARDS*

ABSTRACT

Laws regulating the collection, use, and disclosure of personal data are (mostly) constitutional, and critics who suggest otherwise are wrong. Since the New Deal, American law has rested on the wise judgment that, by and large, commercial regulation should be made on the basis of economic and social policy, rather than blunt constitutional rules. This has become one of the basic principles of American constitutional law. Although some observers have suggested that the United States Supreme Court's recent decision in Sorrell v. IMS Health Inc. *changes this state of affairs, such readings are incorrect.* Sorrell *involved a challenge to a poorly drafted Vermont law that discriminated on the basis of both content and viewpoint. Such a law would have been unconstitutional if it had regulated even unprotected speech. As the* Sorrell *Court made clear, the real problem with the Vermont law at issue was that it did not regulate enough, unlike the "more coherent policy" of the undoubtedly constitutional federal Health Insurance Portability and Accountability Act of 1996.*

Data privacy law should thus rarely be thought of as implicating serious constitutional difficulties, and this is a good thing. As we move into the digital age, in which more and more of our society is affected or constituted by data flows, we face a similar threat. If "data" were somehow "speech," virtually every economic law would become clouded by constitutional doubt. Economic or commercial

* Professor of Law, Washington University. This Article is adapted from chapter five of my book, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 73-91 (2015). Extracts from this chapter are printed by permission of Oxford University Press, USA (www.oup.com). For helpful comments and suggestions, I would like to thank my co-participants at the *William & Mary Law Review* Symposium, especially my copanelist Julie Cohen and my Washington University colleagues Greg Magarian and John Inazu.

policy affecting data flows—which is to say all economic or social policy—would become almost impossible. This might be a valid policy choice, but it is not one that the First Amendment commands. Any radical suggestions to the contrary are unsupported by our constitutional law. In a democratic society, the basic contours of information policy must ultimately be up to the people and their policy-making representatives, and not to unelected judges. We should decide policy on that basis, rather than on odd readings of the First Amendment.

TABLE OF CONTENTS

INTRODUCTION

Privacy and free speech are siblings with a long and complicated relationship. Both have a common parent in Justice Louis Brandeis, and for over a century they have developed together. Like siblings, they have sometimes bickered, but as they have matured they have often gone their own ways. Privacy and free speech can each mean many things, so we should not be surprised that this is the case.[1]

Although both privacy and free speech are products of earlier centuries, we now live in an age of personal information. Such personal information drives the economy and can be used to influence policy, our elections,[2] our identities,[3] and even our moods.[4] This is the case whether we call it "personal information" or the currently fashionable buzzword "big data." Whatever we call it, information is power. That power is neither inherently good nor inherently bad; it is merely a social reality that we have to live with.[5]

Democratic societies usually regulate complex social realities. We have laws dealing with industrialization and pollution, with market capitalism and fraud, and with social equality and racism. Although social norms and practices remain important, complex social realities are also typically a subject for law and legal regulation. Nevertheless, sometimes we decide that democratic regulation is too dangerous, even for complex social problems. Thus, most democratic societies deny themselves the power to police the field of public debate or the marital choices of consenting adults. In the United

1. *See* Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1343 (2010).

2. *See* Sasha Issenberg, *A More Perfect Union: How President Obama's Campaign Used Big Data to Rally Individual Voters*, MIT TECH. REV. (Dec. 19, 2012), http://www.technologyreview.com/featuredstory/509026/how-obamas-team-used-big-data-to-rally-individual-voters/ [http://perma.cc/5C69-ZJF6].

3. *See* Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 43-44 (2013) http://www.stanfordlawreview.org/sites/default/files/online/topics/66_StanLRevOnline_41_RichardsKing.pdf [http://perma.cc/SFU5-CGSC].

4. *Journal That Published Facebook Mood Study Expresses "Concern" at Its Ethics*, GUARDIAN (July 3, 2014, 9:10 PM), http://www.theguardian.com/technology/2014/jul/04/journal-published-facebook-mood-study-expresses-concern-ethics [http://perma.cc/TY5R-HY58].

5. Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 395, 432 (2014).

States—in sharp contrast to the rest of the world—issues of campaign finance and market power,[6] hate speech and equality,[7] and, increasingly, gun possession and violence[8] seem to be entering this category of "too dangerous to regulate." We lawyers typically call such laws "unconstitutional," finding that they violate some provision of the Constitution, such as the First, Second, or Fourteenth Amendments.

My goal in this Article is to explain why regulation of the commercial trade in personal data will be consistent with the First Amendment, at least most of the time. Blanket assertions that regulation of personal information flows threatens freedom of expression misunderstand either the nature of data privacy law, the nature of First Amendment rights, or both. A few kinds of privacy rights certainly run into conflict with the First Amendment, most notably the old Warren and Brandeis argument for a tort by which the rich and famous could keep unflattering and embarrassing truths about themselves out of the newspapers.[9] But privacy can mean many things, and most of these things are fully consistent with the American commitments to the broad rights of freedom of speech and press. Our laws use the term "privacy" to refer to the many laws regulating personal data, including consumer credit and video rental information and information given to doctors and lawyers. Despite calls from industry groups and a few isolated academics that these laws somehow menace free public debate, the vast majority of information privacy law is constitutional under ordinary settled understandings of the First Amendment.[10] Policymakers can

6. *See, e.g.*, McCutcheon v. FEC, 134 S. Ct. 1434, 1442 (2014) (holding that a law imposing aggregate limits on individuals' campaign contributions violated the First Amendment); Citizens United v. FEC, 558 U.S. 310, 365-66 (2010) (holding that the government cannot suppress political speech on the basis of the speaker's corporate identity and striking down portions of the Bipartisan Campaign Reform Act of 2002 restricting corporate expenditures for electioneering communications as unconstitutional).

7. *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 391 (1992) (striking down a hate crime statute because it discriminated against racist viewpoints and thus violated the First Amendment).

8. *See, e.g.*, District of Columbia v. Heller, 554 U.S. 570, 635 (2008) (holding that a ban on possession of handguns in the home violated the Second Amendment).

9. *See infra* notes 19-21 and accompanying text.

10. *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1155 (2005) ("[W]hen the First Amendment and privacy have come into conflict in the past, ... the First Amendment has universally triumphed.").

thus make information policy on the merits rather than being distracted by spurious free speech claims.

Throughout the world, democratic societies regulate personal data using laws that embody the "Fair Information Practices" or FIPs. The FIPs are a set of principles that regulate the relationships between business and government entities that collect, use, and disclose personal information about "data subjects," and which were developed by the United States government in the 1970s.[11] Over the past decade, some—but not all—industry groups and a handful of scholars have argued that the FIPs somehow offend the First Amendment.[12] This is an argument seemingly strengthened by the Supreme Court's 2011 decision in *Sorrell v. IMS Health Inc.*, which struck down a Vermont law preventing drug company representatives—but no one else—from using data-based marketing to speak to physicians.[13]

Before *Sorrell*, there was a settled understanding that general commercial regulation of the huge data trade was not censorship. On the contrary, it was seen as part of the ordinary business of commercial regulation that fills thousands of pages of the United States Code and the Code of Federal Regulations. Nothing in the *Sorrell* opinion should lead policymakers to conclude that this settled understanding has changed. The poorly drafted Vermont law in *Sorrell* discriminated against particular kinds of protected speech (in-person advertising) and particular kinds of protected speakers (advertisers but not their opponents).[14] Such content- and viewpoint-based discrimination would doom even *unprotected speech* under well-settled First Amendment law. As the Court made clear, the real problem with the Vermont law at issue was that it did not regulate *enough*, unlike the "more coherent policy" of the undoubtedly

11. *See generally* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

12. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1115-17 (2000).

