


2005

Reconciling Data Privacy and the First Amendment

Neil M. Richards

Washington University in St. Louis School of Law, nrichards@wustl.edu

Follow this and additional works at: https://openscholarship.wustl.edu/law_scholarship

 Part of the [Constitutional Law Commons](#), [First Amendment Commons](#), [Jurisprudence Commons](#), [Legal Studies Commons](#), and the [Privacy Law Commons](#)

Repository Citation

Richards, Neil M., "Reconciling Data Privacy and the First Amendment" (2005). *Scholarship@WashULaw*. 512.

https://openscholarship.wustl.edu/law_scholarship/512

This Article is brought to you for free and open access by the Law School at Washington University Open Scholarship. It has been accepted for inclusion in Scholarship@WashULaw by an authorized administrator of Washington University Open Scholarship. For more information, please contact digital@wumail.wustl.edu.

RECONCILING DATA PRIVACY AND THE FIRST AMENDMENT

Neil M. Richards^{*}

This Article challenges the First Amendment critique of data privacy regulation—the claim that data privacy rules restrict the dissemination of truthful information and thus violate the First Amendment. The critique, which is ascendant in privacy discourse, warps legislative and judicial processes and threatens the constitutionalization of information policy. The First Amendment critique should be rejected for three reasons. First, it mistakenly equates privacy regulation with speech regulation. Building on scholarship examining the boundaries of First Amendment protection, this Article suggests that “speech restrictions” in a wide variety of commercial contexts have never triggered heightened First Amendment scrutiny, refuting the claim that all information flow regulations fall within the First Amendment. Second, the critique inaccurately describes current First Amendment doctrine. To demonstrate this point, this Article divides regulations of information flows into four analytic categories and demonstrates how, in each category, ordinary doctrinal tools can be used to uphold the constitutionality of consumer privacy rules. Third, the critique is normatively unpersuasive. Relying on recent intellectual histories of American constitutional law, this Article argues that fundamental jurisprudential reasons counsel against acceptance of the First Amendment critique. From the perspective of privacy law, there are striking parallels between the critique’s advocacy of “freedom of information” and the discredited “freedom of contract” regime of Lochner. More importantly, from the perspective of First Amendment law, the critique threatens to obliterate the distinction between economic and political rights at the core of post–New Deal constitutionalism. Rejecting the First Amendment critique thus has real advantages. At the level of policy, it preserves the ability of legislatures to develop information policy in a nuanced way. And at the level of theory, it preserves the basic dualism upon which the modern edifice of rights jurisprudence is built.

^{*} Associate Professor of Law, Washington University. The author would like to thank the following people who helped immeasurably at the various stages of this project: Sam Bagenstos, Ken Bamberger, Kathie Barnes, Lillian BeVier, Chris Bowers, Trey Childress, John Harrison, Chris Hoofnagle, Peter Joy, Orin Kerr, Pauline Kim, Tom Nachbar, Troy Paredes, Wendy Niece Richards, Bo Rutledge, Joel Seligman, Daniel Solove, Peter Swire, and Eugene Volokh. This Article was also shaped significantly by the participants in law faculty workshops at the University of Virginia, Washington University, the College of William & Mary, the University of Illinois, Ohio State University, and the University of Alabama. Yvonne Ingram and Carol Wibbenmeyer provided invaluable secretarial help, and Sid Karamaju, Matt Kriegel, Megan Dredla, and Matt Bunda provided excellent research assistance.

INTRODUCTION.....	1150
I. THE FIRST AMENDMENT CRITIQUE OF DATA PRIVACY REGULATION.....	1154
A. The Database Problem.....	1156
B. The First Amendment Critique.....	1160
II. ARE PRIVACY RULES SPEECH RULES?.....	1165
A. Privacy Regulation Through Codes of Fair Information Practices.....	1166
B. The Constitutional Metaphysics of "Speech".....	1168
III. CATEGORIZING PRIVACY RULES UNDER THE FIRST AMENDMENT.....	1181
A. Information Collection Rules.....	1182
B. Information Use Rules.....	1190
C. Information Disclosure Rules.....	1194
1. Contract-based Nondisclosure Rules.....	1201
2. Creation of Nondisclosure Rules via Generally Applicable Law.....	1204
D. Regulation of Direct Marketing.....	1207
IV. THE PERILS OF VOLOKHNER.....	1210
A. The First Amendment Critique and "Freedom of Information" as <i>Lochner</i>	1211
B. The First Amendment Critique and the Bifurcated Review Project.....	1217
CONCLUSION.....	1221

INTRODUCTION

Although private-sector databases containing large amounts of personal information have existed for several decades, a number of recent technological advances and cultural shifts have enabled the easier dissemination of such information and the creation of larger, more detailed, and more useful databases.¹ While these advances permit ever-more efficient and valuable uses of consumer information by businesses, they also raise a cluster of undeniable but poorly defined legal issues about the rights of consumers to participate in, oversee, or control the ways in which data about them is used. Proposals attempting to resolve this so-called "database problem"² have been bedeviled by a range of practical and theoretical objections. Foremost among these objections is the widely held belief that because the First Amendment protects

1. See, e.g., FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* (1997); LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999); DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* (2004); *TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE* (Philip E. Agre & Marc Rotenberg eds., 1997); Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393 (2002); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

2. Scholars grappling with the "database problem" have argued that the rights of individuals are threatened by detailed private-sector databases containing profiles of their preferences. These profiles contain potentially embarrassing information, including information about their health, political views, or sexual activities or inclinations. See generally SOLOVE, *supra* note 1, at 13–26.

at its core the dissemination of truthful information, any right of “data privacy” is in direct conflict with the First Amendment because any attempt to regulate the flow of personal data would inevitably require the government to impose unconstitutional restrictions on speech. This position, which I call the “First Amendment critique” of data privacy, enjoys widespread currency in the legal academy, the private sector, and recent privacy jurisprudence. For example, Eugene Volokh has argued that “[w]e already have a code of ‘fair information practices,’ and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits).”³

This Article takes issue with the conventional wisdom that regulating databases regulates speech, that the First Amendment is thus in conflict with the right of data privacy, and that the Constitution thereby imposes an insuperable barrier to basic efforts to tackle the database problem. I argue that the relationship between privacy and the First Amendment is complex, but that it is not irreconcilable. Much of the perceived conflict results from an underappreciation of the definitional murkiness that suffuses existing legal conceptions of “privacy” and “speech.” Such murkiness has allowed what are essentially consumer protection issues in the economic rights context to be transformed into civil rights issues of the highest magnitude, as opponents of data privacy regulation have seized upon the First Amendment as a handy means of derailing proposals to deal with the database problem. The First Amendment critics overstate the First Amendment issues at stake in the context of most database regulation proposals, because such proposals are not regulation of anything within the “freedom of speech” protected by the First Amendment. Putting First Amendment rights talk to one side allows us to look at data privacy rules more clearly. And this new clarity reveals that a wide variety of these rules are fully justifiable under well-established First Amendment theory, either because they do not regulate “speech” protected by the First Amendment, or because they are legitimate speech regulations under existing doctrine.

My approach has, I believe, significant advantages for both data privacy and free speech. On the privacy side, harmonizing data privacy with free speech removes a significant theoretical and practical obstacle to constructive discussions about, and potential solutions to, the database problem. It also avoids the constitutionalization of domestic information policy, permitting that policy to be developed in a way that reflects the enormous complexity of the issue. And on the speech side, recognizing the murky way that we perceive the

3. 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, 1051 (2000).

existence of First Amendment problems allows us to assess both speech and nonspeech issues more effectively. More fundamentally, resisting the creep of First Amendment analysis into the economic rights and commercial context preserves the basic and essential division between civil and economic rights at the core of modern constitutionalism.

I develop these claims in four parts. Part I sets forth the data privacy issues raised by the collection, aggregation, and use of large amounts of personal information by private-sector businesses. Next, it sketches the First Amendment critique, which posits that attempts to regulate the database problem through law run directly into the unyielding strictures of the First Amendment. Under this view, data privacy rules that give individuals the right to control how their personal information is used restrict communications between speakers and thus impermissibly burden protected speech. The critique suggests not only that legal protection of data privacy is contrary to current First Amendment jurisprudence, but also that creating new free speech exemptions to permit data privacy “speech restrictions” would have many unfortunate consequences, including providing powerful rationales to support other, less benign speech restrictions. I argue that although the critique raises a host of practical and theoretical problems for data privacy law, information policy, and even free speech theory itself, existing scholarly responses to the First Amendment critique of database regulation are either incomplete or unsatisfying because they grant too much ground to the First Amendment critics with respect to the scope of the First Amendment in this context.

Part II responds to the First Amendment critics by suggesting that the simple logic equating privacy regulation with speech regulation is incorrect. Indeed, this is entirely the wrong way to frame the issue, as it rests on an overbroad conception of the types of rules that are perceived to implicate First Amendment analysis. The First Amendment critics’ assumption not only ignores the reality that few data privacy rules actually involve speech, but also significantly overstates the breadth of the protection afforded by the First a protected by the First Amendment, because large categories of “speech” regulations (such as criminal solicitation, anticompetitive offers, and copyright infringement) do not in reality trigger heightened First Amendment scrutiny. Building upon the work of the few scholars to have examined the First Amendment in this way, I suggest that much of this “speech” is either outside the scope of the freedom of speech protected by the First Amendment, or constitutes a hitherto unnoticed category of speech warranting rational basis review. I then defend this conception of the scope of First Amendment analysis against both First Amendment critics and

their pro-privacy opponents, each of whom too readily accepts the presence of a tension or conflict between privacy rules and speech rights.

Following this reconceptualization of the relationship between free speech and privacy, Part III responds to the First Amendment critique in more detail, demonstrating how existing doctrine fully supports a wide variety of privacy regulations without violating the First Amendment. In order to assess and demonstrate the constitutionality of such rules more easily, I divide privacy rules that implicate information flows into four categories: collection rules, use rules, disclosure rules, and telemarketing rules. Information collection rules, which govern the circumstances under which persons can collect information about others, create virtually no First Amendment problems and have been upheld in a wide variety of contexts. Similarly, information use rules also raise few issues of constitutional magnitude, because our law does not consider the use of information to make decisions to be “speech” any more than collecting information is “speaking.” While information disclosures are a harder case than use or collection, I demonstrate that, when properly conceptualized, nondisclosure rules in the database context do not significantly implicate the First Amendment. Regulating how two parties to a commercial transaction act with respect to information received during that transaction no more offends the Constitution than does government regulation of other aspects of the commercial relationship. Indeed, our law is replete with instances in which confidential information is protected against disclosure under a whole host of public and private law rules, few of which have ever been thought to involve restrictions on speech. Finally, I address direct regulation of telemarketing, and argue that although such regulation certainly implicates the commercial speech rights of telemarketers, the First Amendment nevertheless permits significant regulation of telemarketing activity. Accordingly, I argue, ordinary data privacy rules are fully consistent with the First Amendment.

Finally, Part IV contends with the First Amendment critique at a more abstract level, placing the critique in its historical and jurisprudential context. I argue that when viewed from the twin perspectives of privacy law and First Amendment law, the real theoretical problems of the First Amendment critique are made manifest. From the privacy law perspective, the modern First Amendment critique of data privacy regulation will, if it is unchallenged, prohibit discussion and resolution of the tremendously thorny database problem, thereby constitutionalizing national information policy and placing its resolution outside the democratic process. Indeed, the parallels are striking between the strong form of the First Amendment critique and the discredited “liberty of contract” doctrine of the *Lochner* period. Drawing upon

recent scholarship treating legal history as a species of intellectual history, I argue that both *Lochner* and the First Amendment critique represent responses to the leading economic public policy issue of their day with a liberal theory of rights constitutionalism that is fundamentally flawed. Finally, looking at the critique from the First Amendment law perspective, I argue that the broad, expansive, and slippery conceptualization of the First Amendment at the core of the First Amendment critique is ultimately inconsistent with the basic dualist premise of modern constitutionalism—the bifurcated standards of judicial review given to civil versus economic rights. I assert the critique paves the way for the obliteration of the distinction between economic and civil rights at the core of post-*Lochner* American constitutionalism. Serious recognition of the First Amendment critique would result not only in the constitutionalization of a major and complex policy issue, but also would threaten to unravel the basic premise upon which post-New Deal constitutionalism is based.

I. THE FIRST AMENDMENT CRITIQUE OF DATA PRIVACY REGULATION

Scholars exploring the conflict between the right of privacy and the First Amendment have traditionally located its origins with the publication of Samuel Warren and Louis Brandeis's foundational 1890 article "The Right to Privacy."⁴ In their article, Warren and Brandeis sought to establish a common law tort of "privacy" to protect principally against intrusions by an overzealous media.⁵ Although a conflict between privacy and speech might thus seem inevitable, this conclusion is belied somewhat by the fact that both privacy law and modern First Amendment doctrine can trace their origins back to the turn of the twentieth century when both were guided significantly by the writings of Louis Brandeis. Thus, while Brandeis's famous *Harvard Law Review* article is widely understood as the progenitor of twentieth-century privacy law,⁶ his concurrence in *Whitney v. California*⁷ has been equally influential in the creation and development of modern free speech jurisprudence.⁸

4. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); see also LAWRENCE M. FRIEDMAN, *AMERICAN LAW IN THE TWENTIETH CENTURY* 369 (2002); Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 1 (1979); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 292 (1983).

5. See Warren & Brandeis, *supra* note 4, at 195.

6. See, e.g., Glancy, *supra* note 4, at 1; Zimmerman, *supra* note 4, at 292.

7. 274 U.S. 357, 372–80 (1927) (Brandeis, J., concurring).

