Washington University in St. Louis

SCHOOL OF LAW

Why Data Privacy Law is (Mostly) Constitutional

Neil M. Richards
Professor of Law
Washington University School of Law

Adapted from *Intellectual Privacy*, Chapter Five

(under contract, Oxford University Press, 2014)

Executive Summary

A few kinds of privacy rights 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 them out of the newspapers. But privacy can mean many things, and most of these things are fully consistent with the American commitments to broad rights of free speech and free press. Specifically, we 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. Policymakers can 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. 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, an argument seemingly strengthened by the Supreme Court's 2011 decision in *Sorrell v. IMS Health*, which struck down a Vermont law preventing drug reps (but no one else) from using data-based marketing to speak to physicians.

Before *Sorrell*, there was a settled understanding that general commercial regulation of the huge data trade wasn't censorship. It was seen on the contrary 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). Such content- and viewpoint 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 didn't regulate *enough*, unlike the "more coherent policy" of the undoubtedly constitutional federal Health Insurance Portability and Accountability Act of 1996.

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 every day that are more clearly "speech" than a data flow, from blogging and singing in the shower to insider trading, sexually harassing co-workers, verbally abusing children, and even hiring assassins. Well-settled First Amendment allows us to separate out which of these activities cannot be regulated (the first two) from those which can (the rest). First Amendment lawyers don't 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 long-standing First Amendment values. And commercial regulation – of sexual harassment, unfair trade practices, and commercial data flows based on the FIPs —is rarely threatening to First Amendment values, properly understood by their settled meaning.

The ordinary understandings of First Amendment lawyers are supported by a more fundamental reason. 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. This has become one of the basic principles of American Constitutional law. 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 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.

Privacy law is thus (mostly) constitutional. And when we're talking about the regulation of commercial data flows, it's entirely constitutional, except for a few poorly-drafted outliers like 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 policymaking representatives, and not to unelected judges. We should decide policy on that basis, rather than on odd readings of the First Amendment.

Chapter Five:

Data

Up to this point in the book, I've shown how the classic notion of privacy – Warren and Brandeis' disclosure tort against the press – is largely inconsistent with the First Amendment as we understand it today. The main problem with the tort is that it targets the press for publishing the embarrassing truth under a blurry standard. But privacy can mean many things beyond the right to prevent the press from making embarrassing disclosures about us. We 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. Are these data privacy rules unconstitutional, too?

Throughout the world, democratic societies regulate personal data using laws that embody the "Fair Information Practices." The "FIPs," as they are called by privacy professionals, 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. The FIPs, perhaps ironically, were developed by the United States Government in the 1970s, which wanted to establish some minimal best practices for the processing of personal data. The government report which announced them described the FIPs as "five basic principles" which automated data systems must ensure:

- 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 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 reasonable precautions to prevent misuse of the data.[1]

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.[2] They have different meanings in different places and contexts, but at bottom they 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. They are the foundation of the OECD Privacy Guidelines, and the basis for the 1995 EU Data Protection Directive, 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.[3] Legal scholar Joel Reidenberg has 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.[4]

The FIPs have been remarkably durable, but other principles have been proposed from time to time. In January 2012, EU regulators proposed revisions to the almost 20-year-old Data Protection Directive. The most controversial of these was for a new fair information principle, "*Le Droit à l'Oubli*," commonly translated into English as "The Right to Be Forgotten."[5] The Right to be Forgotten is the idea that at some point, personal data should be deleted and not persist in databases forever. It was popularized by privacy scholar Viktor Mayer-Schönberger in his 2009 book *Delete*.[6] Implementation of this right into the FIPs could take several forms. On the 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.[7] But on the other hand, the Right to Be Forgotten could be interpreted as a right to have websites remove personal data, or 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 EU in 2012 seems to be of this latter, stronger sort.[8]

Taking a step back, it's important to consider the constitutional status of these rules – not just the Right to Be Forgotten, but the FIPs as a whole. These are the questions I want to examine in this chapter, and they are some of the most important questions we face in our increasingly digital society. 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?