13. 131 S. Ct. 2653, 2672 (2011).

14. *Id.* at 2660.

constitutional federal Health Insurance Portability and Accountability Act of 1996.[15]

Notwithstanding the Court's clarity on this point, a few observers have suggested that data flows are somehow "speech" protected by the First Amendment. But the "data is speech" argument makes no sense from a First Amendment perspective. People do things with words every day that are clearly "speech": from blogging and singing in the shower, to insider trading, sexually harassing coworkers, verbally abusing children, and even hiring assassins. Well-settled First Amendment doctrine allows us to separate out which of these activities cannot be regulated (the first two) from those which can (the rest).[16] First Amendment lawyers do not ask whether something is "speech," because almost everything is expressive in some way. Instead, they ask which kinds of government regulation are particularly threatening to longstanding First Amendment values. The question is not the "speechiness" of the *human activity* being regulated, but the purpose and effect of the *government regulation*. When we look at the regulation of commercial data flows from this basic, unobjectionable premise of First Amendment law, we see that such regulations will rarely be problematic. Commercial regulation—of sexual harassment, unfair trade practices, and commercial data flows based on the FIPs—is thus rarely threatening to First Amendment values, properly understood by their settled meaning.

A more fundamental reason supports this conclusion as well. During the New Deal, American society decided that, by and large, commercial regulation should be made on the basis of economic and social policy rather than blunt constitutional rules.[17] This has become one of the basic principles of American constitutional law. As we move into the digital age, in which data flows affect or even constitute more and more of our society, we face a similar threat. If "data" were somehow "speech," and this had First Amendment consequences, constitutional doubt would cloud virtually every form of economic regulation we have. Economic or commercial policy affecting data flows, which is to say all economic or social policy, would

15. *Id.* at 2668 (quoting Greater New Orleans Broad. Ass'n. v. United States, 527 U.S. 173, 195 (1999)).

16. *See infra* notes 115-22 and accompanying text.

17. *See infra* notes 130-34.

become almost impossible. This might turn out to be a valid policy choice, but it is not one that the First Amendment as we have understood it until now commands. Any radical suggestions to the contrary are unsupported by our constitutional law. Indeed, they are an attempt to make radical changes to the basic contours of that law.

Privacy law is thus (mostly) constitutional. And when we are talking about the regulation of commercial data flows, it is entirely constitutional, except for a few poorly drafted outliers, such as the law struck down in *Sorrell*. In a democratic society, the basic contours of information policy must ultimately be up to the people and their policy-making representatives, and not to unelected judges. We should decide policy on that basis, rather than on odd readings of the First Amendment.

I. TWO KINDS OF PRIVACY RIGHTS

Privacy as a concept has proven notoriously hard to define. This is not because privacy is unimportant. On the contrary, it is the importance of privacy as a value that has caused us to add many different and sometimes contradictory meanings to the term. One leading conceptual work on the subject, for example, defines privacy as having sixteen different dimensions.[18] Although there are many different ways to describe things we might want to label as "private," when it comes to legal questions of privacy and free expression, two kinds of privacy matter the most.

The first kind of privacy is tort privacy. This is the classic formulation of privacy as a right to prevent speakers, usually the press, from publishing true but embarrassing facts on the grounds that they cause emotional harm or distress.[19] This is the classic argument from Warren and Brandeis's 1890 article *The Right to Privacy*, codified into American tort law by the work of the eminent torts scholar William Prosser from the 1940s through the 1970s.[20] In prior work, I have argued that the classic notion of

18. *See generally* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008) (proposing a "taxonomy" of privacy encompassing sixteen categories illustrating privacy problems).

19. Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMMS. & HIGH TECH. L. 357, 359-60 (2011).

20. *Id.* at 363-64.

privacy—Warren and Brandeis's disclosure tort against the press—is largely inconsistent with the First Amendment as we understand it today. The main problem with the tort is the form its regulation takes: it targets the press for publishing the embarrassing truth under a blurry standard. In a post-*New York Times v. Sullivan* era, punishing the press for publishing newsworthy truth is at the core of what the First Amendment should protect, and appropriately so.[21]

But privacy can mean many things beyond the right to prevent the press from making embarrassing disclosures about us. In fact, given its First Amendment problems, the tort form of privacy that protects us against embarrassing but true disclosures is likely to have limited utility outside the problem of "revenge porn" or nonconsensual pornography. Increasingly, when we say "privacy" in a digital age, we are concerned not with publication by newspapers, but rather with the collection, disclosure, and use of our personal information by known and unknown government and corporate entities.[22] We also use the term "privacy" to refer to the many laws regulating personal data, including consumer credit and video rental information, and information given to doctors and lawyers.[23] Let us call this second kind of privacy "data privacy" to distinguish it from tort privacy. Are these data privacy rules also unconstitutional?

Throughout the world, democratic societies regulate personal data using laws that embody the FIPs. The FIPs are one of the most important concepts in privacy law. They are a set of principles that regulate the relationships between business and government entities that collect, use, and disclose personal information about "data subjects"—the ordinary people whose data is being collected and used.[24] Perhaps ironically, the FIPs were developed by the United States government in the 1970s because the government wanted to establish some minimal best practices for the processing of personal data.[25] The government report that announced the FIPs described

21. *Id.* at 368, 373-74.

22. Richards & King, *supra* note 5, at 410-11.

23. *Id.*

24. SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., *supra* note 11, at xxii-xxiii.

25. *Id.*

them as "five basic principles" to which automated data systems must adhere:

> There must be no personal data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[26]

The FIPs were embodied into law in the United States in the Privacy Act and the Fair Credit Reporting Act, and then spread throughout the world.[27] They have different meanings in different places and contexts, but at bottom the FIPs guarantee that data is processed according to fair rules that give data subjects *notice* about how their data is collected and used, and some *choice* about certain uses of their data.[28] They are the foundation of the Organization of Economic Cooperation and Development's privacy guidelines and the basis for the European Union's 1995 European Community Directive on Data Protection, a framework governing data collection and use in the European Union that requires EU member states to adopt their own country-specific data protection laws.[29] Joel

---

26. *Id.* at xx-xxi.

27. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)); Fair Credit Reporting Act of 1970, Pub. L. No. 90-32, 84 Stat. 1128 (codified as amended at 15 U.S.C. § 1681 (2012)); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶¶ 44-47 (2001), https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/rotenberg-fair-info-practices.pdf [http://perma.cc/J3AA-R5Z5] (discussing how the FIPs have "contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection").

28. *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., *supra* note 11, at xx-xxi.

29. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 37-40 (4th ed. 2011).