8. See HARRY KALVEN, JR., *A WORTHY TRADITION: FREEDOM OF SPEECH IN AMERICA* 156–66 (1988); DAVID M. RABBAN, *FREE SPEECH IN ITS FORGOTTEN YEARS* 369 (1997); G. EDWARD WHITE, *THE CONSTITUTION AND THE NEW DEAL* 143 (2000); Ashutosh A. Bhagwat, *The Story of Whitney v. California: The Power of Ideas*, in *CONSTITUTIONAL LAW STORIES* 407, 407–08

Although privacy and speech have shared an uneasy coexistence in American law, this tension is a product of a conceptual murkiness shared by both doctrines, rather than any fundamental incompatibility. Despite its recognition for over a century,⁹ the right to privacy has been poorly articulated and only vaguely theorized. As a result, modern commentators despair at ever being able to define “privacy” coherently.¹⁰ Although the First Amendment has received greater theoretical attention by judges and scholars, latent murkiness in First Amendment theory also persists, exacerbating the perceived tensions with privacy theory.¹¹ Nevertheless, when the First Amendment and privacy have come into conflict in the past, most significantly in a long line of Supreme Court cases invalidating attempts to impose liability on the press for committing the tort of disclosure of private information, the First Amendment has universally triumphed.¹² Such a result is undoubtedly consistent with the basic tenet of modern constitutional law that public discussions of issues of matters of public concern “should be uninhibited, robust, and wide-open.”¹³ Modern First Amendment critics of data privacy regulation hearken back to this long tradition of privacy being in tension with the First Amendment, with privacy inevitably losing out when weighed against the constitutional primacy of free speech. And although defenders of privacy have struggled to articulate a theory whereby privacy rules can withstand First Amendment scrutiny, few scholars have been able to articulate persuasive justifications why any right of data privacy should survive when pitted against the robust modern First Amendment.¹⁴

With this context in mind, I attempt in this part to frame the basic problem facing scholars, judges, and lawmakers confronting the conceptual intersection of data privacy and the First Amendment. First, I briefly describe the database problem in order to identify the practical stakes in this often theoretical debate. Second, I describe the First Amendment critique of data privacy regulation. I argue that no compelling response to the First Amendment critique has yet been fully articulated in the privacy literature; although a few scholars have attempted to take on the First Amendment critics, their arguments are neither complete nor convincing.

(Michael C. Dorf ed., 2004); Vincent Blasi, *The First Amendment and the Ideal of Civic Courage: The Brandeis Opinion in Whitney v. California*, 29 WM. & MARY L. REV. 653, 668 (1988).

9. See Kent Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335.

10. See Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202 (1998); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1088 (2002).

11. See *infra* Part II.

12. See, e.g., *Bartnicki v. Vopper*, 532 U.S. 514 (2001).

13. *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964).

14. See *infra* note 71 and accompanying text.

A. The Database Problem

There is a vast and often redundant literature describing the database problem, and I have no intention of adding to it here.¹⁵ However, a brief overview of the contours of the problem will be helpful in setting up and contextualizing the analysis that follows. Governments have been keeping records about their citizens for centuries, most notably tax and criminal records.¹⁶ In the nineteenth century, the federal census raised what we would today call privacy concerns and federal law was amended to protect the confidentiality of information collected by the government.¹⁷ In the twentieth century, with the expansion of American government during and after the New Deal period, dozens of national government agencies including the FBI, the Internal Revenue Service, the military, and the Social Security Administration began keeping trillions of records on individual citizens.¹⁸ The invention and spread of increasingly cheaper and more capable computers only facilitated this process, particularly as the use of social security numbers as uniquely effective personal identifiers enabled agencies to link records and integrate them with other databases, including state and private databases.¹⁹ As the Supreme Court has recognized, modern government possesses an "accumulation of vast amounts of personal information in computerized data banks or other massive government files," including information taken from "[t]he collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of our criminal laws."²⁰

Public sector databases do create significant privacy problems, including increasing the risk of identity theft, chilling expressive but eccentric behaviors, revealing embarrassing information to private parties, and raising the specter of an Orwellian state.²¹ But such problems can be addressed (at least

15. For a detailed discussion of the database problem, see sources cited *supra* note 1.

16. See, e.g., ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 12 (2000); David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 31-32 (1999); Solove, *supra* note 1, at 1400 & n.29.

17. See Act of Mar. 1, 1889, ch. 319, §§ 8, 13, 25 Stat. 760 (imposing \$500 fine for disclosure of census information); see also Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1905 (1981).

18. See BALLARD C. CAMPBELL, THE GROWTH OF AMERICAN GOVERNMENT 231-32 (1995).

19. See *id.* at 232.

20. United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 770 (1989) (quoting *Whalen v. Roe*, 429 U.S. 589, 605 (1977)).

21. See Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1138 (2002).

at a theoretical level) through ordinary public law rules without any significant constitutional impediments.²² No one suggests that the government has a right to publish any and all secrets it learns about its citizens absent a need to do so; indeed, the Supreme Court has stated on several occasions that individuals have a constitutional right to prevent the government from making public at least certain kinds of information about themselves.²³

The same technological advances that have permitted the creation of public sector databases have also allowed businesses and other private-sector entities to keep ever larger and more detailed records about individuals. These records can be created from a variety of sources, including publicly available government records, human resource databases, promotional activities such as contests and mass mailings, and transactional data from noncash purchases, frequent shopper programs, and Internet and telephone use.²⁴ Information collected from these sources often has more value as a saleable commodity than for the purposes for which it was originally collected. Indeed, corporations are eager to acquire many different kinds of information about consumers, including information about their lifestyles, tastes, and even psychological profiles.²⁵ Such information is provided by the “profiling industry,” a group of companies that aggregate information contained in private databases to create consumer profiles that are then offered for sale to interested parties, be they private or public.²⁶ The level of detail contained in such profiles is striking, and can include information such as a person’s social security number, shopping preferences, health information (including diseases and disorders suffered), financial information, race, weight, clothing size, arrest record, lifestyle preferences, hobbies, religion, reading preferences, homeownership, charitable contributions, mail order purchases and type, and pet ownership.²⁷ Such information can be bought for as little as \$65 per thou-

22. For example, the Privacy Act of 1974, 5 U.S.C. § 552a (2000), gives individuals certain rights with respect to data about them in federal government databases.

23. E.g., *Nixon v. Adm’r of Gen. Servs.*, 433 U.S. 425 (1977); *Whalen*, 429 U.S. 589. Backstopping this constitutional protection is the Freedom of Information Act, 5 U.S.C. § 552. Although the Act generally provides for public access to information held by the government, it exempts from disclosure certain categories of government information, the disclosure of which might constitute an “unwarranted invasion of personal privacy.” *Id.* §§ 552(b)(6), 552(b)(7)(C).

24. See, e.g., SOLOVE, *supra* note 1, at 19; Philip E. Agre, *Introduction to TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE*, *supra* note 1, at 1, 3; Elec. Privacy Info. Ctr., *Privacy and Consumer Profiling*, at <http://www.epic.org/privacy/profiling/>.

25. See Solove, *supra* note 1, at 1404.

26. Such companies are also known as “commercial data brokers,” or “CDBs.” See generally Chris J. Hoofnagle, *Big Brother’s Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT’L L. & COM. REG. 595 (2004).

27. Elec. Privacy Info. Ctr., *supra* note 24.

sand names, categorized by the type of consumer sought by marketers.²⁸ One profiling company was reported to have personal and private information about virtually every consumer in the United States, Britain, and Australia.²⁹ In addition to being intrusive and deeply unsettling to many people, the multibillion dollar profiling industry provides the lifeblood of data on which the direct marketing industry survives.³⁰

At the practical level, such activities raise at least four kinds of privacy concerns. First, databases can be used to process “sensitive information”—nonnewsworthy but nonetheless potentially embarrassing or highly personal information. Most people would be horrified if this information floated freely from database to database. Second, “über-databases” can be created, composed of nonsensitive information in such enormous quantities that the database constitutes a highly detailed dossier of a person’s entire existence.³¹ Third, the information contained in consumer profiles can be quite inaccurate.³² Finally, there are no meaningful legal requirements that personal information in consumer profiles be kept securely. If used improperly, the sheer level of detail contained in consumer profiles can facilitate crimes such as identity theft,³³ stalking,³⁴ or harassment.³⁵

Large-scale private databases also significantly raise the stakes for government surveillance. Governments have long used private records to spy upon their citizens—often with sinister consequences³⁶—and the availability of

28. See *id.*

29. See A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1473–74 (2000); see also SOLOVE, *supra* note 1, at 18–21 (collecting other examples).

30. See Ely R. Levy & Norman I. Silber, *Nonprofit Fundraising and Consumer Protection: A Donor’s Right to Privacy*, 15 STAN. L. & POL’Y REV. 519, 543–44 (2004).

31. See, e.g., Karas, *supra* note 1, at 437–39.

32. See, e.g., John Rothchild, *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*, 74 IND. L.J. 893, 972–73 (1999).

33. See Daniel J. Solove, *Identity Theft, Privacy and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003).

34. One of the most alarming incidents involves the case of Amy Boyer, who was murdered at her workplace by a man who received Boyer’s date of birth, social security number, home address, and work address from an information broker. The information broker had used pretexting—using already available information and lying about one’s identity and purpose—to get Boyer to reveal her employment information. See *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1009 (N.H. 2003).

35. In one case, a major profiling company used inmates to process consumer data surveys. One of the prisoners used information from one woman’s survey—including her name, address, buying habits, and medical information—to harass her, sending her a sexually explicit letter sprinkled with personal, identifying details and proposing to visit her home upon his release. See Stanley S. Arkin, *Misuse and Misappropriation of Electronically Stored Information*, N.Y. L.J., July 23, 2001, at 3.

36. Perhaps the most sinister such use of business records occurred in 1940, when the invading German armies used business records, among other sources, to identify Jews for roundup by the Gestapo. See Richard Sobel, *The Degradation of Political Identity Under a National Identification*

larger and more detailed private records about people makes such forms of surveillance easier for governments to engage in.³⁷ Indeed, recent activities by the federal government to investigate and forestall terrorism have frequently relied on computerized private-sector customer records containing financial, airline passenger, and other data.³⁸ The government also has been contracting increasingly with private businesses, by acquiring databases of personal information and funding novel private-sector data collection projects.³⁹ To the extent such private data collection is not state action, it allows the government, in effect, to outsource surveillance beyond the scope of otherwise applicable statutory and constitutional restrictions.⁴⁰

Database privacy is a complex problem, and database regulation would be costly.⁴¹ This is particularly true insofar as privacy regulations by their very nature would tend to keep information away from individuals who would like to see it, be they employers, credit card companies, potential spouses, or even journalists. And regulation of profiling practices would provide, at a minimum, significant economic costs to that industry. But many scholars have argued that there are other costs to privacy regulation. Kent Walker asserts that “[l]egislating privacy comes at a cost: more notices and forms, higher prices, fewer free services, less convenience, and, often, less security.”⁴² Some commentators have argued that broad privacy rules would not only be costly, but also could lead to unintended consequences such as a decrease in self-regulation, services offered to the public, and data made available for research.⁴³ Law and economics scholars like Richard Posner conclude that privacy rules inefficiently decrease the total supply of information, increase

System, 8 B.U. J. SCI. & TECH. L. 37, 52 (2002); see also WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION 22–23 (1992).

37. See Hoofnagle, *supra* note 26, at 611 (noting that database companies package personal data for sale to law enforcement and offer substantial discounts to government customers).

38. See Robert O’Harrow, Jr., *In Terror War, Privacy vs. Security*, WASH. POST, June 3, 2002, at A1; see also Karen E. Jones, Comment, *The Effect of the Homeland Security Act on Online Privacy and the Freedom of Information Act*, 72 U. CIN. L. REV. 787 (2003).

39. See SOLOVE, *supra* note 1, at 168–74.

40. See Hoofnagle, *supra* note 26, at 635–37.

41. For varying estimates, see Ted Bridis, *Industry Studies Attack Web-Privacy Laws*, WALL ST. J., Mar. 13, 2001, at B6 (estimating that regulation would cost the ninety largest financial institutions \$17 billion per year); see also ROBERT W. HAHN, AN ASSESSMENT OF THE COSTS OF PROPOSED ONLINE PRIVACY LEGISLATION 22–23 & tbl.2 (2001) (estimating a \$36 billion cost for online privacy regulation), available at <http://www.bbbonline.org/UnderstandingPrivacy/library/whitepapers/hahnstudy.pdf>; Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL’Y 87 (2001) (estimating a \$17.6 billion cost of privacy legislation relating to medical information costs).

42. Walker, *supra* note 41, at 87–88.

43. Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 158–61 (2002).

transaction costs, and encourage fraud.⁴⁴ Others extend this argument and claim that the inefficiency of privacy rules means that consumers are actually better off with less privacy regulation than with more, as the free, unfettered flow of information leads to a socially optimal result of lower prices for consumers.⁴⁵

B. The First Amendment Critique

The foregoing has not intended to propose regulatory solutions to the database problem, but merely to suggest that this problem is important, complex, and demands serious and thoughtful deliberation before it can be resolved in any meaningful way. Indeed, the database problem has produced no shortage of proposals seeking to address its privacy implications.⁴⁶ But virtually all such proposals run squarely into what I call the “First Amendment critique”: the claim that because the creation, assembly, and communication of information are at the core of the First Amendment, data privacy rules that restrict this expressive activity improperly burden free speech and are thus largely or entirely unconstitutional. The First Amendment critique is a significant theoretical and practical obstacle to data privacy regulation because it asserts that the First Amendment automatically resolves any privacy policy issues created by the database problem by preventing any regulatory solution that impinges upon the free flow of information. The simplicity and salience of the critique have caused it to become part of the conventional wisdom in the data privacy debate.⁴⁷ Indeed, privacy scholars have

44. See, e.g., RICHARD A. POSNER, *OVERCOMING LAW* 531–51 (1995); Richard A. Posner, *Blackmail, Privacy, and Freedom of Contract*, 141 U. PA. L. REV. 1817 (1993); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 632–33 (1980). But see Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2397–99 (1996) (arguing that privacy rules are rational from a law and economics perspective).