I will argue in this chapter that the answers to these questions will generally be "no." Most data privacy regulations do not involve the First Amendment at all, 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 whether we can regulate data flows at all. In a society in which data flows are becoming increasingly important, this is really 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 "data" is somehow "speech."

Let's begin with the FIPs. The FIPs are a code of best practices for the handling of personal information by businesses and government. But statutes embodying the FIPs do far more than merely regulate information flows or prevent disclosures. Legal scholar 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. Only principle three (providing protection against the use or disclosure of sensitive data) reflects the notion of idea of information privacy preventing other people from talking about you.[9] 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 under anyone's reading.[10]

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's 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, it does not police an unwieldy line between public and private, and it does not remedy primarily emotional harm. Instead, FERPA, the federal statute that imposes this requirement, regulates the "education records" of a university, carefully defines the records that are within its scope, and regulates the relationship between university and student, rather than imposing rules on the disclosure of grades (for example) under all circumstances.[11] Other statutes embodying the FIPs operate similarly, and rather than targeting news reports of celebrities, at their best they protect the confidentiality of the information we need to live our lives, like our library, medical, and financial records.[12] Generally-applicable regulation of commercial data simply doesn't raise the First Amendment concerns that the disclosure tort does.[13] And confidentiality rules that

regulate the obligations of parties to a relationship rather than whether a fact can be published by anyone pose even fewer First Amendment problems.[14]

Not everyone agrees with me on this point, including some technologists, academics, and corporate lobbyists. For example, in an influential article, legal scholar Eugene Volokh argues that most privacy rules are inconsistent with free speech. 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." 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.[15] Although not all free speech or privacy scholars agree with Volokh, his argument (or ones like it) has been influential.[16] Others have questioned the constitutionality of something like the Right to be Forgotten, calling it (in the words of one excited journalist) "the biggest threat to free speech on the Internet in the coming decade."[17]

The Supreme Court has not been quite so enthusiastic about the death of privacy. As previous chapters have explained, the Court has heard several cases pitting the disclosure tort or similar legal theories against First Amendment claims by the press.[18] But although 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. As the Court explained somewhat wordily in the *Bartnicki* case,

> "[o]ur 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."[19]

And 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.[20] Nor do professional duties of confidentiality like the attorney-client privilege, or contractual agreements not to disclose information. Lawyers cannot credibly argue that they have a First Amendment right to divulge their client's confidences,[21] 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.[22] Similarly, restrictions on the sale of targeted marketing lists under the Fair Credit Reporting Act have survived First Amendment attack, with the Supreme Court declining to get involved.[23]

This traditional approach makes a lot of sense. Privacy and free speech are both important human values, and it is important to tread carefully and not make over-broad

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. But as I have shown in previous chapters, the First Amendment critique of privacy law is strong where the privacy claims resemble the traditional Warren and Brandeis argument for tort privacy. It 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 (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. *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, so it is worth looking at in some detail.

The Data Broker

IMS Health Services calls itself a "health analytics company," which means it provides personal data, analysis, and other information services in the health care industry.[24] In common 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. It 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 humans beings seeking health care (that is, essentially everyone).[25]

One of the services that IMS and other data brokers provide is data to support something called "physician detailing." 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. 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. Detailing doesn't just rely on the personal charm and persuasive power of the drug reps. Instead, it relies on another kind of detail – lots of data about what kinds of products to market to individual doctors.

This is where IMS and other data brokers come into the story. IMS buys prescription records from pharmacies in bulk, and uses these records to assemble profiles of the prescribing patterns of individual doctors. Drug reps can then "detail" those doctors, knowing the habits of the doctor better than the doctor does herself. Detailing is a massive industry – one that is both data- and manpower-intensive. The

multi-billion-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.[26] 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. They sought to drive down drug prices, and to ensure that doctors made prescribing decision 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.[27]

Concerned about the effect of these laws on their profits, IMS and other data brokers challenged them in court. The First Circuit Court of Appeals upheld New Hampshire's law in the 2009 *Ayotte* case,[28] but in the 2011 *Sorrell* case, a deeply divided Supreme Court struck down the Vermont law under the First Amendment.[29]

Writing for a majority of six Justices, Justice Kennedy concluded that the Vermont law violated the First Amendment because it restricted the speech of marketers only, but not that of other speakers. As he put it succinctly, "[t]he 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."[30]