Reidenberg summarized the evolved FIPs as guaranteeing four basic protections against data misuse: (1) standards for *data quality*, which ensure that data is acquired legitimately and is used in a manner consistent with the purpose for which it was acquired; (2) standards for *transparency* or openness of processing, such as giving individuals meaningful notice regarding how their information is being used; (3) special protections for *sensitive data* (for example, race, sexual preference, political views, or telephone numbers dialed), such as requiring opt-in consent before such data may be used or disclosed; and (4) some standards of *enforcement* to ensure compliance.[30]

The FIPs have been remarkably durable, but legislators have proposed other principles from time to time. In January 2012, E.U. regulators proposed revisions to the almost-twenty-year-old Data Protection Directive.[31] The most controversial of these was the proposal of a new fair information principle, "Le Droit à l'Oubli," commonly translated into English as "The Right to Be Forgotten."[32] The right to be forgotten, which was popularized by Victor Mayer-Schönberger in his 2009 book, *Delete*, is the idea that at some point, personal data should be deleted, rather than persist in databases forever.[33] Implementation of this right into the FIPs could take several forms. On one hand, it could be a somewhat innocuous general requirement that data not last forever, like the requirements in the Fair Credit Reporting Act or the Video Privacy Protection Act that records from background checks or of movie watching be destroyed as soon as is practicable.[34] On the other hand, the right to be forgotten could be interpreted as a right to have websites remove

30. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 514-16 (1995).

31. Press Release, Eur. Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm [http://perma.cc/X3NK-EM9Y].

32. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012) http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf [http://perma.cc/T6GG-RVGT].

33. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE, ix, 12-15, 198-99 (2009).

34. 15 U.S.C. § 1681w (2012) (discussing the disposal of records in the consumer financial information context); 18 U.S.C. § 2710(e) (2012) (discussing the destruction of old records in the context of video tape rental or sale records).

personal data, images, or news stories that a person thought violated their right to privacy. Under this view, the right to be forgotten would turn the web into our own personal Wikipedia, giving us the right to edit data about ourselves as we like. The version of the right proposed by the European Union in 2012 seems to be of this latter, stronger sort.[35]

Taking a step back, it is important to consider the constitutional status of these rules—not just the right to be forgotten, but the FIPs as a whole. These questions are some of the most important questions we face in our increasingly digital society, and they are the ones I will examine in this Article. Do the FIPs restrict protected free speech? If so, are they unconstitutional in whole or in part? More generally, if Warren and Brandeis's conception of privacy is largely inconsistent with the First Amendment, what about rules that regulate the disclosure of personal data in the marketplace? Must we extend the First Amendment critique of privacy against the press to all nondisclosures rules? Is privacy always a threat to free speech?

My argument in this Article is that the answers to these questions should generally be "no." Most data privacy regulations do not involve the First Amendment because they do not restrict the flow of data, much less the freedom of speech. Rules placing nondisclosure obligations on data processors will rarely place burdens on First Amendment values, especially if they are couched as confidentiality rules. A few such rules, such as a broad view of the right to be forgotten, might certainly threaten free speech, especially as they come to look more like the disclosure tort. But in general, applying the FIPs to databases and data processing of ordinary commercial data is not censorship, and treating such rules as being outside the central concern of the First Amendment is consistent with the better reading of First Amendment law.

This conclusion is not just a better reading of the legal doctrine; the question of whether data privacy rules censor free speech raises the question of whether we can regulate data flows at all. In a society in which data flows are becoming increasingly important,

35. CTR. FOR DEMOCRACY & TECH., ON THE "RIGHT TO BE FORGOTTEN": CHALLENGES AND SUGGESTED CHANGES TO THE DATA PROTECTION REGULATION (2013), *available at* http://perma.cc/U2J4-T3B8.

this is akin to asking whether we can have commercial regulation at all. Good policy, as well as our constitutional traditions of democratic self-government, counsel against a broad and dangerous reading of the First Amendment that somehow equates "data" with "speech."

The best place to begin is with the FIPs. The FIPs are a code of best practices for the handling of personal information by businesses and government.[36] They can inform both the practices of corporate and government entities, and also be embodied in substantive legal rules. But statutes embodying the FIPs do far more than merely regulating information flows or preventing disclosures. Paul Schwartz has shown that under Reidenberg's four-part taxonomy of fair information practices, principle one, ensuring data quality; principle two, ensuring transparency of processing; and principle four, ensuring enforcement, simply have nothing to do with speech under anyone's definition.[37] Only principle three, which provides protection against the use or disclosure of sensitive data, reflects the notion that information privacy prevents other people from talking about you.[38] Thus, even if you accept the idea that nondisclosure rules create First Amendment problems, major forms of information privacy protection envisioned by codes of fair information practices and protected by current laws have nothing whatsoever to do with the First Amendment.[39]

As for rules regulating disclosure of commercial data transfers, the vast majority of these rules are consistent with the First Amendment. The obligation that a university should keep its students' records confidential, for example, is very different from the old Warren and Brandeis tort. It is one thing to gag the press in its entirety from reporting on Mabel Warren's dinner parties, and quite another to require a university to keep its student records presumptively secret. This confidentiality rule does not target the press, police an unwieldy line between public and private, or remedy primarily emotional harm. Instead, the Family Educational Rights and Privacy Act of 1974, the federal statute that imposes this

36. See *supra* notes 24-26 and accompanying text.

37. Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1561-62 (2000).

38. *Id.* at 1561-63.

39. Richards, *supra* note 10, at 1167-68.

confidentiality requirement, regulates the "education records" of a university, carefully defines the records that are within its scope, and governs the relationship between university and student.[40] Other statutes embodying the FIPs operate similarly, and rather than targeting news reports of celebrities, at their best the statutes protect the confidentiality of the information we need to live our lives, such as our library, medical, and financial records.[41] Generally applicable regulation of commercial data simply does not raise the First Amendment concerns that the disclosure tort does,[42] and confidentiality rules that regulate the obligations of parties to a relationship, rather than whether someone can publish a fact, pose even fewer First Amendment problems.[43]

Not everyone agrees with me on this point, including some technologists, academics, and corporate lobbyists. For example, in an influential article, Eugene Volokh argues that most privacy rules are inconsistent with free speech.[44] Considering the various "codes of fair information practices" imposed by law upon commercial processors of personal data, Volokh asserts that "the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me."[45] He argues that although private agreements to restrict speech are enforceable under contract law, any broader, government-imposed code of fair information practices that restricts the ability of speakers to communicate truthful data about other people is inconsistent with the most basic principles of the First Amendment.[46] Although not all free speech or privacy scholars agree with Volokh, his argument (or ones like it) has been influential.[47] Others have questioned the constitutionality of something like the right to be forgotten, calling

40. 20 U.S.C. § 1232g (2012).

41. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x (2012) (discussing consumer financial information); 45 C.F.R §§ 160-264 (2013) (discussing health privacy); MO. REV. STAT. § 182.817 (2000) (providing an example of a representative state library privacy statute).

42. *See* Richards, *supra* note 10, at 1194-1207.

43. Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1660-63 (2009).