45. See, e.g., FRED H. CATE, FIRST AMENDMENT CTR., *THE PRIVACY PROBLEM: A BROADER VIEW OF INFORMATION PRIVACY AND THE COSTS AND CONSEQUENCES OF PROTECTING IT* (2003), available at <http://www.firstamendmentcenter.org/PDF/FirstReport.privacyproblem.pdf>; HAHN, *supra* note 41; PAUL H. RUBIN & THOMAS M. LENARD, *PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION* 8–9 (2002); Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2, ¶ 21–33, at http://stlr.stanford.edu/STLR/Articles/00_STLR_2/index.htm; see also FED. TRADE COMM’N, *PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE* (2000) (dissenting statement of Commissioner Orson Swindle), available at <http://www.ftc.gov/os/2000/05/privacyswindle.htm>.

46. See Hahn & Layne-Farrar, *supra* note 43 (collecting and assessing numerous such proposals).

47. See, e.g., Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1375–76 (2000).

been unable to refute the critique,⁴⁸ allowing it to dominate both constitutional jurisprudence and democratic policymaking with respect to data privacy.

The most prominent First Amendment critic is Eugene Volokh. Volokh starts from the proposition that although data privacy sounds unthreatening in the abstract, “the difficulty is 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.”⁴⁹ Accordingly, while private agreements to restrict speech are enforceable under express and implied contract principles, 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.⁵⁰ Indeed, Volokh goes so far as to conclude that “despite their intuitive appeal, restrictions on speech that reveals personal information are constitutional under current doctrine only if they are imposed by contract, express or implied.”⁵¹ Volokh’s argument can be boiled down to two basic elements: First, data privacy regulation that restricts the communication of information and that is not grounded in contract violates the First Amendment; and second, the changes to existing doctrine necessary to permit data privacy rules could be used to justify other, more sinister exceptions to free speech doctrine.⁵²

Other scholars make arguments similar to Volokh’s. Relying on the Supreme Court cases invalidating the privacy tort in the context of media publication of truthful facts, Fred Cate has argued more bluntly that electronic information flows should be entitled to full First Amendment protection, and that any attempt to restrict the communication of truthful data faces a high (if not insurmountable) First Amendment obstacle.⁵³ Solveig Singleton also suggests that efforts to regulate consumer privacy in the database

48. See *infra* note 71.

49. Volokh, *supra* note 3, at 1050–51.

50. *Id.* at 1051.

51. *Id.* at 1122.

52. *Id.* at 1051; see also *id.* at 1051 & n.4, 1116 (stating that “[C]odes of fair information practices” to protect privacy rights would not only “raise[] serious First Amendment problems” but would also make it “much easier for people to accept ‘codes of fair reporting,’ ‘codes of fair debate,’ ‘codes of fair filmmaking,’ ‘codes of fair political criticism,’ and the like.” (footnote omitted)). Volokh expands on the issue of slippery slopes at a more general level in Eugene Volokh, *The Mechanisms of the Slippery Slope*, 116 HARV. L. REV. 1026 (2003).

53. See CATE, *supra* note 1, at 68–71. Cate concludes that “[a]ny government effort to protect privacy, either directly or through the passage or enforcement of laws permitting suits by private parties, faces significant First Amendment obstacles.” *Id.* at 71; see also CATE, *supra* note 45, at 10–22; Fred H. Cate, *The First Amendment and the National Information Infrastructure*, 30 WAKE FOREST L. REV. 1, 48–50 (1995); Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35, 49–58 (2002).

context run squarely into established First Amendment limits on government power.⁵⁴ Singleton concludes “there is no justification for regulating the collection and use of data by the private sector. Regulations intended to protect privacy by outlawing or restricting the transfer of consumer information would violate rights of free speech.”⁵⁵ The critique has resonated not just with numerous scholars of a conservative or pro-business bent,⁵⁶ but also with liberal First Amendment scholars such as Robert O’Neil,⁵⁷ Rodney Smolla,⁵⁸ and Michael Froomkin.⁵⁹ Laurence Tribe has also argued publicly that the processing of personal data by telephone companies is speech entitled to full First Amendment protection. Tribe argued that such data is created and assembled by telephone companies for marketing, and that “the First Amendment protects [a speaker’s] right not only to advocate their cause but also to select what they believe to be the most effective means of so doing.”⁶⁰ Finally, other scholars who might not adopt the strong Volokh-Singleton formulation of the First Amendment critique nevertheless accept its basic premise that data privacy raises real

54. Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 132–53 (2000).

55. SOLVEIG SINGLETON, PRIVACY AS CENSORSHIP: A SKEPTICAL VIEW OF PROPOSALS TO REGULATE PRIVACY IN THE PRIVATE SECTOR (Cato Inst. Policy Analysis No. 295, 1998), at <http://www.cato.org/pubs/pas/pa-295.html>; Solveig Singleton, *Reviving a First Amendment Absolutism for the Internet*, 3 TEX. REV. L. & POL. 279 (1999) (arguing more generally for stronger First Amendment protection in the electronic context).

56. In addition to Volokh, *supra* note 3, and Solveig Singleton’s articles, *supra* notes 54–55, see, for example, TOM W. BELL, INTERNET PRIVACY AND SELF-REGULATION: LESSONS FROM THE PORN WARS 6–7 (Cato Inst., 2001), available at <http://www.cato.org/pubs/briefs/bp65.pdf>; JEREMY D. MISHKIN, MEDIA LAW RESOURCE CTR., PRIVACY ONLINE 2.0, at 11–13 (2002), at <http://www.medialaw.org/Template.cfm?Section=Archive7&Template=/ContentManagement/ContentDisplay.cfm&ContentID=1068>; Tom W. Bell, *Pornography, Privacy, and Digital Self Help*, 19 J. MARSHALL J. COMPUTER & INFO. L. 133, 144–46 (2000); Bruce E.H. Johnson, *The Battle Over Internet Privacy and the First Amendment*, COMPUTER & INTERNET L., Apr. 2001, at 21; Bruce E.H. Johnson & Kavita Amar, *Privacy Questions Arising in the Context of Commercial Speech*, in 1 COMMUNICATIONS LAW 2002, at 7, 7–8 (PLI Intellectual Prop. Practice Course, Handbook Series No. G-726, 2002); Robert A. Levy, *Turn the Ringer Off*, NAT’L REV. ONLINE, Oct. 2, 2003, at <http://www.nationalreview.com/comment/levy200310020827.asp> (arguing that the FCC’s Do-Not-Call Registry violates the First Amendment); Jonathan M. Winer, *Regulating the Free Flow of Information: A Privacy Czar as the Ultimate Big Brother*, 19 J. MARSHALL J. COMPUTER & INFO. L. 37, 47 & n.47 (2000).

57. ROBERT M. O’NEIL, THE FIRST AMENDMENT AND CIVIL LIABILITY 74–90 (2001).

58. Rodney A. Smolla, *Privacy and the First Amendment Right to Gather News*, 67 GEO. WASH. L. REV. 1097, 1138 (1999) (“As matters stand today, strong First Amendment doctrines stand in the way of many of the most meaningful privacy reforms.”).

59. Froomkin, *supra* note 29, at 1521–23 (concluding that the First Amendment raises serious questions about the constitutionality of existing federal privacy statutes).

60. Brief for Appellant at 6, *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (No. 98-3451).

First Amendment issues, and that regulation of consumer privacy needs to be crafted carefully to avoid constitutional objections.⁶¹

The salience of the First Amendment critique in academic and legal discourse has influenced both courts and policymaking. As a result, the First Amendment critique is a major obstacle to coherent data privacy regulation. Two recent cases illustrate the jurisprudential uncertainty that the critique has fomented. In *U.S. West, Inc. v. FCC*,⁶² the Tenth Circuit struck down as an unconstitutional burden on commercial speech a rule imposing a duty of confidentiality upon telephone companies with respect to customer data collected in the course of providing telephone service. Similarly, the First Amendment critique played a significant role in the recent litigation over the FCC's "Do-Not-Call" Registry, which allows consumers who do not wish to receive commercial telemarketing calls to place their telephone numbers on a list of numbers that telemarketers are forbidden from calling.⁶³ Applying the critique, a federal district court invalidated the Registry as an unconstitutional infringement on commercial speech.⁶⁴ Although the Tenth Circuit correctly⁶⁵

61. See, e.g., Vera Bergelson, *It's Personal, But Is It Mine? Towards Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 396–400 (2003) (noting that the First Amendment problems identified by Volokh, Singleton, and others should significantly shape the legal response to consumer privacy issues); Walker, *supra* note 41, at 123. Walker writes:

Recognizing that we are legislating in the shadow of the First Amendment suggests a powerful guiding principle for framing privacy regulations. Like any laws encroaching on the freedom of information, privacy regulations must be narrowly tailored and powerfully justified. . . . [L]egislators should identify a specific and real harm and tailor any responsive laws narrowly.

Id.; see also Stan Karas, *Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance*, 7 U. FLA. J. TECH. & POL'Y 3 (2002); James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 26–27 (2005); Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 675 (2002); William McGeveran, Note, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1822–24 (2001) (arguing that First Amendment principles render many consumer privacy rules unconstitutional, and shape outcomes); Scott Shorr, Note, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1811–18 (1995) (proposing a contractual approach to the problem of consumer credit reports because credit companies have a First Amendment right to disclose consumer credit information); Kyle Thomas Sammin, Note, *Any Port in a Storm: The Safe Harbor, The Gramm-Leach-Bliley Act, and the Problem of Privacy in Financial Services*, 36 GEO. WASH. INT'L L. REV. 653, 656 (2004).

62. 182 F.3d 1224.

63. 16 C.F.R. § 310.4(b)(1)(iii)(B) (2004).

64. *Mainstream Mktg. Servs. Inc. v. FTC*, 283 F. Supp. 2d 1151, 1167–68 (D. Colo. 2003), *rev'd*, 358 F.3d 1228, 1241 (10th Cir. 2004).

65. I have argued elsewhere that the Tenth Circuit's reversal of the lower court was correct, both as a doctrinal and a normative matter. See Caroline E. Mayer, *National No-Call List Upheld by Court*, WASH. POST, Feb. 18, 2004, at E1 ("The court [correctly] concluded that the right of people to enjoy their homes outweighs the right of companies to intrude upon that privacy to try and sell them things," Richards said.).

reversed the lower court on appeal,⁶⁶ the First Amendment critique nevertheless seriously complicated resolution of the issue, with the constitutionality of the Registry in limbo for months. Despite the ultimately satisfactory resolution of the Do-Not-Call litigation from a privacy perspective, courts remain deeply divided over the salience of the critique.⁶⁷ The Supreme Court has said little with respect to this issue, and has not granted certiorari to clear up the confusion among lower courts.⁶⁸

In addition to its effects on litigation, the First Amendment critique is a potent weapon against privacy rules in the legislative process. Perhaps because the critique is an easy political argument for opponents of regulation to make, and because it invites litigation whenever new privacy measures are enacted, lawmakers and regulators are likely to take the critique into account in drafting privacy rules, thereby skewing the outcome of such deliberative processes. For example, when the State of Washington attempted to pass a privacy bill in early 2000, the attempt was scuttled by business groups proffering Professor Volokh's claims that the free flow of commercial information is constitutionally compelled.⁶⁹ These examples illustrate the practical significance of the First Amendment critique—the confusion and discord that it is causing in both democratic policymaking and the courts.

Perhaps because of the inherent appeal of First Amendment arguments generally to legal academics (especially those who tend to support privacy rights),⁷⁰ surprisingly few scholars have challenged the First Amendment critique in any detail. Indeed, although a handful of scholars have disagreed with the arguments of Volokh and others who advocate the critique, they

66. *Mainstream Mktg. Servs.*, 358 F.3d at 1250–51.

67. *See, e.g.,* *L.A. Police Dep't v. United Reporting Publ'g Corp.*, 528 U.S. 32 (1999); *United Reporting Publ'g Corp. v. Cal. Highway Patrol*, 146 F.3d 1133, 1140 (9th Cir. 1998) (holding a California statute prohibiting release of arrestee names and addresses for commercial purposes unconstitutional under the *Central Hudson* test). In the context of credit report regulation, other courts have accepted the critique's premise that the sale of databases is "speech," but these courts have applied intermediate scrutiny and found the privacy interests sufficient to outweigh the business speech interests. *See, e.g.,* *Trans Union Corp. v. FTC*, 245 F.3d 809, 818–19 (D.C. Cir. 2001) (restricting a consumer reporting agency's sale of targeted marketing lists did not violate the First Amendment); *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). *But see* *Equifax Servs., Inc. v. Cohen*, 420 A.2d 189 (Me. 1980) (invalidating under the First Amendment a state law requiring the consent of a consumer before a firm could request that consumer's credit history).

68. *See, e.g.,* *Trans Union LLC v. FTC*, 536 U.S. 915 (2002) (Kennedy, J., dissenting from denial of certiorari).

69. *See* Johnson, *supra* note 56, at 23–24.

70. *See, e.g.,* THOMAS I. EMERSON, TOWARD A GENERAL THEORY OF THE FIRST AMENDMENT 76 (1966) ("Any society sincerely interested in protecting the right of privacy is hardly likely to be at the same time hostile to the right of free expression. Both interests tend to have the same friends and the same enemies.").

have done so either in short essays or in sections of longer pieces.⁷¹ This is unfortunate, because the First Amendment critique asserts a simple, constitutionalized solution to a complex and thorny social problem of the first importance. To be clear, I believe that the simplistic mantra of “freedom of information” is no more a satisfying solution to the complex database problem facing the digital age than the “freedom of contract” was to the industrial age a century ago.⁷² In the rest of this Article, I lay out a series of doctrinal, conceptual, and jurisprudential responses to the First Amendment critique. Reconceptualizing the First Amendment issues at stake in the database context reveals that the policy choices behind the regulation of private information in the computer age are not foreordained by the First Amendment.