In reaching this conclusion, the Court ruled that the "sale, disclosure, and use of prescriber-identifying information" was protected by the First Amendment. Moreover, because the Prescription Confidentiality Act prohibited people from using the information for marketing, the Court found that the Act "disfavor[ed] marketing, that is, speech with a particular purpose. More than that, the statute disfavors particular speakers, namely pharmaceutical manufacturers."[31] 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, it created content- and viewpoint-based restrictions on expression. Under settled First Amendment law, content- and viewpoint-based discrimination is presumptively unconstitutional. And 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 restrictions) is usually invalid. Most especially, discrimination against particular speakers or messages ("viewpoint-based" restrictions) is virtually always invalid. For example, in the famous case of *RAV v. City of St. Paul* (1992), 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.[32] Cross-burning of this sort can be punished under a variety of theories, including threats, fighting words, and the intentional infliction of emotional distress. Cross-burning usually falls under what First Amendment parlance calls "unprotected speech." But the St. Paul law targeted only racist speech, and not the speech of toleration. (It punished racist cross-burning, but not other kinds of cross-burning, like the ones in Madonna's "Like a Prayer" video). Because it discriminated on the basis of viewpoint by treating racist viewpoints more harshly, it was unconstitutional.[33] Thus, viewpoint discrimination against speech that was *otherwise "unprotected" by the First Amendment* violated the First Amendment.

In *Sorrell*, the Court reached the same conclusion, relying explicitly on *RAV*: The Prescription Confidentiality Act banned uses of the data in marketing communications, but not educational ones.[34] 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.

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.[35] Such a conclusion is a straightforward application of basic free speech law – the government can't tell human speakers what arguments they can and can't make, and what data they can and can't rely on. And it can't 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. Vermont had made the argument that the Prescription Confidentiality Act did not regulate speech, but merely conduct: the sale of information as a commodity. (The First Circuit in the New Hampshire case had upheld New Hampshire's anti-detailing law on this exact basis). As the Supreme Court put it:

> 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.[36]

But though the Court hinted that the sale of a database might be "speech," it stopped short of that sweeping conclusion, because the regulation's discrimination against marketers was a content- and viewpoint-based restriction.[37] In this respect, the Court continued its tradition of moving carefully and slowly in cases involving the conflict between privacy rules and freedom of speech.

What *Sorrell* Means

What is the significance of *Sorrell* for data privacy law? The short answer is that it's not clear, because the opinion itself isn't clear. From a First Amendment perspective, the Vermont statute was clumsily drafted, but the Court's opinion is 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.[38]

Nevertheless, some observers have suggested that *Sorrell* might mean the end of privacy law, because it assumed that data flows are "speech." The inevitable result of this conclusion, these scholars argue, is that all laws regulating the flows of data are now constitutionally suspect. 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."[39] More generally, Jane Bambauer argues enthusiastically that "for all practical purposes, and in every context relevant to the privacy debates, data is speech. Privacy regulations are rarely (if ever) incidental burdens to knowledge. Instead, [they are] deliberately designed to disrupt knowledge-creation."[40] In their reading of *Sorrell* these scholars echo the earlier claim of Eugene Volokh that data privacy law under the FIPs are no more than "a right to stop people from talking about you."[41]

If this interpretation were to become the law, the implications would be striking, Information privacy law as we know it would be dead. If data is "speech," every restriction on the disclosure (not to mention the collection or use) of information would face heightened First Amendment scrutiny, and 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 ISPs and marketers keep of what web sites we visit. Arguably, even such venerable nondisclosure rules such as the attorney-client duty of confidentiality would also have to satisfy the demands of 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." But even Justice Kennedy was careful to make clear that the holding in *Sorrell* did not render privacy law unconstitutional in general. In 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,[42] rather than (in his view) the haphazard methods it had used, the law would have been constitutional.[43]

There is thus another reading of both *Sorrell* and First Amendment law generally 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 *RAV*, the case is a reminder that the government cannot impose viewpoint restraints on particular speakers like marketers. 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. This was the case because "Privacy 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."[44]

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 it raises the broader question 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 chapter, I want to show why "is data speech?" is a poor way to ask a very important question. I will also argue that 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 most basic foundations on which modern constitutional law has been built.