44. Volokh, *supra* note 12, at 1051.

45. *Id.* at 1050-51.

46. *Id.* at 1051.

47. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 68-71 (1997).

it, in the words of one excited commentator, "the biggest threat to free speech on the Internet in the coming decade."[48]

The Supreme Court has not been quite so enthusiastic about the death of privacy. The Court has heard several cases pitting the disclosure tort or similar legal theories against First Amendment claims by the press.[49] Even though free speech has usually defeated privacy in these cases, the Court's tradition has been to move carefully, refusing to rule categorically that claims by the press to publish true material always trump privacy claims. The Court explained this somewhat wordily in *Bartnicki v. Vopper*:

> Our cases have carefully eschewed reaching this ultimate question, mindful that the future may bring scenarios which prudence counsels our not resolving anticipatorily.... We continue to believe that the sensitivity and significance of the interests presented in clashes between [the] First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case.[50]

In some of those other contexts, the Court has rejected claims that other kinds of privacy violate the First Amendment. Trespass, eavesdropping, wiretapping, stalking, and industrial espionage do not receive special First Amendment protection;[51] nor do professional duties of confidentiality like the attorney-client privilege, or contractual agreements not to disclose information.[52] Lawyers cannot credibly argue that they have a First Amendment right to divulge their client's confidences,[53] nor can reporters claim that the First Amendment gives them the right to break agreements with confidential sources that they will not disclose their identities.[54] Similarly, restrictions on the sale of targeted marketing lists under

---

48. Rosen, *supra* note 32, at 88.

49. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 527-28 (2001); Fla. Star v. B.J.F., 491 U.S. 524, 526 (1989); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 105-06 (1979); Okla. Publ'g Co. v. Dist. Court, 430 U.S. 308, 311-12 (1977); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495-97 (1975).

50. *Bartnicki*, 532 U.S. at 529 (quoting *Fla. Star*, 491 U.S. at 532-33).

51. *See generally* Richards, *supra* note 10, at 1182-84 (collecting examples).

52. *See id.* at 1172-73.

53. Solove & Richards, *supra* note 43, at 1654, 1670.

54. Cohen v. Cowles Media Co., 501 U.S. 663, 670 (1991).

the Fair Credit Reporting Act have survived First Amendment attack, with the Supreme Court declining to get involved.[55]

This traditional approach makes sense. Privacy and free speech are both important human values, and it is important to tread carefully and not make overbroad claims about the death of privacy or the absolute protection afforded to speech. Both privacy and free speech claims can come in many guises and serve many different interests, and blunt pronouncements in this area have the power to cause significant harm. This is a complex issue, and it deserves a nuanced solution. The First Amendment critique of privacy law is strong when the privacy claims resemble the traditional Warren and Brandeis argument for tort privacy.[56] But that critique is much weaker in other contexts, and it is hard to see how duties of confidentiality—whether imposed on banks, attorneys, or even data brokers—threaten First Amendment values. Under this traditional approach, the law is in balance—privacy claims that menace a free press are presumptively unconstitutional, but codes of fair information practices, which are the foundation of data privacy law, and professional duties of confidentiality are left intact.

Yet in 2011, the Supreme Court decided a case called *Sorrell v. IMS Health Inc.*, which some fear upset that balance in favor of broad First Amendment protection against all privacy rules.[57] *Sorrell* is the Court's most recent word on whether the First Amendment critique of privacy does, or should, apply to privacy law in the data context. As such, the case is worth examining in some detail.

II. THE DATA BROKER CASE

IMS Health (IMS) provides personal data, analysis, and other information services in the health care industry.[58] In common

55. In *Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2011), the Supreme Court denied certiorari, although Justice Kennedy dissented. 536 U.S. 915, 916 (2002) (Kennedy, J., dissenting from denial of certiorari). For another example, see *Individual Reference Serv's Group, Inc. v. FTC*, 145 F. Supp. 2d 6 (D.D.C. 2001), *aff'd sub nom. Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002).

56. Richards, *supra* note 19, at 363-64.

57. 131 S. Ct. 2653 (2011).

58. On its website, IMS declares itself "the world's leading information, services and technology company dedicated to making healthcare perform better," and a provider of "analytics and proprietary application suites ... to enable our clients to run their operations more

parlance, it is a data broker, a company that sells information and answers to questions based on data. IMS is part of the so-called Big Data revolution. Its business is to collect information, assemble it into large databases, and mine it for insight by applying sophisticated analytic techniques. IMS specializes in analyzing trends in health care transactions so that the health companies that are its customers have more information about the market, the competition, and the human beings seeking health care—that is, essentially everyone.[59]

One of the services that IMS and other data brokers provide is data to support something called "detailing."[60] You may have noticed representatives from pharmaceutical companies visiting your doctor. These "drug reps" drop off free samples of drugs along with branded pens and paper.[61] More importantly, they are there to persuade your doctor to prescribe their company's drugs to you, rather than another company's drugs or no drugs at all. This direct marketing is known in the trade as detailing, because drug reps give details about their products to the doctors.[62] Detailing does not merely rely on the personal charm and persuasive power of the drug reps. Instead, it relies on another kind of detail—large quantities of data about what kinds of products to market to individual doctors.

This is when IMS and other data brokers come into the story. These companies buy prescription records from pharmacies in bulk and use these records to assemble profiles of the prescribing patterns of individual doctors.[63] Drug reps can then detail those doctors, knowing the habits of the doctor better than the doctor does herself.[64] Detailing is a massive industry that is both data- and

---

efficiently." *About IMS Health*, IMSHEALTH, http://www.imshealth.com/portal/site/ imshealth (follow "About IMS Health" hyperlink) [http://perma.cc/JH9P-BAGC] (last visited Mar. 24, 2015).

59. *Id.*

60. Rikin S. Mehta, *Why Self-Regulation Does Not Work: Resolving Prescription Corruption Caused by Excessive Gift-Giving by Pharmaceutical Manufacturers*, 63 FOOD & DRUG L.J. 799, 799-802, 816 (2008) (discussing "pharmaceutical detailing" and "gifting" by which pharmaceutical sales representatives will provide gifts in addition to selling pharmaceutical drugs).

61. *Id.* at 799-802.

62. *Id.* at 801-02.

63. Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, 36 VT. L. REV. 931, 938-939 (2012).

64. *Id.* at 938-40.

manpower-intensive.[65] The multibillion dollar costs of detailing, like advertising and other marketing costs, are ultimately passed on to the patients who buy the drug prescribed by the doctor from their pharmacy.[66] The pharmacies then sell the new records to data brokers, and the cycle continues.