II. ARE PRIVACY RULES SPEECH RULES?

One of the basic assumptions of the First Amendment critics is that regulating privacy is the same as regulating speech. This view is best summarized by Eugene Volokh, who argues:

[T]he 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. We already have a code of “fair information practices,” and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits), whether the communication is “fair” or not. While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.⁷³

This part tackles and rebuts this foundational assumption at the conceptual level. Although there exists much ambiguity not only in privacy law but also in the

71. The only piece that challenges the critique in depth is Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967 (2003). Solove's concern, however, is to justify privacy nondisclosure rules more generally (that is, outside the database context), not only against a First Amendment critique, but also against other normative challenges to keeping information private. *Id.* at 969–76. As I explain *infra* Part II, my approach to the First Amendment diverges significantly from Solove's, as I believe he grants too much ground to the First Amendment critics. Other scholars who have addressed the First Amendment critique of data privacy in a more abbreviated fashion include Cohen, *supra* note 47, at 1409–23, providing a thoughtful theoretical overview of data privacy issues and devoting fourteen pages to the issue; Kang, *supra* note 10, at 1287, providing a proposal for online privacy reform; and Paul Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000), a symposium comment to Volokh's article.

72. See *infra* Part IV.

73. Volokh, *supra* note 3, at 1050–51 (citations omitted).

scope of the First Amendment, there are definite, significant areas in which the two do not conflict. I hope to show that substantial regulation of privacy rights is possible without implicating the First Amendment at all, thereby setting the stage for a doctrinal and jurisprudential reconciliation in subsequent parts between the First Amendment and the right of data privacy.

Part II.A addresses the fundamental assumption of the First Amendment critics that privacy regulation means speech regulation. I argue that most data privacy regulations in the form of a “code of fair information practices” have nothing to do with free speech under anyone’s definition. Part II.B focuses on the regulation of information flows and suggests that the First Amendment accords heightened scrutiny to far fewer regulations of “speech” than previous scholars have assumed. I argue that First Amendment critics and the few privacy scholars to have responded to them have improperly conflated information flows—such as the sale of a database—with the “freedom of speech” protected by the First Amendment. In my view, there are valid First Amendment reasons for drawing distinctions between speech and information flows. Recognizing such distinctions provides a superior way of conceptualizing the First Amendment implications of the database problem.

A. Privacy Regulation Through Codes of Fair Information Practices

Regulation of the collection, use, and disclosure of personal data is often proposed as a code of fair information practices.⁷⁴ Such proposals call for a combination of tort and public law to regulate the relationship between the individuals who provide data and the entities that would collect, use, and disclose it.⁷⁵ One early code of fair information practices was envisioned by the federal Department of Housing, Education, and Welfare in 1973, which recommended that organizations collecting data should adhere to a series of norms. These included a prohibition on secret data collection, a right of access by individuals to view data about themselves and correct false data, and a right to prevent information collected for one purpose from being used for other purposes.⁷⁶ This report was the basis for the federal Privacy Act of 1974,⁷⁷ which established general rules for the collection, retention, use, and disclosure

74. See Schwartz, *supra* note 71, at 1561.

75. See Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 8, at http://stlr.stanford.edu/STLR/Articles/01_STLR_1/index.htm.

76. 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), available at <http://www.epic.org/privacy/hew1973report/>.

77. 5 U.S.C. § 552a (2000).

of personal information held by the federal government.⁷⁸ In particular, Section (e) of the Privacy Act mandates that federal agencies follow fair information practices.⁷⁹

The norms established by the Housing Department's report and the Privacy Act have been tremendously influential in the United States and other countries, and many scholars agree that there is a global consensus regarding the basic standards of fair information practices for both the public and private sectors.⁸⁰ Joel Reidenberg has summarized this consensus as guaranteeing four 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.⁸¹

Recognizing the similarity between the privacy issues in the public and private-sectors, numerous state and federal laws impose codes of fair information practices in a variety of private-sector contexts. Such statutes attempt to protect consumers from inappropriate uses of personal data by businesses.⁸² Federal examples of such laws include the Fair Credit Reporting Act,⁸³ the Electronic Communications Privacy Act (ECPA),⁸⁴ the Video Privacy Protection Act (VPPA),⁸⁵ and the Family Educational Rights and Privacy

78. For an assessment of the Privacy Act, see Robert Gellman, *Does Privacy Law Work?*, in *TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE*, *supra* note 1, at 193.

79. See Schwartz, *supra* note 71, at 1561 n.12; see also PAUL M. SCHWARTZ & JOEL R. REIDENBERG, *DATA PRIVACY LAW* § 5 (1996).

80. See Gellman, *supra* note 78, at 196.

81. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 *IOWA L. REV.* 497, 514–15 (1995). For an alternate but equivalent formulation of these principles, see Gellman, *supra* note 78, at 195–202.

82. For a comprehensive overview of the many federal statutes governing private sector records, see generally DANIEL J. SOLOVE & MARC ROTENBERG, *INFORMATION PRIVACY LAW* 491–566 (2003).

83. 15 U.S.C.A. § 1681–1681t (West 1998 & Supp. 2004) (regulating the disclosure and the use of consumer credit information, and giving consumers the right to receive copies of credit records and to correct erroneous information contained in such records).

84. 18 U.S.C.A. § 2511 (West 2000 & Supp. 2004) (prohibiting, inter alia, intentional interception of contents of telephone conversations or e-mail, and disclosure of contents of such communications to others).

85. 18 U.S.C. § 2710 (2000) (prohibiting video stores from disclosing to third parties videos that its customers have rented). The great irony of the VPPA is that it was passed in reaction to the disclosure of Supreme Court nominee Robert Bork's video records during his confirmation. Bork's nomination was defeated in part because of his opposition to a constitutional right of privacy. See RICHARD C. TURKINGTON & ANITA L. ALLEN, *PRIVACY LAW* 494 (2d ed. 2002).

Act.⁸⁶ Violations of such federal codes of fair information practices for the private sector are punished by both criminal law prosecutions and private tort law actions, which authorize significant minimum statutory and punitive damages.⁸⁷

Statutes that embody fair information principles do far more than merely regulate information flows or prevent disclosures. Paul Schwartz has argued 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.⁸⁸ Only principle three (providing protection against the use or disclosure of sensitive data) "corresponds to Volokh's idea of information privacy as the right to stop people from speaking about you."⁸⁹ Although I agree that many fair information practices do not regulate speech, if the First Amendment critics are correct that principle three nondisclosure rules are speech restrictions that violate the First Amendment, it follows that government enforcement of such rules under principle four by either direct regulation or the enforcement of tort judgments similarly violates the First Amendment. But, as I demonstrate below, nondisclosure rules, just like other elements of fair information practices applied to commercial databases, are fully consistent with the First Amendment. The most important point to take from the preceding discussion, however, is that even if one accepts that nondisclosure rules create First Amendment problems, significant 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.

B. The Constitutional Metaphysics of "Speech"

The insight that information privacy rules are usually modeled upon a code of fair information practices allows us to separate out many of the types of privacy regulations that have nothing to do with speech. It also shows that the rhetorical suggestion that all privacy rules are speech rules is significantly

86. 20 U.S.C.A. § 1232g (West 2000 & Supp. 2004) (regulating the disclosure of educational records maintained by primary, secondary, and postsecondary institutions that receive federal funds).

87. See, e.g., 18 U.S.C.A. § 2511(4)(a) (criminally punishing violations with fines up to \$10,000 and up to five years imprisonment); *Id.* § 2520(b)–(c) (authorizing a civil action for violations under which successful plaintiffs can obtain, in addition to attorney's fees and punitive damages, compensatory damages equal to the greater of (1) the sum of actual damages and defendant's profit as a result of the violation or (2) statutory damages equal to the greater of \$100 per day of violation or \$10,000).

88. Schwartz, *supra* note 71, at 1561–62.

89. *Id.* at 1562.

overblown. But Schwartz and Reidenberg's typology merely tells us that while some parts of a code of fair information practices regulate information flows, much of a typical code has nothing to do with information flows. Their model does not ultimately help us with the really hard question at the core of the First Amendment critique—the constitutional status of information flow regulation.⁹⁰

The critics argue that regulation of information flows is regulation of speech, and that free information flows are therefore as constitutionally mandated as free speech. What then do we make of this claim that information flow regulation is a “right to stop other people from speaking about you”?⁹¹ I believe that most privacy regulation that interrupts information flows in the context of an express or implied commercial relationship is neither “speech” within the current meaning of the First Amendment,⁹² nor should it be viewed as such.⁹³ By contrast, the handful of scholars who have previously responded to this question have tended to assume that all information flows are speech, and then disagreed about whether the First Amendment allows or prohibits various forms of privacy regulations. In so doing, these scholars have rejected the notion that at least some forms of data flows might fall outside the scope of heightened First Amendment protection.⁹⁴ But by neglecting to consider the boundaries of the First Amendment, scholars seeking to reconcile privacy regulation with the First Amendment have conceptualized the problem improperly, and thereby have missed an important opportunity to explain precisely why privacy rules are fully consonant with our traditions of robust protection for free speech.

Is it conceptually possible to treat commercial information flows as falling outside the “freedom of speech” that the First Amendment protects? That is, even if the critics are correct that the creation or sale of a database is a “communication” of information, is that communication necessarily speech that warrants heightened scrutiny under the First Amendment? Making this determination requires an assessment of the boundaries of First Amendment protection. Unfortunately, in spite of the importance of the First Amendment

90. See, e.g., Volokh, *supra* note 3, at 1054–55.

91. *Id.* at 1049.

92. See *infra* Part III.

93. See *infra* Part IV.

94. See Schwartz, *supra* note 71, at 1564; Solove, *supra* note 71, at 975–1032 (considering and rejecting this approach); Volokh, *supra* note 3, at 1080–87 (same). One notable exception is Julie Cohen, who has suggested at a theoretical level that regulation of information markets might not implicate heightened First Amendment review. Cohen, *supra* note 47, at 1417. Cohen's arguments are thoughtful, although she does not develop them in detail and notes that “[m]uch work remains to be done.” *Id.* at 1415–16. Nevertheless, my argument in this part builds undeniably upon Cohen's nuanced and sophisticated analysis.

to American legal and political culture,⁹⁵ very little has been written on the line between the “freedom of speech” protected by the First Amendment and that which is not protected. This lack of attention is even more surprising when one considers the large number of First Amendment cases decided by the Supreme Court alone over the past four decades,⁹⁶ as well as the even more voluminous bulk of First Amendment scholarship by legal and other academics.⁹⁷

The handful of scholars who have studied this issue suggest that a freedom of speech⁹⁸ challenge to a regulation requires a court to answer two questions. The first question is whether there is a First Amendment issue in the first place—whether the regulation infringes upon the “freedom of speech” that the First Amendment protects. The scholarship addressing this issue frames the question as one involving the “coverage,”⁹⁹ the “boundaries,”¹⁰⁰ the “ambit,”¹⁰¹ or most commonly the “scope”¹⁰² of the First Amendment. This question—what I will call the “scope question”—asks whether the activity in question is speech that the First Amendment protects at all.

If the answer to the scope question is “yes,” the Court must answer a second question. This question focuses on the “level”¹⁰³ of “obligation”¹⁰⁴ or strength of First Amendment “protection.”¹⁰⁵ In answering the second question, a court must determine what portion of “the full arsenal of First Amendment rules, principles, standards, distinctions, presumptions, tools, factors, and three-part tests becomes available to determine whether the particular speech will actually wind up being protected.”¹⁰⁶ I call this question the “level of protection” question.

95. See, e.g., Frederick Schauer, *First Amendment Opportunism*, in *ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA* 175 (Lee C. Bollinger & Geoffrey R. Stone eds., 2002).

96. Daniel Farber estimates that “the Supreme Court has decided well over two hundred First Amendment cases, most of them since 1970.” DANIEL A. FARBER, *THE FIRST AMENDMENT* 1–2 (2d ed. 2003).

97. One leading casebook cites 395 principal First Amendment articles in its table of authorities. GEOFFREY R. STONE ET AL., *THE FIRST AMENDMENT* 633–41 (2d ed. 2003).

98. Or indeed any issue of the applicability of a constitutional right more generally. See Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 *HARV. L. REV.* 1765, 1771 (2004).

99. *Id.* at 1769.

100. KENT GREENAWALT, *SPEECH, CRIME, AND THE USES OF LANGUAGE* 40 (1989).

101. Harry Kalven, Jr., *The Reasonable Man and the First Amendment*: Hill, Butz, and Walker, 1967 *SUP. CT. REV.* 267, 278.

102. See generally C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 *UCLA L. REV.* 964 (1978); see also Laurent B. Frantz, *The First Amendment in the Balance*, 71 *YALE L.J.* 1424, 1434–35 (1962); Martin H. Redish, *Killing the First Amendment With Kindness: A Troubled Reaction to Collins and Skover*, 68 *TEX. L. REV.* 1147, 1149–50 (1990).

103. Kalven, *supra* note 101, at 278.

104. Frantz, *supra* note 102, at 1436.

105. Schauer, *supra* note 98, at 1769. See generally *id.* at 1769 & nn.10–11 (collecting sources).

106. *Id.* at 1769.