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" doesn't mean it is beyond regulation. Nor does the fact that something is labeled "speech" qualify it for special protection by the First Amendment. Humans do lots of things every day with words - we talk on the phone, we write books and emails and blogs, we sing in the shower. But 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 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.

But this kind of problem is one that 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 government from denying any person "the equal protection of the laws." 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." 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 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's a good thing, because a government that cannot treat people differently much of the time cannot regulate for the common good.

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." When the government uses race to discriminate, we become suspicious, and judges scrutinize the laws much more carefully. This is why Jim Crow laws are unconstitutional, and why even "benign" forms of discrimination like affirmative action must be carefully justified. For these laws, to be constitutional they must be narrowly tailored to a compelling government interest.[45]

But because a small subset of suspect classifications is treated differently, the rest of the law can function. For example, the state can deny drivers licenses, tattoos, and beer to fifteen-year-olds. For these laws, as long as the law is rationally related to a legitimate government purpose, it is constitutional. There are certainly hard cases at the margins, but 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. All discrimination 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, though it does not get recognized as frequently.[46] Speech is everywhere, but only certain kinds of speech restrictions that are especially dangerous get looked at under the full force of the First Amendment. There are, of course, the famous categories of "unprotected speech" – incitement, obscenity, fighting words, threats, falsely shouting fire in theatres, and so forth. 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.[47] Legal scholar Frederick Schauer has called this idea "First Amendment salience" - we are so used to regulations of words and information outside the normal attention of First Amendment law that we often don't notice them.[48] They aren't salient, so we don't 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, First Amendment 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.[49] American lawyers are perhaps the group most protective of free speech in the history of the world.[50] 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 or information from heightened First Amendment protection. They do this so that 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. 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. But 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, like political speech or protest, commentary on matters of public concern, artistic expression, or (less importantly) advertising to consumers that proposes a commercial transaction.[51]

One might ask a very good question at this point, which is why all "speech," broadly defined, isn't 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 don't 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 often horrifying discrimination and hate speech.[52] Often, this is done for good 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," broadly defined, isn't 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 by setting aside laws passed by the democratic process. Legal scholar Alexander Bickel famously called this the "counter-majoritarian difficulty": It is undemocratic for unelected judges to strike down laws passed by our elected representatives.[53] 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 can't speak out about unfair laws, it's hard to call those laws democratic. But the counter-

majoritarian difficulty also suggests that exceptions to the basic idea that democratic laws are the law of the land must be limited. 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 them protecting democratic rights (like free speech). Central to this compromise is an important lesson from almost a century ago, to which we now turn.

Rejecting Digital *Lochner*

There's a famous parable in Constitutional Law that has been taught to virtually every first-year law student for decades. The parable goes something like this: 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, cheap textiles, and shaped the modern world into a form that we (or at least our parents) could recognize. But 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.[54] But the Supreme Court struck many of these laws down as infringements on personal liberty. 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."[55]

This era in Supreme Court history is named after the infamous 1905 case of *Lochner v. New York*.[56] In *Lochner*, the Supreme Court struck down a New York law regulating the safety of bakers. *Lochner* was not the first Supreme Court case to protect economic rights against government regulation, nor was it the last, but it is the case that has given its name to the era of strong constitutional protection of economic rights, lasting from the late nineteenth century until the late 1930s.[57] 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.[58] 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. This inconsistency became most apparent during the Great Depression, when *Lochner*-style doctrines were used to invalidate

portions of the New Deal.[59] 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 – much of this book is about how to do that in the context of thinking, reading, and speaking. 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 argument along these lines.[60] Justice Breyer made a similar point in his *Sorrell* dissent, arguing "[a]t 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."[61] The many new uses to which we 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, where the trade in information is a multi-billion dollar industry, government should be able to regulate the huge flows of personal information, as well as the uses to which this information can be put. Moreover, if our lives become digital, but if data is speech, regulation of many kinds of social problems will become impossible. There will certainly be cases at the borders, 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 the *Lochner* case that the freedom of contract should immunize them from regulation. We 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. But the ambiguity of the Right to Be Forgotten is a helpful point on which to end this Part of the book, because it illustrates my general argument: Ordinary commercial regulations of the data trade are constitutional, but tort rights to censor the media aren't.