Concerned about rising drug prices, Vermont and other New England states passed laws designed to restrict the costly practice of data-based detailing.[67] They sought to drive down drug prices and ensure that doctors made prescribing decisions on the basis of their own independent judgment rather than data-based persuasion by marketers. Vermont's Prescription Confidentiality Act prohibited pharmacies and health insurance companies from selling doctors' prescription data for marketing purposes and prohibited drug reps from using the data for marketing purposes, including detailing.[68]

IMS and other data brokers challenged the laws in court, arguing that the regulations violated their corporate free-speech rights. The First Circuit Court of Appeals upheld New Hampshire's law in the 2008 case, *IMS Health Inc. v. Ayotte*,[69] but in the 2011 *Sorrell* case, a deeply divided United States Supreme Court struck down the Vermont law as unconstitutional.[70]

Writing for a majority of six Justices, Justice Kennedy concluded that the Vermont law violated the First Amendment because it restricted the speech of only marketers, and not of other speakers.[71] As he put it succinctly, "The State has burdened a form of protected expression that it found too persuasive. At the same time, the State has left unburdened those speakers whose messages are in accord with its own views. This the State cannot do."[72]

In reaching this conclusion, the Court ruled that the "sale, disclosure, and use of prescriber-identifying information" was protected by the First Amendment.[73] Moreover, because the Prescription

65. *Id.* at 940-42.
66. *Id.*
67. *Id.* at 955-58.
68. VT. STAT. ANN. tit. 18, § 4631 (2010).
69. 550 F.3d 42, 64 (1st Cir. 2008), *abrogated by* Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).
70. *Sorrell*, 131 S. Ct. at 2672.
71. *Id.*
72. *Id.*
73. *Id.* at 2663.

Confidentiality Act prohibited people from using the information for marketing, the Court held that the Act "disfavor[ed] marketing, that is, speech with a particular purpose. More than that, the statute disfavor[ed] specific speakers, namely pharmaceutical manufacturers."[74] The Court's logic was straightforward: because the sale of the data was protected by the First Amendment, and its use for marketing was prohibited, the statute created content- and viewpoint-based restrictions on expression.[75] Under settled First Amendment law, content- and viewpoint-based discrimination are presumptively unconstitutional.[76] Because Vermont could not give a sufficiently compelling reason to save the statute, it was invalid.

Two parts of this conclusion are significant. First, the principal defect with the Prescription Confidentiality Act was its *discrimination* against certain kinds of protected speech and certain kinds of protected speakers. This is a basic principle of First Amendment law—discrimination among types of speech (content-based restriction) is usually invalid.[77] Most especially, discrimination against particular speakers or messages (viewpoint-based restriction) is almost always invalid.[78] For example, in the famous case of *R.A.V. v. City of St. Paul*, the Court struck down a hate crime statute that had been used to prosecute a man who had burned a cross on the front lawn of an African-American family.[79] The State can punish cross burning of this sort using a variety of legal theories, including threats, fighting words, and the intentional infliction of emotional distress.[80] Cross burning often falls under what First Amendment parlance calls unprotected speech,[81] but the St. Paul law targeted only racist speech, and not the speech of toleration.[82] It punished racist cross burning, but not other kinds of cross burning, like in Madonna's infamous *Like a Prayer* music video. Because the law discriminated on the basis of viewpoint by treating racist viewpoints

74. *Id.*
75. *Id.*
76. *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 391 (1992); Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd., 502 U.S. 105, 115-16 (1991).
77. *Simon & Schuster, Inc.*, 502 U.S. at 115.
78. *See R.A.V.*, 505 U.S. at 391.
79. *Id.* at 396.
80. Virginia v. Black, 538 U.S. 343, 358-60 (2003).
81. *See id.* at 357-60.
82. *R.A.V.*, 505 U.S. at 391-92.

more harshly, it was unconstitutional.[83] Thus, viewpoint discrimination against speech that was *otherwise unprotected by the First Amendment* violated the First Amendment.[84]

In *Sorrell*, the Court reached the same conclusion, relying explicitly on *R.A.V.* because the Prescription Confidentiality Act banned uses of the data in marketing communications, but not educational ones.[85] As the Court put it,

> it appears that Vermont could supply academic organizations with prescriber-identifying information to use in countering the messages of brand-name pharmaceutical manufacturers and in promoting the prescription of generic drugs. But § 4631(d) leaves detailers no means of purchasing, acquiring, or using prescriber-identifying information. The law on its face burdens disfavored speech by disfavored speakers.[86]

Because the law banned the use of data for speech by the marketers, but allowed it for speech by their political opponents, it discriminated on the basis of viewpoint and was thus unconstitutional.[87] Such a conclusion is a straightforward application of basic free-speech law—the government cannot tell human speakers what arguments they can and cannot make, and what data they can and cannot rely on. The government also cannot discriminate between speakers, letting some but not others rely on a particular piece of information.

The second significant element of the opinion in *Sorrell* was a suggestion that the sale of a database was somehow speech protected by the First Amendment.[88] Vermont had made the argument that the Prescription Confidentiality Act did not regulate speech, but merely conduct: the sale of information as a commodity.[89] The First

83. *Id.*
84. *Id.*
85. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2663-64 (2011) (citing *R.A.V.*, 505 U.S. at 391).
86. *Id.* at 2663.
87. *Id.*
88. *Id.* at 2667.
89. *Id.*

Circuit in the New Hampshire case had upheld New Hampshire's antidetailing law on this exact basis.[90] As the *Sorrell* Court held:

> This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment.... Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.[91]

Although the Court hinted that the sale of a database might be speech, the Court stopped short of that sweeping conclusion because the regulation's discrimination against marketers was a content- and viewpoint-based restriction.[92] In this respect, the Court continued its tradition of moving carefully and slowly in cases involving a conflict between privacy rules and freedom of speech. And it most certainly did not hold that government regulation of databases and marketing based upon data analytics is equivalent to government regulation of the content of the news.

III. WHAT *SORRELL* MEANS

What is the significance of *Sorrell* for data privacy law? The short answer is that it is not clear because the opinion itself was not clear. From a First Amendment perspective, the Vermont statute was clumsily drafted, but the Court's opinion was hardly a model of clarity either. Moreover, Justices Breyer, Ginsburg, and Kagan would have upheld the Prescription Confidentiality Act notwithstanding its poor drafting, on the ground that the law was merely lawful regulation of a commercial enterprise and threatened the First Amendment barely, if at all.[93]

Nevertheless, some observers have suggested that *Sorrell* might mean the end of privacy law, because it assumed that data flows are

90. IMS Health Inc. v. Ayotte, 550 F.3d 42, 52 (1st Cir. 2008), *abrogated by Sorrell*, 131 S. Ct. 2653.

91. *Sorrell*, 131 S. Ct. at 2667 (citations omitted).

92. *Id.*

93. *Id.* at 2673 (Breyer, J., dissenting).

speech.[94] These scholars argue that the inevitable result of this conclusion is that all laws regulating the flows of data are now constitutionally suspect.[95] Ashutosh Bhagwat worries that "the Court's hints in this regard have dramatic, and extremely troubling, implications for a broad range of existing and proposed rules that seek to control disclosure of personal information in order to protect privacy."[96] More enthusiastically, Jane Bambauer argues that "for all practical purposes, and in every context relevant to the current debates in information law, data is speech. Privacy regulations are rarely incidental burdens to knowledge. Instead, they are deliberately designed to disrupt knowledge creation."[97] In their readings of *Sorrell*, these scholars echo the earlier claim of Eugene Volokh that data privacy law under the FIPs is no more than "a right to have the government stop you from speaking about me."[98]

If this interpretation became the law, the implications would be striking: information privacy law as we know it would be dead. If data were speech, every restriction on the disclosure—not to mention the collection or use—of information would face heightened First Amendment scrutiny, and would be presumptively unconstitutional. This would jeopardize not just medical privacy rules, but most likely financial privacy rules, reader privacy rules, and any hope of imposing the FIPs to Internet data such as the logs Internet service providers and marketers keep of which websites we visit. Arguably, even such venerable nondisclosure rules as the attorney-client duty of confidentiality would also have to satisfy the demands of heightened First Amendment scrutiny, for these rules also place nondisclosure obligations on lawyers not to speak confidences.