Courts and scholars invariably focus upon the level of protection question in First Amendment analysis, with the unfortunate result that the scope question has been significantly understudied. Nevertheless, the scope question remains a critical one. The initial work done in this area by Kent Greenawalt on language, speech, and crime concluded that even though much of what the criminal law punishes is “speech” within the common dictionary or lay understanding of the term, imposing criminal punishment for speech is rarely, if ever, considered to raise First Amendment concerns.¹⁰⁷ Thus, we do not perceive the speech used to engage in fraud, to make criminal threats, to form and advance conspiracies, or to solicit criminal acts as First Amendment speech.¹⁰⁸ Punishment imposed on such speech is, both doctrinally and theoretically, not an “abridg[ement]” of the “freedom of speech.”¹⁰⁹ Frederick Schauer has expanded Greenawalt’s list beyond the criminal context, noting that the First Amendment does not apply to government regulations of speech in the contexts of securities, antitrust, labor organizing, copyrights, trademarks, sexual harassment, the regulation of doctors, lawyers, and other professionals, and vast amounts of evidence and tort law.¹¹⁰ Schauer argues that the fact that the First Amendment’s boundaries are much narrower than the ordinary understanding of the word “speech” suggests the need for further study of the concept of “constitutional salience”—“the often mysterious political, social, cultural, historical, psychological, rhetorical, and economic forces that influence which policy decisions surface as constitutional issues and which do not.”¹¹¹

Unfortunately, calling things “speech” or “not speech” and thereby placing large areas of speech beyond the scope of the First Amendment tends to make people nervous. There is, however, an alternative method of approaching the inquiry. Rather than looking at which communications are “speech” and which are “not speech,” it is possible to view the category of “unprotected” speech as something like the rational basis category that exists in other areas of rights jurisprudence, but which never has been articulated in the context of the First Amendment. Under this approach, all “speech” would be covered by the First Amendment, but the scope question could be viewed as a threshold for invoking heightened scrutiny in much the same way that

107. GREENAWALT, *supra* note 100, at 58, 79–87; Kent Greenawalt, *Criminal Coercion and Freedom of Speech*, 78 NW. U. L. REV. 1081 (1983); Kent Greenawalt, *Speech and Crime*, 1980 AM. B. FOUND. RES. J. 645.

108. See GREENAWALT, *supra* note 100, at 79–140 (collecting cases).

109. See U.S. CONST. amend. I.

110. Schauer, *supra* note 98, at 1777–84.

111. *Id.* at 1768.

suspect classification analysis performs this role in equal protection and due process jurisprudence. "Speech," in the ordinary sense of the term, that fails the scope question would receive rational basis review. For example, in Equal Protection Clause jurisprudence, a court assessing the constitutionality of a classification must compare the type of classification with the list of so-called "suspect classes." While racial classifications receive strict scrutiny and classifications made on the basis of sex receive intermediate scrutiny, classifications involving economic rights receive minimal judicial scrutiny.¹¹² Similarly, in the due process context, economic rights are assessed under rational basis review, while the existence of a "fundamental right," such as reproductive autonomy or the right to vote, increases the level of scrutiny.¹¹³

Viewed in this way, the scope and level of protection questions in First Amendment analysis would operate in a similar manner: The scope question determines whether heightened scrutiny is warranted, and if it is, the level of protection question allocates the appropriate doctrinal formulation with which to assess the constitutionality of the speech restriction. For example, regulation of the content of political speech broadcast from a loudspeaker van would be assessed under a strict scrutiny standard, while a content-neutral regulation of the noise level emanating from such a van would be assessed under intermediate scrutiny.¹¹⁴ But economic regulation of the market for loudspeakers or electrical appliances would receive rational basis review.

Critically, then, just as a classification falling outside one of the suspect categories in equal protection analysis would receive rational basis review, so too would regulations of speech falling outside the scope of the First Amendment. Speech in this category, whether we call it "unprotected speech" or "speech outside the scope of the First Amendment," is merely speech within the dictionary definition of the term that does not warrant heightened protection against government regulation. This might be the case because the speech is threatening,¹¹⁵ obscene,¹¹⁶ or libelous,¹¹⁷ and thus part of the "established" categories of "unprotected speech." But it might also be the case because

112. See ERWIN CHERMERINSKY, *CONSTITUTIONAL LAW* 474, 529–30 (2001).

113. See *id.* at 695.

114. *Kovacs v. Cooper*, 336 U.S. 77, 97 (1949) (Frankfurter, J., concurring).

115. *Virginia v. Black*, 538 U.S. 343 (2003) (holding that state bans on "true threats" are compatible with the First Amendment); see also *R.A.V. v. City of St. Paul*, 505 U.S. 377, 388 (1992) ("[T]hreats of violence are outside the First Amendment . . .").

116. *Roth v. United States*, 354 U.S. 476, 485 (1957) (holding that obscene materials are outside the scope of First Amendment protection); see also *Miller v. California*, 413 U.S. 15, 24 (1973) (establishing a three-part test for determining whether speech is obscene and therefore outside First Amendment protection).

117. *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 268 (1964) (stating that libelous speech is not protected by the Constitution but must not be used as a guise for punishing criticism).

the speech is an insider trading tip,¹¹⁸ a false statement in a proxy statement,¹¹⁹ an offer to create a monopoly in restraint of trade,¹²⁰ or a breach of the attorney-client privilege.¹²¹ In either case, the speech would be outside the scope of the First Amendment and could be regulated as long as a rational basis exists for so doing. Such an approach to First Amendment analysis is not just descriptively accurate, but is entirely defensible under current doctrine, because the freedom of speech is one of the “fundamental rights” protected by the Fourteenth Amendment’s Due Process Clause against the states.¹²²

In the specific context of privacy and speech, this approach would work in an identical fashion. Ordinary public and private law rules regulating businesses engaged in the trade in customer data would be, like other forms of commercial regulation, outside the scope of the First Amendment and thus subject to rational basis review.¹²³ Examples of such laws would include a paradigmatic code of fair information practices regulating the commercial assembly, processing, and use of large-scale consumer databases. Such regulations would constitute “laws of general applicability” under current doctrine and would not warrant heightened judicial scrutiny beyond the deferential standard applied to most economic regulations. By contrast, regulations of privacy rules that restrict protected speech or that burden conduct with a significant expressive component would fall within the scope of the First Amendment. Such regulations would thus warrant heightened judicial scrutiny. For example, regulation of speech on matters of public or general concern (such as articles in *Consumer Reports*, disclosure of newsworthy private facts about individuals, discussions of the merits of particular companies, or even some gossip about individuals) would warrant heightened (and most likely strict) scrutiny. Other forms of lesser-protected speech such as telemarketing¹²⁴ or regulation of conduct

118. *United States v. Stewart*, No. 03 CR. 717(MGC), 2004 WL 113506, at *2 (S.D.N.Y. Jan. 26, 2004) (mem.).

119. *Ohralik v. Ohio State Bar Ass’n*, 436 U.S. 447, 456 (1978) (citing *Mills v. Elec. Auto-Lite Co.*, 396 U.S. 375 (1970)).

120. *Id.* (citing *Am. Column & Lumber Co. v. United States*, 257 U.S. 377 (1921)).

121. *United States v. Longo*, 70 F. Supp. 2d 225, 264 (W.D.N.Y. 1999) (holding that the proper remedy for evidence gained as a breach of the attorney-client privilege is suppression of the evidence).

122. See CHEMERINSKY, *supra* note 112, at 695.

123. My purpose at this stage of the analysis is merely to sketch the basic conceptual framework that courts should apply in approaching the intersection of privacy and speech. In Part III of this Article, I attempt to demonstrate in greater detail how this approach is consistent with the bulk of modern free speech jurisprudence, and how ordinary doctrinal tools can be applied to demonstrate the constitutionality of most meaningful regulatory responses to the database problem. Because doctrinal rules are only as good as the policies underlying them and the consequences they produce, in Part IV, I attempt a more abstract normative defense of the jurisprudential implications of my approach.

124. See *infra* Part III.D.

with a significant expressive component (such as a law outlawing cameras)¹²⁵ would receive intermediate scrutiny under the commercial speech doctrine. But the ordinary regulation of the commercial data trade would receive only rational basis review, just as the economic regulation in our loudspeaker example would.

To be clear, I believe that this model accurately describes the way First Amendment law implicitly approaches the scope question. I also believe, however, that this approach is normatively superior to the current conceptual framework used by scholars, who too often neglect the scope question. Looking at restrictions of “speech” in terms of the scope question first can provide a way of resolving their First Amendment status without forcing them into existing doctrinal categories into which they might not fit well. Looking carefully at whether regulation of information flows and databases is really a regulation of speech within the scope of the First Amendment could thus produce a potentially satisfying doctrinal and theoretical response to the First Amendment critique, allowing us to separate the easy, nonspeech cases away from the minority of cases in which free speech and data privacy are in conflict. Such an approach has at least two additional advantages. First, by separating the regulations that threaten First Amendment values from those that do not, it is possible to have a more honest debate about the public policy implications of additional privacy protections in the database context. The benefits and pitfalls of privacy rules can thus be debated on their own merits by scholars and by legislative bodies, free from the unnecessary, distracting, and discourse-distorting effects of fundamentally spurious First Amendment arguments. Such a discussion is, as I have suggested, currently being short-circuited by constitutional objections when privacy rules are drafted and by needless First Amendment litigation after their enactment.¹²⁶ And when such litigation does arise, this approach avoids having the merits of the regulations at issue settled after judicial proceedings in which policy arguments are forced to masquerade as theories of constitutional interpretation. Second, by separating out the easy cases, we can more easily focus on providing doctrinal and theoretical solutions to the really difficult (and important) ones—cases in which the First Amendment and privacy are actually in conflict.

The First Amendment critics would, I imagine, have two responses to this approach. First, they would argue that the exceptions to the scope of the First Amendment are few, defined, and narrowly construed, covering only such established doctrinal categories as obscenity, “incitement, false

125. See *infra* notes 213–215 and accompanying text.

126. See *supra* notes 62–69 and accompanying text.

statements of fact, threats, and the like.”¹²⁷ Second, they would argue that even though new exceptions could certainly be created, doing so would create a pernicious and dangerous precedent for other, more nefarious exceptions to protected free speech in the future.¹²⁸

With respect to the first argument, I am not convinced that the critics accurately describe the universe of free speech cases. The First Amendment critics are correct that the Supreme Court has held that much of what we think of as communicative speech falls within the scope of the First Amendment, and the Court has also held a few categories to be outside the scope and thus to constitute “unprotected speech.” But the Court has never held in a blanket fashion that all communications fall within the scope of the First Amendment and are thus subject to heightened protection. Indeed, as the examples identified by Greenawalt and Schauer reveal, there are many areas of law regulating the content of speech that are not thought to be within the scope of the First Amendment as either a doctrinal or theoretical matter.¹²⁹ And as Schauer has argued in responding to an analogous claim, to take the position of the First Amendment critics

is to be afflicted with the common ailment of spending too much time with the casebooks—defining the domain of constitutional permissibility by reference to those matters that have been considered viable enough to be litigated in, and close enough to be seriously addressed by, the courts, especially the Supreme Court. But if we are interested in the speech that the First Amendment does not touch, we need to leave our casebooks and the Supreme Court’s docket behind; we must consider not only the speech that the First Amendment noticeably ignores, but also the speech that it ignores more quietly.¹³⁰

As a descriptive matter, then, the universe of speech within the scope of the First Amendment, as defined by existing case law, is significantly smaller than the universe of “speech,” as understood by the dictionary or lay definition, because the universe of “exceptions” to the Free Speech Clause is far greater than is conventionally thought.¹³¹

127. EUGENE VOLOKH, *THE FIRST AMENDMENT: PROBLEMS, CASES AND POLICY ARGUMENTS* 2 (2001).

128. See Volokh, *supra* note 3, at 1084–88.

129. See *supra* notes 107–111 and accompanying text.

130. Schauer, *supra* note 98, at 1777–78.

131. The scholarship of Eugene Volokh can be seen as trying to use existing doctrinal tools to bring these unappreciated or underappreciated contexts within the ambit of First Amendment protection. His response to my claim would presumably be “I am arguing that courts ought not ignore the First Amendment this way; when speech is being restricted based on its content, courts should explicitly explain why this restriction is permissible.” Eugene Volokh, *Speech as Conduct: Generally Applicable Laws, Illegal Courses of Conduct, “Situation-Altering Utterances,” and the Uncharted*

If the First Amendment critics are thus wrong as a descriptive or interpretive matter about the universe of speech, what about their second claim that creating “new” exceptions to existing doctrinal categories would be a bad idea? Eugene Volokh argues that the changes in jurisprudence necessary to reconcile data privacy with the First Amendment—whether by creating new data privacy exceptions to existing free speech doctrine, or expanding existing exceptions such as commercial speech doctrine—would open the door for a variety of other, more sinister speech restrictions. For example, Volokh argues that widening the exception for speech on matters of private concern would give a strong argument to those who wish to restrict other types of “private” speech that do not address matters of public concern, such as sexually themed speech ranging from “pornography to art to sexual humor.”¹³² Similarly, he suggests, broadening commercial speech doctrine to accommodate data privacy speech restrictions would stretch the doctrinal category to such a degree that many types of socially beneficial speech and commentary about economic matters would also fall into the category of regulatable commercial speech, “[g]iving the government an ill-defined but potentially very broad power to restrict such speech.”¹³³

I am not convinced by Volokh’s slippery slope argument, for three reasons. First, treating the sale of a consumer database as outside the First Amendment does not create a “new exception” to existing doctrine. To the contrary, there is very little authority assessing the constitutional status of rules of this sort, which suggests that these regulations have never been thought to raise First Amendment problems.¹³⁴ Rather than creating a “new exception” to existing doctrine, such restrictions more likely fall as a descriptive matter into what Schauer terms the “speech that [the First Amendment] ignores more quietly.”¹³⁵

Zones, 90 CORNELL L. REV. (forthcoming 2005) (manuscript at 58 n.212, on file with author); see also sources cited *infra* note 372 and accompanying text. To the extent that this is a normative argument rather than a descriptive one, I respond to it *infra* Part IV.

132. Volokh, *supra* note 3, at 1098.

133. *Id.* at 1087.

134. For example, in his dissent from the denial of certiorari in the *Trans Union* case, Justice Kennedy noted that the law was unsettled about how to characterize the sale of a targeted marketing list containing the names and addresses of consumers. *Trans Union LLC v. FTC*, 536 U.S. 915, 916 (2002) (Kennedy, J., dissenting from denial of certiorari). Justice Kennedy did seem to hint that he thought the lists were entitled to some protection, but a dissent from a denial of certiorari has no precedential value. To the contrary, Kennedy’s dissent reveals the confusion in this area of First Amendment law, as he acknowledges that the Court’s plurality opinion in *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749 (1985), is in some tension with his own views of the scope of heightened First Amendment protection.