At the most basic level, the general encouragement that personal data *should* be deleted at some point poses no constitutional problems. As I will explain in Chapter 11, 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 health, political, or financial data. Governments could promote the importance of this social norm without mandating it, which would be clearly constitutional.

We could also imagine the Right to Be Forgotten being imposed on certain data holders as a consequence of their relationship with users who supply them with their 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. (Of course, most sites, including Facebook already provide this feature, though the law does not require it). 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 information 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 (like criminal records and lawsuits older than seven years).[62] At least where 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, it is because the version of the right proposed for the revisions to the EU Directive have taken essentially this form that the proposal has generated so much free speech concern. The proposed regulation would allow anyone to require any online service provider to delete any information they had about them.[63] This is a much more sweeping version of the right, which would, for instance, allow the deletion of potentially newsworthy information about a person provided by others.[64] 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.

But 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 *Le Droit à l'Oubli* 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, and not to unelected judges. Making policy mistakes is sometimes a price we pay for self-government.

---

[1] U.S. Dep't Of Health, Educ. & Welfare, *Records, Computers, And The Rights Of Citizens: Report Of The Secretary's Advisory Comm. On Automated Personal Data Systems* (1973).
[2] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 STAN. TECH. L. REV. 1 (2001).
[3] DANIEL J. SOLOVE AND PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 37-40 (4th ed. 2011).
[4] Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 514–15 (1995).
[5] European Commission, *Commission Proposes a Comprehensive Reform of the Data Protection Rules* (Jan. 25, 2012), http://ec.europa.eu/justice/newsroom/dataprotection/news/120125_en.htm.
[6] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009).
[7] 18 U.S.C. § 2710(e); 15 U.S.C. § 1681(w).
[8] Center for Democracy and Technology, *On The "Right To Be Forgotten": Challenges And Suggested Changes to the Data Protection Regulation*, May 2, 2013, available at https://www.cdt.org/files/pdfs/CDT-Free-Expression-and-the-RTBF.pdf.
[9] Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1561-62 (2000).
[10] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1167-68 (2005).
[11] 20 U.S.C. § 1232g.
[12] See, *e.g.*, MO. REV. STAT. § 182.817 (2000); (representative state library privacy statute); Health Insurance Portability and Accountability Act Regulations (HIPAA), 45 C.F.R §§ 160-64 (2002) (Health privacy); Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970) (consumer financial information).
[13] Richards, *Data Privacy*, *supra*, at 1194-1207.
[14] Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650 (2009).
[15] 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, 1050-51 (2000).
[16] FRED H. CATE, PRIVACY IN THE INFORMATION AGE 68-71 (1997).
[17] Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2013).
[18] 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 (1979); Okla. Publ'g Corp. v. Okla. County Dist. Court, 430 U.S. 308 (1977); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975).
[19] *Bartnicki*, 532 U.S. at 529 (quoting Florida Star, 491 U.S. at 532-33).
[20] See generally Richards, *Data Privacy*, *supra*, at 1182-83 (collecting examples).
[21] Solove & Richards, *supra*.
[22] Cohen v. Cowles Media, 501 U.S. 663, 670 (1991).
[23] Trans Union Corp. v. FTC, 245 F.3d 809, 818–19 (D.C. Cir. 2001); Individual Reference Servs. Corp. 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). The Supreme Court denied certiorari, Trans Union LLC v. FTC, 536 U.S. 915 (2002), although Justice Kennedy dissented. Trans Union LLC v. FTC, 536 U.S. 915, 916 (2002) (Kennedy, J., dissenting from denial of certiorari).
[24] On its website, IMS declares itself as "a leading provider of information, services and technology for the healthcare industry," and as a provider of "Analytics and services: Integrated solutions across healthcare to optimize commercial effectiveness, clinical decisions and care delivery." See www.imshealth.com.
[25] *Id.*