This reading of *Sorrell* has some support in dictum in Justice Kennedy's opinion, which suggested that regulation of information flows was indistinguishable from regulating speech.[99] But even Justice Kennedy was careful to make clear that the holding in *Sorrell* did not render privacy law unconstitutional in general.[100] In

94. *See id.* at 2663 (majority opinion).

95. *See, e.g.*, Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 855 (2012).

96. *Id.* at 856.

97. Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 63 (2014).

98. Volokh, *supra* note 12, at 1051.

99. *Sorrell*, 131 S. Ct. at 2665.

100. *Id.* at 2668.

particular, he suggested that if Vermont had addressed doctor confidentiality "through a more coherent policy" like the federal Health Insurance Portability and Accountability Act of 1996,[101] rather than (in his view) the haphazard methods it had used, the law would have been constitutional.[102]

There is thus another reading of both *Sorrell* and First Amendment law that is less menacing to data privacy law and to the FIPs. Under this reading, the problem with the Vermont law was not that it regulated data flows, but that it imposed viewpoint restrictions on unprotected speech. In other words, *Sorrell* is not the beginning of the end for data privacy law. Instead, like *R.A.V.*, the case is a reminder that the government cannot impose viewpoint restraints on particular speakers, like marketers.[103] Under this view, *Sorrell* invalidated one particularly clumsy attempt to regulate marketing, but it does not follow from this that data privacy law is largely unconstitutional. In fact, as Justice Kennedy suggested, the statute would have been less problematic if it had imposed *greater* duties of confidentiality on the data, rather than just restricting marketing uses.[104] This would be the case because "[p]rivacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers."[105]

I think that this narrower reading of *Sorrell* is the better one, but ultimately *Sorrell* is just one case with a poorly explained holding. Yet the case raises broader questions of how much force the First Amendment should play in the regulation of data privacy. Is the trade in personal data commercial regulation of the sort that does not and should not concern free expression doctrine? Or, as some commentators believe, is data speech? In the next two Sections of this Article, I want to show why asking "is data speech?" is a poor way to ask a very important question. I will also argue that however we frame the question, subjecting general nondisclosure rules on commercial data flows to the full force of the First Amendment would be a very bad idea. In fact, doing so would uproot one of the

101. 42 U.S.C. § 1320d-2 (2012); 45 C.F.R. §§ 160, 164 (2013).
102. *Sorrell*, 131 S. Ct. at 2668.
103. *See generally* R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).
104. *Sorrell*, 131 S. Ct. at 2668.
105. *Id.* at 2672.

most basic foundations on which modern constitutional law has been built.

IV. THE SILLINESS OF "DATA=SPEECH"

The "data-is-speech" argument has a certain superficial appeal. After all, if the First Amendment is about protecting people's ability to share ideas and information, and data is information, then the First Amendment should protect people's ability to share data. The argument is clear, and it is consistent—everything is speech, and everything is protected.

But this argument's consistency is a foolish consistency. Just because something is speech does not mean it is beyond regulation. Nor does the fact that something is labeled speech qualify it for special protection under the First Amendment. Consider once more the wide variety of activities humans do every day with words—we talk on the phone, write books, emails, and blogs, and sing in the shower. People also use words to hire assassins, engage in insider trading, sexually harass subordinates in the workplace, and verbally abuse their children. All of these activities are speech, but many of them are well outside the main concerns of the First Amendment. We need to protect some, but we need to regulate others. This is a problem.

The good news is that this kind of problem is one that the law is used to dealing with. Other areas of constitutional law face the same problem. Take, for example, the Equal Protection Clause of the Fourteenth Amendment, which bars the government from denying any person "the equal protection of the laws."[106] A superficial reading of these words would be that the government cannot treat people differently, because to do so would deny them "the equal protection of the laws."[107] Like the data-is-speech argument, this interpretation would have consistency, but it would be a foolish consistency. Governments treat their citizens differently all the time: they discriminate on the basis of age when allocating driver's licenses and health benefits like Medicare; they discriminate on the basis of wealth when setting tax rates, college financial aid, and

106. U.S. CONST. amend. XIV, § 1.
107. *Id.*

welfare benefits; they discriminate on the basis of education and ability when allocating law and medical licenses; and they discriminate on the basis of criminal activity when deciding who can be free and who goes to prison. All of these actions discriminate, but none of them bring down the full weight of the Equal Protection Clause. As long as they are rational, these laws are constitutional. And that is a good thing, because a government that cannot treat people differently for a good reason cannot regulate for the common good.

Of course, treating people differently for a bad reason can be dangerous. To remedy this problem, equal protection law long ago created the idea of a suspect classification: the government is allowed to discriminate among its citizens in lots of ways, but certain kinds of discrimination—classifications on the basis of race, gender, and national origin, for instance—are suspect.[108] When the government uses race to discriminate, we become suspicious, and judges scrutinize the laws much more carefully.[109] This is why Jim Crow laws are unconstitutional and why even benign forms of discrimination like affirmative action must be carefully justified.[110] For these laws to be constitutional they must be narrowly tailored to a compelling government interest.[111]

But because a small subset of suspect classifications is treated differently, the rest of the law can function. For example, the state can deny driver's licenses, tattoos, and beer to fifteen-year-olds. As long as these laws are rationally related to a legitimate government purpose, they are constitutional.[112] There are certainly hard cases at the margins, but they are relegated to those margins. In the main, equal protection law has chosen common sense over a foolish consistency that would require courts to scrutinize every portion of every law that treats people differently.

To put the point succinctly, discrimination is everywhere, but only those few kinds of discrimination that are especially dangerous get a hard look under the Equal Protection Clause.[113] All discrimination

108. *See* GEOFFREY R. STONE, CONSTITUTIONAL LAW 530-35 (7th ed. 2013).
109. *See id.*
110. *See id.*
111. *See* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 687 (4th ed. 2011).
112. *See id.*
113. *See id.*

implicates the Equal Protection Clause, but most kinds get only a cursory glance from courts. And the system works.

Something similar goes on in First Amendment law, although it does not get recognized as frequently.[114] Speech is everywhere, and it is regulated all the time, but only certain kinds of speech restrictions that are especially dangerous get looked at under the full force of the First Amendment.[115] There are, of course, the famous categories of unprotected speech—incitement, obscenity, fighting words, threats, falsely shouting fire in theatres, and so forth.[116] But these are just the tip of the iceberg. Under the surface, beneath our normal attention, there are product labeling requirements, murder-for-hire contracts, securities disclosures and nondisclosures, insider trading rules, agreements to restrain trade, sexually harassing speech that creates a hostile environment in the workplace, and regulations of truthful but misleading commercial offers.[117] Frederick Schauer has called this idea "constitutional salience"—we are so used to regulations of words and information outside the normal attention of First Amendment law that we often do not notice them.[118] They are not salient, so we do not notice them even though they are hiding in plain sight. And the system works.