135. Schauer, *supra* note 98, at 1778.

Second, Volokh's argument takes issue with the very process by which the Supreme Court has structured First Amendment review since at least *New York Times Co. v. Sullivan*,¹³⁶ in which it sketched the modern formulation for how state tort rules that implicate First Amendment concerns should be evaluated. Rather than engaging in the often treacherous task of balancing the values and harms of speech in particular cases, the Supreme Court in *Sullivan* articulated the theory of what scholars have called "definitional"¹³⁷ or "categorical"¹³⁸ balancing. Under this approach, the Court balances the interests involved in a class of speech and sets the level of scrutiny for all cases that fall within the class. In the context of privacy rights, just as in the context of the intersection between tort law and free speech generally, the Supreme Court has settled on a categorical balancing approach to resolve the conflict between privacy claims and free speech.¹³⁹ Volokh may disagree with this approach, but to the extent he argues that creating privacy exemptions under the First Amendment violates the First Amendment, his slippery slope argument appears either to criticize a significant portion of the same free speech jurisprudence he seeks to protect, or implicitly to propose a radical departure from that jurisprudence.

Third, Volokh's argument rests on the premise that creating new "exceptions" from the protection of the First Amendment creates "doctrinal, political, and psychological" arguments for creating other exceptions to the First Amendment by analogy, and that the creation of such exceptions is likely to occur in practice.¹⁴⁰ Although he claims that he is not making a slippery slope argument of a "today this speech restriction; tomorrow the Inquisition" sort,¹⁴¹ his argument is confessedly some form of slippery slope argument, even if it is a more nuanced one than most. In that regard, Volokh's theoretical claim is undercut significantly by the way that the Supreme

136. 376 U.S. 254 (1964).

137. Melville B. Nimmer, *The Right to Speak from Times to Time: First Amendment Theory Applied to Libel and Misapplied to Privacy*, 56 CAL. L. REV. 935, 942-43 (1968).

138. LAURENCE H. TRIBE, *AMERICAN CONSTITUTIONAL LAW* 792-93 (2d ed. 1988); David A. Anderson, *Torts, Speech, and Contracts*, 75 TEX. L. REV. 1499, 1510 (1997).

139. See, e.g., *Bartnicki v. Vopper*, 532 U.S. 514, 534 (2001) ("In this case, privacy concerns give way when balanced against the interest in publishing matters of public importance."). The Court also considers privacy (or at least the line between that which is public and that which is private) as a critical element in allocating the standard of review in defamation cases—public figures must plead and prove more elements than private figures who bring the action in order to recover for damage due to their reputations. Compare *Sullivan*, 376 U.S. at 279-80 (requiring a public figure to prove actual malice to recover for defamation), with *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 347 (1974) (requiring private figures to prove only something more than strict liability to recover damages for actual injury).

140. Volokh, *supra* note 3, at 1052.

141. *Id.*

Court has actually decided free speech cases over the past half-century. Although the Supreme Court has established several categories of speech that do not enjoy either full protection as core speech¹⁴² or any protection whatsoever,¹⁴³ these categories have tended to shrink over time, rather than to grow. For example, although the Supreme Court in the 1940s generally supported free speech rights,¹⁴⁴ it did carve out at least two categories of speech as unprotected by the First Amendment—"fighting words" and commercial speech.

Although Volokh's argument would predict that the "fighting words" doctrine established in *Chaplinsky v. New Hampshire*¹⁴⁵ would lead not only to a broadening of its own doctrinal category but also to the creation of new categories of unprotected speech, this has not happened in practice; indeed, although the Supreme Court has not reversed *Chaplinsky*, it has never subsequently upheld a conviction under the case's theory.¹⁴⁶ Thus, in *Gooding v. Wilson*,¹⁴⁷ when the Court addressed a conviction under a statute substantively identical to the one it upheld in *Chaplinsky*, it declared the statute unconstitutional under the overbreadth doctrine, even though the petitioner in that case had undeniably engaged in activity outside the First Amendment under the "fighting words" doctrine.¹⁴⁸

Similarly, although the Supreme Court held in *Valentine v. Chrestensen*¹⁴⁹ that commercial speech was unprotected speech,¹⁵⁰ subsequent

142. See, e.g., *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557, 563–64 (1980) (stating that commercial speech receives intermediate scrutiny); *United States v. O'Brien*, 391 U.S. 367, 382 (1968) (applying intermediate scrutiny to a conviction for burning a draft card).

143. See, e.g., *Virginia v. Black*, 538 U.S. 343, 359 (2003) ("[T]hreats of violence are outside the First Amendment . . ."); *R.A.V. v. City of St. Paul*, 505 U.S. 377, 388 (1992) (same); *Time, Inc. v. Hill*, 385 U.S. 374, 389–90 (1967) (libelous statements made with "calculated falsehood"); *Roth v. United States*, 354 U.S. 476, 485 (1957) (obscenity); *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942) ("fighting words").

144. See, e.g., WHITE, *supra* note 8; Tony A. Freyer, *The First Amendment and World War II*, [1996] 1 J. SUP. CT. HIST. 83; Neil M. Richards, *The "Good War," the Jehovah's Witnesses, and the First Amendment*, 87 VA. L. REV. 781, 794 (2001) (reviewing SHAWN FRANCIS PETERS, *JUDGING JEHOVAH'S WITNESSES: RELIGIOUS PERSECUTION AND THE DAWN OF THE RIGHTS REVOLUTION* (2000)).

145. 315 U.S. 568 (excluding from First Amendment protection "'fighting' words—those which by their very utterance inflict injury or tend to incite an immediate breach of the peace.>").

146. See, e.g., *Texas v. Johnson*, 491 U.S. 397, 409 (1989); *City of Houston v. Hill*, 482 U.S. 451, 462–63 (1987); *Hess v. Indiana*, 414 U.S. 105, 107 (1973); *Norwell v. City of Cincinnati*, 414 U.S. 14, 16 (1973); *Lewis v. City of New Orleans*, 408 U.S. 913 (1972); *Rosenfeld v. New Jersey*, 408 U.S. 901, 905 (1972); *Gooding v. Wilson*, 405 U.S. 518, 528 (1972); *Cohen v. California*, 403 U.S. 15, 20 (1971); *Street v. New York*, 394 U.S. 576, 592 (1969).

147. *Gooding*, 405 U.S. 518.

148. *Id.* at 528.

149. 316 U.S. 52 (1942).

150. *Id.* at 54–55; see also *Breard v. Alexandria*, 341 U.S. 622, 645 (1951) (reaffirming *Chrestensen* as applied to a prohibition against door-to-door solicitation of magazine subscriptions).

decisions have brought commercial speech within the protections of the First Amendment,¹⁵¹ with the relaxed intermediate scrutiny of *Central Hudson Gas and Electric Corp. v. Public Service Commission*¹⁵² giving way over time to greater and greater protection for commercial speech. As a result, the central issue of commercial speech doctrine has gradually but fundamentally shifted over the last twenty years from whether commercial speech should be protected at all to whether it warrants protection on a par with “core” political speech, as several members of the Court have argued.¹⁵³

It is certainly difficult to predict future events based upon trends from the past. But the robust protection that the courts have given to free speech suggests that refining categories of unprotected or partially protected speech is unlikely to lead to serious free speech problems down the road through any slippery slope mechanism. Indeed, the principal theoretical and practical difficulty at the intersection of speech and privacy is not a problem of protecting speech from privacy, but of safeguarding some privacy protection under a juridical regime in which free speech always wins.

Although most privacy scholars believe that privacy rights are not extinguished by the First Amendment, the handful of such scholars who have disagreed explicitly with the First Amendment critique would also reject an approach to the problem that focuses on the boundaries of the First Amendment. Paul Schwartz and Daniel Solove concede that information disclosure rules raise First Amendment problems, but they believe that an adjusted right of data privacy can stand up to the First Amendment. Schwartz argues that nondisclosure rules can survive balancing against the First Amendment because they “help maintain the boundary between public discourse and the other realms of communication” and because “standards of fair information practices serve to safeguard deliberative democracy by shaping the terms of individual participation in social and political life.”¹⁵⁴ Solove argues that in the context of information disclosure rules, privacy interests should be balanced against First Amendment rights. Although he considers

151. See *Va. State Bd. of Pharm. v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 770 (1976).

152. 447 U.S. 557 (1980).

153. See, e.g., *Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 367–68 (2002) (noting that “several Members of the Court have expressed doubts about the *Central Hudson* analysis and whether it should apply in particular cases” (citing *Greater New Orleans Broad. Assn. v. United States*, 527 U.S. 173, 197 (1999) (Thomas, J., concurring))); *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 501, 510–14 (1996) (Stevens, J.) (joined by Kennedy, Souter, and Ginsburg, JJ.); *id.* at 517 (Scalia, J., concurring in part and concurring in the judgment); *id.* at 518 (Thomas, J., concurring in part and concurring in the judgment); see also William Van Alstyne, *To What Extent Does the Power of Government to Determine the Boundaries and Conditions of Lawful Commerce Permit Government to Declare Who May Advertise and Who May Not?*, 51 EMORY L.J. 1513, 1545 & n.84 (2002).

154. Schwartz, *supra* note 71, at 1563–64.

it tempting to exclude disclosures of private information categorically from the definition of “speech” under the First Amendment, Solove ultimately rejects this approach as “conceptually sloppy or even dishonest absent a meaningful way to argue that these examples do not involve communication.”¹⁵⁵ According to Solove, “[d]ealing with privacy issues by categorizing personal information as nonspeech is undesirable because it cloaks the real normative reasons for why society wants to permit greater regulation of certain communicative activity.”¹⁵⁶ Solove argues that it is both preferable and more intellectually honest to engage in pragmatic, contextual balancing between speech and privacy.¹⁵⁷

Solove’s and Schwartz’s arguments are thoughtful, but I believe they grant too much ground to the First Amendment critique and ultimately may prove to be underprotective of privacy interests, particularly in the database context. First, to the extent these scholars share the same view of the boundaries of the First Amendment as the critics do, I have already addressed these objections.¹⁵⁸ Second, to the extent we disagree whether the sale of databases constitutes “speech” within the scope of the First Amendment, I argue below that under current doctrine, the sale or transfer of most commercial databases does not fall within the protections of the First Amendment.

Third, I doubt that Solove’s balancing approach would provide meaningfully increased protection for privacy protection in the courts. Solove urges courts to depart from the current paradigms under which they balance privacy against the First Amendment—whether the individual is a public or private figure and whether the information is public or private—and to replace them with an approach focusing on “the relationships in which information is transferred and the uses to which information is put.”¹⁵⁹ However, such an approach merely substitutes one vague set of criteria for another and risks an overcontextualized jurisprudence. As Solove concedes, “[i]f social norms about the propriety of disclosures are too diffuse and contestable, then a law protecting against ‘improper’ disclosures may become too unpredictable or even unworkable.”¹⁶⁰ Solove’s solution to this problem of “hyper-contextualism” is essentially the one put forth by Warren and Brandeis over 100 years ago—that courts can articulate the contours of murky rules like negligence on a

155. Solove, *supra* note 71, at 981.

156. *Id.*

157. *Id.* at 976–77.

158. See *supra* notes 127–132 and accompanying text.

159. Solove, *supra* note 71, at 1031.

160. *Id.* at 1026.

case-by-case basis.¹⁶¹ I am skeptical that Solove's contextually pragmatic proposal would work significantly better than the categorically pragmatic method applied by existing jurisprudence. Solove's approach would, I fear, lead to inconsistent results through the processes of courts applying slippery standards on a case-by-case basis. In addition, any balance between the powerful First Amendment and a nuanced right of privacy is unlikely to protect much privacy at all.

Although some form of balancing is perhaps inevitable in the hard cases pitting privacy against the First Amendment, I believe it is not only important to separate out the easy cases from the hard cases, but also that an approach that treats private information differently is more consistent with the workable "categorical balancing" approach courts have taken in the First Amendment context since *New York Times v. Sullivan*. In the next part, I show how this approach works in practice.

III. CATEGORIZING PRIVACY RULES UNDER THE FIRST AMENDMENT

The previous part attempted to complicate the argument of the First Amendment critics that privacy rules necessarily regulate speech protected by the First Amendment. Because many privacy rules have nothing to do with information flows, they have nothing to do with speech. And, as a conceptual matter, privacy rules regulating information flows are not necessarily within the scope of the First Amendment. In this part, I attempt to demonstrate more specifically why privacy rules will rarely, if ever, create a problem under the First Amendment.

Given the notorious slipperiness of the term "privacy,"¹⁶² it is necessary to impose some sort of order on the analysis that follows. Every information flow in the database context can be broken down into a series of stages, which are helpful categories to assess the different kinds of privacy rules that can apply to a transaction in personal information. Information is first collected by companies, then used to assemble databases, disclosed to companies wishing to use the information (either for marketing or for the creation of larger databases), and then often used as the basis for direct marketing, such as telemarketing or junk mail. Accordingly, possible regulations of information flows can be divided into four categories, corresponding to the four stages of information processing performed by the database industry: (1) rules governing the collection of

161. *Id.* at 1027.

162. Privacy scholars have struggled for decades to come up with a workable definition of privacy and have failed to reach a consensus. See Solove, *supra* note 10, at 1088 (collecting sources).

information, (2) rules governing the use of such information, (3) rules governing the disclosure of information, and (4) regulation of direct marketing.

This taxonomy makes, I believe, two significant contributions to the literature on information flows. First, looking at the problem in this way reveals that ordinary information collection and information use rules are not speech rules at all. Information disclosure rules are closer to speech, but in the commercial context they are usually outside the scope of the First Amendment. And while direct regulation of telemarketing is undeniably regulation of commercial speech within the scope of the First Amendment, current doctrine nevertheless permits quite extensive regulation of such speech. Second, regardless of whether individual or categorical sorts of privacy rules ultimately pass muster under the First Amendment, separating out the various types of privacy restrictions on the free flow of information allows us to take a careful look at the constitutional issues raised by four very different types of data privacy rules. In this regard, I hope that this taxonomy is a useful (and hopefully value-neutral) contribution to the discourse on information flows.