[26] Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, 63 VT. L. REV. 931 (2012).
[27] Vt. Stat. Ann., Tit. 18, § 4631 (Supp. 2010).
[28] IMS Health, Inc. v. Ayotte, 550 F.3d 42, 91 (2008).
[29] 131 S.Ct. 2653 (2011).
[30] *Sorrell*, 131 S. Ct. at 2672.
[31] *Id*. at 2663.
[32] 505 U.S. 377 (1992).
[33] *Id*. at 391.
[34] *Sorrell*, 131 S. Ct. at 2657 (citing *RAV, supra*).
[35] *Id*. at 2663
[36] *Id*. at 2667 (citations omitted).
[37] *Id*.
[38] *Id*. at 2763 (Breyer, J., dissenting)
[39] Ashutosh Bhagwat, *Sorrell v. IMS Health: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 856 (2012).
[40] Jane Bambauer, *Is Data Speech?* 66 STAN. L. REV. at [ssrn 7] (forthcoming 2014).
[41] Volokh, *supra*, at 1051.
[42] 42 U.S.C. § 1320d-2; 45 CFR pts. 160 and 164 (2010).
[43] *Sorrell*, 131 S.Ct at 2668.
[44] *Sorrell*, 131 S.Ct. at 2672.
[45] See ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 474, 529–30 (2001).
[46] See Richards, *Data Privacy*, *supra*, at 1168-1181; Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765 (2004).
[47] See Schauer, *supra*, at 1805 (providing examples).
[48] See Schauer, *supra*, at 1768.
[49] See, *e.g*., GEOFFREY R. STONE ET AL., THE FIRST AMENDMENT 3 (4th ed. 2012).
[50] See, *e.g*., RONALD KROTOSZYNSKI, THE FIRST AMENDMENT IN CROSS-CULTURAL PERSPECTIVE 12-25 (2006).
[51] For political expression, *see, e.g*., New York Times v. Sullivan, 376 U.S. 254 (1964); Cohen v. California, 403 U.S. 15 (1971). For artistic expression, *see, e.g*., Burstyn v. Wilson, 343 U.S. 495 (1952); Brown v. Entertainment Merchants Assn., 131 S. Ct. 2729 (2011). For advertising, *see, e.g*., Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of NY, 447 U.S. 557 (1980); Lorillard Tobacco Co. v. Reilly, 533 U.S. 525 (2001).
[52] See*, e.g*., Cites RAV v. City of St. Paul, 505 U.S. 377 (1992) (cross burning); *Cohen*, *supra* note 51, (swearing); Barnes v. Glen Theatre, Inc., 501 U.S. 560 (1991); Schad v. Borough of Mt. Ephraim, 452 U.S. 61 (1981) (nude dancing); Ashcroft v. ACLU, 535 U.S. 564 (2002) (virtual child pornography); Bridges v. California, 314 U.S. 252 (1941) (threats); United States v. Alvarez, 132 S. Ct. 2537 (2012) (lies); Snyder v. Phelps, 131 S. Ct. 1207 (2011) (hate speech); Boy Scouts of America v. Dale, 530 U.S. 620 (2000) (discrimination).
[53] ALEXANDER BICKEL, THE LEAST DANGEROUS BRANCH 16 (1962).
[54] See Barry Friedman, *The History of the Countermajoritarian Difficulty, Part Three: The Lesson of Lochner*, 76 N.Y.U. L. REV. 1383, 1392 (2001).
[55] G. EDWARD WHITE, THE CONSTITUTION AND THE NEW DEAL 241-42 (2000).
[56] 198 U.S. 45 (1905).
[57] BARRY CUSHMAN, RETHINKING THE NEW DEAL COURT (1998).
[58] Jack M. Balkin, *'Wrong the Day it Was Decided': Lochner and Constitutional Historicism*, 85 B.U. L. REV. 677 (2005).
[59] *Id*.
[60] Richards, *Data Privacy*, *supra*, at 1210-21. I should disclose that I gave *pro bono* counsel to the State of Vermont during the *Sorrell* litigation.
[61] *Id*. at 2685 (Breyer, J., dissenting).
[62] 15 U.S.C. § 16781c(b).
[63] European Commission, *supra*.
[64] Center for Democracy, and Technology, *supra*.