Faced with a similar choice between foolish consistency and common sense, judges and scholars have overwhelmingly chosen the latter. The First Amendment has never been interpreted as an absolute protection for all uses of words, much less for automated and mechanized data flows or the sale of information as a commodity.[119] American lawyers are perhaps the group most protective of free speech in the history of the world.[120] But even in the United States, virtually all strong, speech-protective interpretations of the First Amendment carve out large chunks of the ways we use words

---

114. *See* Richards, *supra* note 10, at 1168-81; Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1769 (2004).

115. *See* Schauer, *supra* note 114, at 1769.

116. *See id.* at 1768.

117. *See id.* at 1805 (providing examples).

118. *See id.* at 1768.

119. *See, e.g.*, *id.* at 1769.

120. *See, e.g.*, RONALD J. KROTOSZYNSKI, JR., THE FIRST AMENDMENT IN CROSS-CULTURAL PERSPECTIVE 12-25 (2006).

or information from heightened First Amendment protection.[121] This is so the First Amendment can do its job—protecting political and artistic expression—without swallowing the rest of the law.

From this perspective, we can see why asking whether data is speech is the wrong question. What matters is not the "speechiness" of a category of human activity as much as the purpose and effects of the government regulation at issue. Commercial data flows are certainly within the outermost bounds of the First Amendment, but so too are sexual harassment, criminal and antitrust contracting, threats, and securities disclosures. Putting data flows in this category merely means that the government can regulate them if it acts rationally to further a legitimate government purpose. Something more is needed to show that regulation of commercial data flows is suspect like regulation of traditional categories of expression such as political speech or protest, commentary on matters of public concern, artistic expression, or, less importantly, advertising to consumers that proposes a commercial transaction.[122]

One might ask a very good question at this point: Why is all speech, broadly defined, not protected by the First Amendment? Let me offer two answers to this question, one simple and one more complicated. The simple answer is that because First Amendment lawyers do not want to leave important expressive activities or practices out of the First Amendment's protection, we tend to define speech rather broadly. For example, the Supreme Court has held a vast amount of things to be speech—or at least within the protection of the First Amendment—including cross burning, swearing, nude dancing, virtual child pornography, threats, lies, and horrifying discrimination and hate speech.[123] Often, this is done for good

121. *Id.*

122. For cases about the regulation of political expression, see, for example, *Cohen v. California*, 403 U.S. 15, 26 (1971); and *New York Times Co. v. Sullivan*, 376 U.S. 254, 292 (1964). For cases about the regulation of artistic expression, see, for example, *Brown v. Entertainment Merchants Ass'n*, 131 S. Ct. 2729, 2742 (2011); and *Burstyn v. Wilson*, 343 U.S. 495, 506 (1952). For cases about the regulation of advertising, see, for example, *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 571 (2001); and *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557, 571-72 (1980).

123. *See, e.g.*, United States v. Alvarez, 132 S. Ct. 2537, 2551 (2012) (holding lies to be speech); Snyder v. Phelps, 131 S. Ct. 1207, 1220-21 (2011) (holding hate speech to be speech); Ashcroft v. ACLU, 535 U.S. 564, 585-86 (2002) (holding virtual child pornography to be speech); Boy Scouts of Am. v. Dale, 530 U.S. 640, 661 (2000) (holding discriminatory speech as within the First Amendment's protection); R.A.V. v. City of St. Paul, 505 U.S. 377, 396

reason, to protect potentially valuable dissenting political speech from the tyranny of the majority. But notice that when we expand the outermost bounds of what is speech, there is a risk that everything becomes expressive or potentially expressive. The more this happens, the less room we have for ordinary legal rules, even ones that have no purpose or even effect of political or artistic censorship. All speech is not protected by the First Amendment because if we define "speech" broadly enough, the First Amendment would swallow the law, making ordinary regulation impossible.

This brings us to the more complicated answer, which has to do with a basic tension in constitutional law. Constitutional rights are protected by judges setting aside laws passed by the democratic process. Alexander Bickel famously called this the "counter-majoritarian difficulty": it is undemocratic for unelected judges to strike down laws passed by our elected representatives.[124] Judicial intervention is justified when it invalidates restrictions on free speech, voting, or political equality, because without such safeguards, we have reason to distrust all laws. If we cannot speak out about unfair laws, it is hard to call those laws democratic. But the countermajoritarian difficulty also suggests that exceptions to the basic idea that democratic laws are the law of the land must be limited.[125] If judges made all of the law, we would no longer be living in a representative democracy, but in an oligarchy at best. Modern American constitutional law rests on the necessary compromise between democratic laws and undemocratic protection of civil liberties. For the system to work, it relies on the undemocratic exceptions being limited, and on those exceptions protecting democratic rights, like free speech. Central to this compromise is an important lesson from almost a century ago, to which we now turn.

(1992) (holding cross burning to be speech); Barnes v. Glen Theatre, Inc., 501 U.S. 560, 572 (1991) (holding nude dancing as protected within the First Amendment); Schad v. Mt. Ephraim, 452 U.S. 61, 76-77 (1981) (holding nude dancing as protected); *Cohen*, 403 U.S. at 15 (holding swearing as protected speech); Bridges v. California, 314 U.S. 252, 278 (1941) (holding threats as protected speech).

124. ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH 16 (1962).

125. *See id.* at 16-17.

V. REJECTING DIGITAL *LOCHNER*

There is a famous parable in constitutional law that has been taught to virtually every first-year law student for decades. In the late nineteenth and early twentieth centuries, the Industrial Revolution transformed American society. On the one hand, it produced great fortunes and technological innovation that made what had been impossible commonplace. These new innovations included factories, steam engines, railroads, cars, airplanes, and cheap textiles, and they shaped the modern world into a form that we—or at least our parents—could recognize. On the other hand, the Industrial Revolution produced enormous social costs, including huge wealth inequality, poverty, child labor, unsafe industrial working conditions, and pollution. Faced with these problems, Congress and the state legislatures tried to fix the problems of the perilous industrial workplace while preserving its benefits. Progressive legislators passed laws preventing child labor, regulating unsafe working conditions, and imposing minimum wage and maximum hours laws, overtime requirements, product labeling laws, and antitrust laws.[126] But the Supreme Court struck many of these laws down as infringements on personal liberty.[127] Afraid that laws regulating economic transactions could lead to wealth redistribution or socialism, the Court held that much of this economic regulation violated the Fourteenth Amendment's Due Process Clause, infringing on the rights of workers and employers to what it called the "liberty of contract."[128]

This era in Supreme Court history is named after the infamous 1905 case of *Lochner v. New York*. In *Lochner*, the Supreme Court struck down a New York law regulating the safety of bakers.[129] *Lochner* was not the first Supreme Court case to protect economic rights against government regulation, nor was it the last, but it was the case that gave its name to the era of strong constitutional protection of economic rights, lasting from the late nineteenth

126. *See* Barry Friedman, *The History of the Countermajoritarian Difficulty, Part Three: The Lesson of* Lochner, 76 N.Y.U. L. REV. 1383, 1392 (2001).