A. Information Collection Rules

Information collection rules govern the process of gathering data and assembling databases. They represent the legal regime covering the ways in which entities acquire information and specify when collection is permissible and when it is not. Examples include requiring a company to obtain a customer's permission before it makes a record of the customer's data, regulating the use of cookies to gather information on the Internet, and regulating or prohibiting the use of scanning devices to intercept telephone conversations or e-mails.

A wide variety of rules operate, directly or indirectly, to restrict access to information without raising First Amendment issues. Most fundamentally, generally applicable property and tort law prohibits information collection by separating the public sphere from the private. It is no defense to a claim of trespass for the trespasser to assert that he infringed the property rights of another to gain information. In addition to trespass, most states recognize the intrusion into seclusion tort,¹⁶³ one of the four "privacy torts" recognized

163. See *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060, 1067 (Colo. Ct. App. 1998) (noting that the "vast majority of courts in other jurisdictions" have recognized not only other types of privacy claims, but also specifically "intrusion upon seclusion" claims). Indeed, with Minnesota most recently adopting the privacy tort via the common law in 1998, see *Lake v. Wal-Mart Stores Inc.*, 582 N.W.2d 231, 235 (Minn. 1998), only North Dakota and Wyoming have never recognized a cause of action for invasion of privacy, see O'NEIL, *supra* note 57, at 77.

by William Prosser as having evolved out of Warren and Brandeis's *Right to Privacy* article.¹⁶⁴ The intrusion tort goes much further than trespass and imposes liability upon anyone "who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person."¹⁶⁵ Courts have applied this tort to mail tampering,¹⁶⁶ eavesdropping,¹⁶⁷ nonconsensual entry into homes,¹⁶⁸ sexual harassment,¹⁶⁹ repeated intimidating phone calls,¹⁷⁰ overzealous surveillance or "shadowing,"¹⁷¹ and sexual voyeurism.¹⁷² Other sorts of information collection rules regulate unfair business practices such as industrial espionage. For example, the tort of misappropriation of trade secrets "protects a person's right to keep certain information 'secret,' by providing a cause of action against anyone who misappropriates a reasonably protected secret."¹⁷³

164. See William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 388–89 (1960); Warren & Brandeis, *supra* note 4. The torts themselves, however, were as much the creation of Prosser as of Warren and Brandeis. See *infra* notes 276–287 and accompanying text.

165. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

166. E.g., *Birnbaum v. United States*, 436 F. Supp. 967, 978 (E.D.N.Y. 1977) (recognizing an invasion of privacy when the Central Intelligence Agency opened and copied plaintiff's mail).

167. E.g., *McDonald's Corp. v. Levine*, 439 N.E.2d 475, 480 (Ill. App. Ct. 1982) (stating that violations of the Illinois Eavesdropping Act of 1977 can constitute an actionable intrusion upon seclusion); *Hamberger v. Eastman*, 206 A.2d 239, 244 (N.H. 1964) (holding that placing a listening device in plaintiff's bedroom is an invasion of privacy).

168. E.g., *Ford Motor Co. v. Williams*, 132 S.E.2d 206, 211–12 (Ga. Ct. App. 1963) (establishing liability for nonconsensual entrance into plaintiff's home, even though no one was there); *Gerard v. Parish of Jefferson*, 424 So. 2d 440, 445 (La. Ct. App. 1982) ("The right to privacy includes the right to be free from unwarranted intrusion into one's own quarters.").

169. E.g., *Stevenson v. Precision Standard, Inc.*, 762 So. 2d 820, 826 (Ala. 1999) (noting that sexual harassment could rise to the level of intrusion upon seclusion if it includes "egregious inquiries into one's sex life coupled with intrusive and coercive sexual demands"); *Philips v. Smalley Maint. Servs. Inc.*, 435 So. 2d 705, 711 (Ala. 1983) (defendant's conduct was "an 'examination' into [plaintiff's] 'private concerns,' that is, improper inquiries into her personal sexual proclivities and personality"); *Pearson v. Kancilia*, 70 P.3d 594 (Colo. Ct. App. 2003).

170. E.g., *Carey v. Statewide Fin. Co.*, 223 A.2d 405, 406–07 (Conn. Cir. Ct. 1966) (holding that creditor's harassing phone calls to plaintiff's home and the hospital "is actionable as an invasion of plaintiff's right to privacy"); *Housh v. Peth*, 133 N.E.2d 340, 344 (Ohio 1956) (holding that creditors who harassed a debtor with repeated phone calls at late hours for a three-week period were liable for intrusion upon seclusion).

171. E.g., *Nader v. Gen. Motors Corp.*, 255 N.E.2d 765, 771 (N.Y. 1970) (noting that surveillance may be "so overzealous as to render it actionable"); *Galella v. Onassis*, 353 F. Supp. 196, 227–28 (S.D.N.Y. 1972) (holding that a defendant who ignored restraining orders to photograph a plaintiff and the plaintiff's family violated the invasion of privacy).

172. E.g., *Harkey v. Abate*, 346 N.W.2d 74, 76 (Mich. Ct. App. 1983) (installation of see-through panels in women's restroom). See generally RICHARD C. TURKINGTON & ANITA A. ALLEN, *PRIVACY LAW: CASES AND MATERIALS* (1999) (collecting cases).

173. *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1238 n.42 (8th Cir. 1994).

In addition to state tort law, certain forms of eavesdropping (including industrial espionage)¹⁷⁴ are also prohibited by federal law. The Electronic Communication Privacy Act (ECPA) prohibits the use of any “device” to intercept the contents of an aural conversation.¹⁷⁵ The ECPA has been held to outlaw, *inter alia*, secret tape recording of meetings,¹⁷⁶ hidden microphones,¹⁷⁷ the surreptitious eavesdropping on or recording of telephone conversations,¹⁷⁸ and the participation of telephone companies in illegal government wiretapping.¹⁷⁹ Furthermore, many states also have statutes providing analogous civil actions¹⁸⁰ that in some instances offer more protection than the ECPA.¹⁸¹

In the consumer context, information collection rules require disclosures by businesses and informed consent by consumers. These rules even outlaw commercial data gathering that is unfair or unconscionable. For example, fraud law generally governs the receipt of any thing of value (including personal

174. The Supreme Court has noted that the need to protect information from industrial espionage is one of the core interests that the federal Wiretap Act was enacted to address. *Bartnicki v. Vopper*, 532 U.S. 514, 530 n.16 (2001).

175. 18 U.S.C.A. § 2511 (West 2000 & Supp. 2004).

176. *Earley v. Executive Bd. of the United Transp. Union*, 957 F. Supp. 997 (N.D. Ohio 1996) (surreptitious tape recording of arbitration panel).

177. *Cross v. Ala. State Dep't of Mental Health & Mental Retardation*, 49 F.3d 1490 (11th Cir. 1995).

178. *Glazner v. Glazner*, 347 F.3d 1212, 1221 (11th Cir. 2003) (recording wife's telephone conversations without her consent); *United States v. Dossey*, 66 Fed. Appx. 528, 531 (6th Cir. 2003) (hidden recording device attached to commercial establishment's telephones); *Bess v. Bess*, 929 F.2d 1332, 1336 (8th Cir. 1991) (tape recording wife's telephone conversations); *Dunn v. Blue Ridge Tel. Co.*, 868 F.2d 1578, 1582–83 (11th Cir. 1989) (employer monitoring telephone call); *Epps v. St. Mary's Hosp. of Athens*, 802 F.2d 412 (11th Cir. 1986) (fellow employee monitoring telephone call); *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983) (employer monitoring telephone call); *Goodspeed v. Harman*, 39 F. Supp. 2d 787, 792–94 (N.D. Tex. 1999) (intentional eavesdropping on neighbor's cordless telephone calls using a police scanner); *In re State Police Litig.*, 888 F. Supp. 1235 (D. Conn. 1995) (recordings of telephone conversations made by police commission, which did not listen to them); *George v. Carusone*, 849 F. Supp. 159, 164 (D. Conn. 1994) (same); *Pascale v. Carolina Freight Carrier Corp.*, 898 F. Supp. 276, 282 (D.N.J. 1995) (employer's workplace recording of employees' telephone conversations with wives); *Biton v. Menda*, 812 F. Supp. 283, 283 (D.P.R. 1993) (nonconsensual recording of telephone conversation with stockbroker).

179. *Jacobson v. Rose*, 592 F.2d 515 (9th Cir. 1978).

180. *E.g.*, CAL. PENAL CODE § 631 (West 1999); FLA. STAT. ANN. § 934.10 (West 2001); MASS. ANN. LAWS ch. 272, § 99Q (Law. Co-op. 2004); MINN. STAT. ANN. §§ 626A.13, 626A.32 (West 2003); N.Y. PENAL LAW § 250 (McKinney 2000); WASH. REV. CODE ANN. § 9.73.060 (West 2003).

181. The Massachusetts wiretapping statute, MASS. ANN. LAWS ch. 272, § 99, has been held more restrictive than ECPA and, thus, not subject to preemption by the federal law. *United States v. Smith*, 726 F.2d 852, 862 (1st Cir. 1984); *accord* MINN. STAT. ANN. §§ 626A.13, 626A.32 (unlike ECPA, provides civil remedy for violations involving intrastate communications).

data) under false pretenses.¹⁸² The use of fraud or other deceptive practices in obtaining consumer data could also constitute a violation of the Uniform Deceptive Trade Practices Act (UDTPA),¹⁸³ and would fall within the powers of the Federal Trade Commission (FTC) to deter and punish unfair trade practices under section five of the Federal Trade Commission Act.¹⁸⁴ Another important federal consumer protection law, the Fair Credit Reporting Act, regulates the assembly of credit reports, allowing, for example, employers to obtain credit reports for “employment purposes” only if the employee or potential employee first authorizes the collection in writing.¹⁸⁵

A variety of federal laws regulate information collection in the electronic context. Anti-hacking laws such as the Computer Fraud and Abuse Act (CFAA) impose criminal penalties on hackers by essentially exporting trespass law to the electronic world. For example, the CFAA imposes criminal punishment on anyone who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.”¹⁸⁶ Federal wiretapping law, of which the ECPA is a significant part, also proscribes the intentional interception of the contents of an electronic communication such as an e-mail or telephone conversation,¹⁸⁷ without the consent of one of the parties to the communication,¹⁸⁸ and punishes a violation through both criminal¹⁸⁹ and tort law remedies.¹⁹⁰ The Children’s Online Privacy Protection Act regulates the collection of information from children by web sites, imposing notice and express parental consent requirements.¹⁹¹

182. See E. ALLAN FARNSWORTH, *CONTRACTS* § 4.28 (3d ed. 1999); see also *RESTATEMENT (SECOND) OF CONTRACTS* §§ 159–173 (1981) (discussing elements of fraudulent misrepresentations); *RESTATEMENT (SECOND) OF TORTS* §§ 525–548A (1977) (same).

183. See *Minnesota ex rel. Hatch v. Fleet Mortgage Corp.*, 158 F. Supp. 2d 962, 966–68 (D. Minn. 2001) (holding that a bank’s failure to disclose to customers that it planned to share customer information with telemarketers stated a claim under the UDTPA and state fraud law).

184. Federal Trade Comm’n Act § 5, 15 U.S.C. § 45 (2000). The FTC has indicated that it understands the Act to grant it such authority and has brought actions pursuant to this authority. See, e.g., *Gateway Learning Corp.*, No. C-4120 (FTC Sept. 10, 2004), available at <http://www.ftc.gov/os/caselist/0423047/0423047.htm>.

185. 15 U.S.C.A. § 1681b(b) (West 1997 & Supp. 2004). See generally SOLOVE & ROTENBERG, *supra* note 82, at 520–21.

186. 18 U.S.C.A. § 1030(a)(2)(C) (West 2000 & Supp. 2004).

187. *Id.* §§ 2510(4), 2511(1)(a).

188. *Id.* § 2511(2)(d).

189. *Id.* § 2511(4)(a) (authorizing imprisonment for up to five years for violations).

190. *Id.* § 2520(c)(2). Successful plaintiffs can obtain damages equal to the greater of (1) the sum of the actual damages and the defendant’s profit as a result of the violation or (2) statutory damages equal to the greater of \$100 per day of violation or \$10,000. *Id.*

191. 15 U.S.C. §§ 6501–6506 (2000).

Finally, to the extent that web sites make representations about their information collection practices in their privacy policies, the FTC reviews these policies under its unfair trade practice jurisdiction.¹⁹² One could imagine an expansion of FTC jurisdiction not only to require privacy policies, but also to dictate the substantive content of the trade practices that these policies address.¹⁹³ Similarly, as part of regulating the commercial relationship between customers and businesses, the law could require that businesses disclose their privacy policies with respect to the subsequent uses and disclosures of data they collect. It would be difficult to argue that regulating the commercial relationship in this manner implicates the First Amendment, even though one could imagine the disclosures as a kind of forced or compelled speech. Moreover, no one considers Securities Exchange Commission or Truth in Lending Act (TILA) disclosures or Food and Drug Administration labeling requirements to raise serious First Amendment issues.

My purpose in this discussion of information collection rules has not been to attempt to catalog them systematically, but rather to suggest their ubiquity. Information collection rules are a common feature of both common and statutory law. Unsurprisingly, these rules do not fall within the scope of the First Amendment under either current First Amendment doctrine or theory. These rules are of "general applicability," neither discriminating against nor significantly impacting the freedoms guaranteed by the First Amendment.¹⁹⁴ The paradigmatic case of a generally applicable law is the private property right against trespass, which does not implicate the First Amendment under well-established doctrine. Thus, in a line of cases involving protests in shopping centers, the Supreme Court has concluded that the First Amendment "has no part to play"¹⁹⁵

192. For example, in 1998 the FTC filed a complaint against a company called GeoCities after it "misrepresented the purposes for which it was collecting personal identifying information from children and adults." GeoCities and the FTC agreed to settle later that year. See Press Release, Fed. Trade Comm'n, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case: Commission Establishes Strong Mechanisms for Protecting Consumers' Privacy Online (Aug. 13, 1998), available at <http://www.ftc.gov/opa/1998/08/geocities.htm>. Although the settlement has been criticized by scholars for being little more than a slap on the wrist, see, e.g., Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1637-38 (1999), the larger point is that information collection regulation of this sort is already within the purview of the FTC and is not considered to be constitutionally infirm. More recently, the FTC has brought charges against a company called Gateway Learning Corporation for allegedly renting out customer information collected from its web site to direct marketers, despite promises to the contrary in its privacy policy. Gateway Learning Corp., No. C-4120 (FTC Sept. 10, 2004), available at <http://www.ftc.gov/os/caselist/0423047/0423047.htm>.