127. G. EDWARD WHITE, THE CONSTITUTION AND THE NEW DEAL 241-42 (2000).

128. *Id.*

129. 198 U.S. 45, 64 (1905).

century until the late 1930s.[130] The *Lochner* Court's economic libertarianism rested on the idea that private property was the bulwark of political liberty, and that a government that has the power to redistribute wealth is a grave threat to liberty.[131] These ideas have a strong tradition in Anglo-American political thought, but there was a problem. A broad government power to regulate economic matters also allows regulations such as minimum wages, maximum hours, workplace safety, and the right to collective bargaining. During the Industrial Revolution, the conservative economic, libertarian view of the Constitution became inconsistent with the needs of a modern, industrial economy.[132] This inconsistency became most apparent during the Great Depression, when *Lochner*-style doctrines were used to invalidate portions of the New Deal.[133] Thus, in the industrial era, a libertarian view of industrial economic liberty made needed regulation impossible.

I fear that acceptance of the data-is-speech argument will repeat these errors of the Industrial Age for the Information Age. Today, great chunks of human society are being transformed into digital form, and we all leave digital footprints every day as we live our lives. It is essential that we preserve strong civil liberties in our digital future. But if the lessons of the twentieth century are that government regulation is sometimes necessary in an industrial economy, we should not forget those lessons in our information economy. In a 2005 article published before the *Sorrell* litigation, I made an early argument along these lines.[134] Justice Breyer made a similar point in his *Sorrell* dissent: "At best the Court opens a Pandora's Box of First Amendment challenges to many ordinary regulatory practices that may only incidentally affect a commercial message. At worst, it reawakens *Lochner*'s pre-New Deal threat of substituting judicial for democratic decisionmaking where ordinary economic regulation is at issue."[135] The many new uses to which we

130. BARRY CUSHMAN, RETHINKING THE NEW DEAL COURT (1998).

131. Jack M. Balkin, *"Wrong the Day It was Decided":* Lochner *and Constitutional Historicism*, 85 B.U. L. REV. 677, 687-88 (2005).

132. *Id.* at 704.

133. *Id.* at 684.

134. Richards, *supra* note 10, at 1211-21. I should disclose that I gave pro bono counsel to the State of Vermont during the *Sorrell* litigation.

135. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2685 (2011) (Breyer, J., dissenting) (citation omitted).

can put data create new possibilities, but also new problems. We need to make choices as a society about what kinds of data privacy rules we should have, and about when data should flow freely. In fact, we might ultimately decide that the best policy is to have very little data privacy.

But, however we as a society choose to regulate data flows, we *must* be able to choose. We must not be sidetracked by misleading First Amendment arguments, because the costs of not regulating the trade in commercial data are significant. As we enter the Information Age, in which the trade in information is a multibillion-dollar industry, the government should be able to regulate the huge flows of personal information, as well as the permissible uses of such information. If our lives become digital, but data is speech, regulation of many kinds of social problems will become impossible. There will certainly be cases at the borders of strong First Amendment because, of course, data will be sometimes tied to important expression. But this is an insufficient reason to give up on regulation of our society as it digitizes. At the dawn of the Industrial Age, business interests persuaded the Supreme Court in *Lochner* and similar cases that the freedom of contract should immunize them from regulation. We must reject the similar calls of modern advocates for digital *Lochner*.

CONCLUSION: THE RIGHT TO BE FORGOTTEN AND INFORMATION POLICY

Let me conclude with a few thoughts about the right to be forgotten. I have argued that most commercial data flows regulated by information privacy law embodying the FIPs should be constitutional, but what about the right to be forgotten? The answer to this question is more complicated, because the right to be forgotten is a poorly defined idea that can mean several different things.[136] But the ambiguity of the right to be forgotten is a helpful point on which to end this Article, because it illustrates my general argument: ordinary commercial regulations of the data trade are constitutional, but tort rights to censor the media are not.

136. *See supra* text accompanying notes 33-34.

At the most basic level, the general encouragement that personal data *should* be deleted at some point poses no constitutional problems. Our digital society cannot be regulated by legal rules alone, and the development of professional norms among data holders to protect values like the FIPs or some variant of the right to be forgotten will be an important part of any solution. This is particularly the case for so-called sensitive data—information that would be particularly harmful if disclosed, such as financial, health, or political data. Governments could promote the importance of this social norm without mandating it, which would be clearly constitutional.

We could also imagine governments imposing the right to be forgotten on certain data holders as a consequence of their relationship with users who supply them with data. For example, imagine a regulation of social networking sites that would require sites like Facebook to allow users to edit information they have supplied to the company, like status updates or contact information.[137] This would be a more substantial requirement than merely promoting social norms, but it should also be constitutional as an ordinary regulation of a commercial relationship. Such rules could also be justified as placing an implied use condition on the receipt of information, the way the law imposes nondisclosure and other use conditions on the information that lawyers receive from their clients. The Fair Credit Reporting Act already gives consumers the ability to correct false information in their credit reports and places limits on the ability of credit reporting agencies to disclose old information about consumers (such as arrest records and lawsuits older than seven years).[138] At least when there is an equivalently important relationship between consumers and data brokers, such regulations should be constitutional in most cases.

On the other hand, the right to be forgotten runs into First Amendment problems when it starts to resemble the old disclosure tort. In fact, the proposal has generated so much free-speech concern because the versions of the right proposed for the revisions to the European Union Directive have taken the tort form. The proposed regulation would allow people to require any Internet service

137. Of course, most sites, including Facebook already provide this feature, though the law does not require it.

138. 15 U.S.C. §§ 1681c-1681i (2012).

provider to delete data about them if there is no legitimate reason to keep it.[139] This is a much more sweeping version of the right, which would allow the deletion of potentially newsworthy information about a person provided by others.[140] It is one thing to give an Internet user the ability to restrict or retract information he or she provides in the context of a commercial relationship, and quite another to allow a person the right to edit any and all information about them on the Internet. Such a broad power would turn the Internet into our own personal Wikipedias and would represent a resuscitation of Mabel Warren's broad right to censor not merely commercial data, but potentially highly newsworthy expression as well.

The fact that this strong form of the right to be forgotten is a threat to free speech does not mean that milder forms of a right to delete are also problematic. Some of these weaker forms of the right might be a bad idea in theory or in actual implementation; they might increase costs, or deter innovations, or be counterproductive. But, they are probably constitutional. Not everything that is a bad idea is unconstitutional, and in a democratic society in a time of technological change, we must be free to make policy mistakes. General principles or rights to make data mortal do not threaten free public debate or democratic self-government. One could imagine a right to be forgotten that is bad policy, but in a democratic society, the basic contours of information policy must ultimately be up to the people, not unelected judges. Making policy mistakes is sometimes a price we pay for self-government.

139. Press Release, Eur. Comm'n, *supra* note 31.

140. *See* CTR. FOR DEMOCRACY & TECH., *supra* note 35.