193. See Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046-47 (2000).

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

195. *Hudgens v. NLRB*, 424 U.S. 507, 521 (1976).

in the general application of trespass law to protestors, because private landowners may, unlike the government, exclude speakers from their property for any reason, including their disagreement with the content of the speaker's message.¹⁹⁶

In at least two cases, however, rules governing information collection might be thought to cross into territory patrolled by the First Amendment. First, reporters engaged in newsgathering (a form of information collection) have argued that they have a First Amendment right under the Free Press Clause of the First Amendment to do so. This issue has been particularly salient of late in cases in which undercover investigative journalists have allegedly committed torts in their pursuit of a story.¹⁹⁷ Although mindful of the importance of a free and vigorous press corps, courts have declined to grant the press an immunity from lawbreaking in pursuit of a story, even a newsworthy one.¹⁹⁸ For example, in the high-profile *Food Lion, Inc. v. Capital Cities/ABC, Inc.*,¹⁹⁹ the Fourth Circuit held that investigative journalists who obtained jobs at a grocery store under false pretenses in order to videotape and publish suspected sanitary abuses trespassed and violated the duty of loyalty under state law.²⁰⁰ Although the law is unclear with respect to whether fraudulently induced consent to enter onto land is valid,²⁰¹ and although the press may get the benefit of the doubt at the margins,²⁰² no case recognizes a First Amendment investigative privilege that provides immunity from generally applicable property and tort rules like trespass.²⁰³

196. See *id.*; see also *Cent. Hardware Co. v. NLRB*, 407 U.S. 539, 547 (1972); *Lloyd Corp. v. Tanner*, 407 U.S. 551, 568 (1972). One exception to this rule, not implicated in the database context, is that the First Amendment does apply to speech restrictions imposed by private actors who have assumed the performance of substantial government functions—for example by operating a “company town.” *Hudgens*, 424 U.S. at 514–21; *Marsh v. Alabama*, 326 U.S. 501, 509 (1946).

197. See O'NEIL, *supra* note 57, at 76–90; see also *id.* at 176–78 (collecting cases).

198. See, e.g., *Galella v. Onassis*, 487 F.2d 986, 995 (2d Cir. 1973) (denying paparazzi First Amendment immunity from liability if they go “beyond the reasonable bounds of news gathering”); *Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971) (noting that the First Amendment provides the news media no license to trespass or intrude into the dwelling of another); *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 477, 493 (Cal. 1998) (finding no First Amendment immunity from tort liability for media attempting to gather material for a potentially newsworthy story); *Miller v. Nat'l Broad. Co.*, 232 Cal. Rptr. 668, 684 (Ct. App. 1986) (same); *Prahl v. Brosamle*, 295 N.W.2d 768, 781 (Wis. Ct. App. 1980) (finding no First Amendment privilege to trespass).

199. 194 F.3d 505 (4th Cir. 1999).

200. *Id.* at 510.

201. See *id.* at 517 (collecting cases).

202. *Id.* at 517–18.

203. Thus, in *Food Lion*, although the panel divided on whether the elements of the various state law torts had been met, compare *id.* at 519–20, with *id.* at 524 (Niemeyer, J., concurring in part and dissenting in part), the panel was unanimous in rejecting the media defendants' argument that the First Amendment created a press privilege to commit torts in the process of newsgathering, *id.* at 520–22; *id.* at 524 (Niemeyer, J., concurring in part and dissenting in part).

The Supreme Court's First Amendment jurisprudence makes clear that even media defendants collecting newsworthy information enjoy no privilege against the application of ordinary private law. Indeed, such rules do not trigger the application of heightened First Amendment scrutiny unless they single the press out for special unfavorable treatment.²⁰⁴ The Court recognized this principle in *Branzburg v. Hayes*,²⁰⁵ when it noted:

It would be frivolous to assert . . . that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws. Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news.²⁰⁶

Similarly, in *Cohen v. Cowles Media*,²⁰⁷ the Court held that “[t]he press may not with impunity break and enter an office or dwelling to gather news.”²⁰⁸ The Court reaffirmed this principle most recently in *Bartnicki v. Vopper*,²⁰⁹ expressly quoting its validation in *Branzburg* of generally applicable information collection rules.²¹⁰

The Court's public law cases imply a similar reasoning. In the Pentagon Papers case, some members of the Court suggested that although the prior restraint doctrine prevented the government from halting the publication of the secret report, the case might have been different had the reporters come before the Court on criminal charges for illegally acquiring classified government documents.²¹¹ Similarly, in *Wilson v. Layne*,²¹² the Supreme Court held that police who brought newspaper reporters into a private home during a search pursuant to a valid warrant nevertheless violated the Fourth Amendment. The newsmen were in effect trespassers, and their media status was deemed

204. If a law singles out the press for special, unfavorable treatment, it is likely to be invalidated. See, e.g., *Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue*, 460 U.S. 575, 592–93 (1983) (holding that a special use tax on ink and paper levied only against periodic publications violates the First Amendment).

205. 408 U.S. 665 (1972).

206. *Id.* at 691; see also *Konigsberg v. State Bar of Cal.*, 366 U.S. 36, 50–51 (1961) (“[G]eneral regulatory statutes, not intended to control the content of speech but incidentally limiting its unfettered exercise, have not been regarded as the type of law the First or Fourteenth Amendment forbade Congress or the States to pass, when they have been found justified by subordinating valid governmental interests . . .”).

207. 501 U.S. 663 (1991).

208. *Id.* at 669.

209. 532 U.S. 514 (2001).

210. *Id.* at 532 n.19.

211. *N.Y. Times Co. v. United States*, 403 U.S. 713, 730 (1971) (White, J., concurring) (stating that several criminal laws protecting government property and preserving government secrets, although not before the court, “are of very colorable relevance to the apparent circumstances of these cases”).

212. 526 U.S. 603 (1999).

irrelevant to the illegal nature of their presence. These cases embody the principle that ordinary information collection rules create no constitutional problems, even as applied to the press, as such rules form the background against which private action plays out. They also demonstrate that there are few, if any, problems with drawing lines in this context between activity that falls within the scope of the First Amendment (for example, publishing a newspaper) and activity that does not (for example, trespass, even for the purposes of gathering information).

Second, even neutral rules regulating conduct such as information collection fall within the scope of the First Amendment when they have a substantial effect upon "conduct with a significant expressive element."²¹³ In such cases, the Court applies intermediate scrutiny consistent with its content-neutral speech restrictions jurisprudence.²¹⁴ One can imagine science fiction-style hypotheticals that would bring information collection rules within this doctrine—for example, a law forbidding the keeping of records or outlawing cameras. But such laws would probably violate the First Amendment under the overbreadth and vagueness doctrines as well, or might even fail rational basis review without calling into question the undeniable constitutionality of ordinary information collection rules.²¹⁵

The larger point to be drawn from these counterexamples is not that ordinary information collection rules raise First Amendment issues. To the contrary, even reporters have had a difficult time asserting a First Amendment privilege against neutral information collection rules.²¹⁶ Information collection by nonmedia entities raises even fewer First Amendment concerns than does newsgathering by the press. And if there are essentially no First Amendment problems with subjecting the press to the basic principles of generally applicable laws, privacy rules regulating data collection by nonmedia entities fall outside the scope of the First Amendment as well. Thus, because reporters cannot claim a First Amendment privilege to gather information in

213. *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706 (1986).

214. See generally *Arcara*, 478 U.S. 697. See also *City of Ladue v. Gilleo*, 512 U.S. 43, 54–55 (1994) (holding that an ordinance prohibiting residents from installing yard signs warrants heightened First Amendment review because it closed off an entire important medium for expression); *United States v. O'Brien*, 391 U.S. 367, 382 (1968) (applying intermediate scrutiny to a conviction for burning a draft card because of the potential impact of application of the conduct rule to important political expression).

215. See Rodney A. Smolla, *Privacy and the First Amendment Right to Gather News*, 67 GEO. WASH. L. REV. 1097, 1128 (1999).

216. Cf. *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 520 (4th Cir. 1999) (noting that application of ordinary private law rules to newsgathering does not violate the First Amendment, even though newsgathering by the media is a protected activity under the Press Clause of the First Amendment).

disregard of tort and property law, it is difficult to envision businesses mounting a colorable free press challenge to consumer-protective privacy rules regulating commercial data transactions. This is particularly true for rules that regulate the commercial relationship between consumers and businesses. In sum, because there are no First Amendment problems with using generally applicable property and tort law to separate the private sphere from the public sphere, the First Amendment critique is simply inapplicable to information collection rules.

B. Information Use Rules

The second category of information flow regulations are restrictions on information use placed on recipients of data. Information use is an analytically distinct activity from information collection, but it is similarly unproblematic from a First Amendment perspective. Information use rules regulate the ways in which data about individuals can be processed, applied, or otherwise used by a person or organization. This category of rules does not include the transfer, sale, or disclosure of the data to third parties.²¹⁷ Information use rules that are relevant to the data privacy debate include the so-called “secondary use prohibition”: the requirement that data collected for one purpose may be used for that purpose only, absent consent.²¹⁸ For example, the secondary use prohibition might operate to bar an Internet Service Provider from using the fact that a person visits political fringe or sex-oriented web sites from using that information to send them personalized advertisements. Alternatively, a use rule might prevent a private business that collects my personal information as part of a transaction from including that information in a customer marketing database.²¹⁹ Other sorts of information use rules include a prohibition on the use of social security numbers to organize, combine, assemble, and process consumer data profiles more easily.²²⁰

As with information collection rules, information use rules permeate the common law and statute books of all jurisdictions.²²¹ For example, professional ethics rules prohibit lawyers from using client information for any purpose

217. I discuss information disclosure rules *infra* Part III.C.

218. See Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1294–1314 (2002).

219. See generally Swire, *supra* note 218.

220. Concern about the improper use of social security numbers dates back at least to the 1973 Department of Health, Education, and Welfare report. U.S. DEPT OF HEALTH, EDUC. & WELFARE, *supra* note 76.

221. See, e.g., MASS. ANN. LAWS ch. 175I, § 13 (Law. Co-op. 1996) (regulating the use of confidential information in insurance transactions).

unrelated to the client's interests.²²² It is also a violation of numerous federal and state antidiscrimination laws to use the fact that a person is a member of a protected class to deny them equal treatment, or to take any one of a variety of other actions.²²³ Similarly, the federal Fair Credit Reporting Act places a wide variety of restrictions on the use of consumer data contained in credit reports, including limiting uses to an enumerated list, including credit review, insurance underwriting, and employment purposes.²²⁴ Employers using credit reports for employment purposes are also prohibited by the Act from any use inconsistent with applicable equal opportunity employment rules.²²⁵ Trade secret law prohibits the use or disclosure of another's trade secrets.²²⁶ Similarly, federal patent law prohibits the use of information contained in someone else's patent to build the invention described in that patent.²²⁷ States place use conditions on social security numbers²²⁸ and information obtained from their motor vehicle records,²²⁹ while federal law places similar use restrictions on census data.²³⁰

222. The current *Model Rules of Professional Conduct* impose both a duty of confidentiality and a duty not to use information, which varies depending on whether the client is a "prospective client," current client, or former client. MODEL RULES OF PROF'L CONDUCT R. 1.18 (2003) (prospective clients); R. 1.6, 1.8(b) (current clients); R. 1.9(c) (former clients).

223. See, e.g., Civil Rights Act of 1964, tit. VII, 42 U.S.C. § 2000e-2(a) (2000) ("It shall be an unlawful employment practice for an employer—(1) to fail or refuse to hire or discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin . . ."); *id.* tit. IX, 20 U.S.C. § 1681(a) (2000) ("No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving Federal financial assistance . . ."); Americans With Disabilities Act, 42 U.S.C. § 12112(a) ("No covered entity shall discriminate against a qualified individual with a disability because of the disability of such individual in regard to job application procedures, the hiring, advancement, or discharge of employees, employee compensation, job training, and other terms, conditions, and privileges of employment."); see also Age Discrimination in Employment Act, 29 U.S.C. § 623 (2000) ("It shall be unlawful for an employer—(1) to fail or refuse to hire or to discharge any individual or otherwise discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's age . . .").

224. 15 U.S.C.A. § 1681b(a)(3) (West 1997 & Supp. 2004).

225. *Id.* § 1681b(b). See generally SOLOVE & ROTENBERG, *supra* note 82, at 520–21.

226. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995) ("A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.").

227. 35 U.S.C. § 271(a) (2000); see also *Neff Instrument Corp. v. Cohu Elecs., Inc.*, 269 F.2d 668, 673 (9th Cir. 1959) (holding the bare manufacture of a single device protected by a patent is infringement, even if device is never used or sold).

228. See, e.g., CAL. CIV. CODE § 1798.85(a)(3) (West Supp 2005) (prohibiting the use of social security numbers in unsecure internet transmissions).

229. See, e.g., OHIO REV. CODE ANN. § 4501.27(A) (West 1999 & Supp. 2004) (regulating the use of personal information "obtained in connection with a motor vehicle record").

230. See, e.g., 13 U.S.C. § 8(c) (2000) (barring use of census information "to the detriment of any respondent").

The Electronic Communications Privacy Act also imposes a use restriction on information that is obtained in violation of its information collection prohibition on intercepting the contents of electronic, wire, or aural communications.²³¹ ECPA's information use prohibition has been upheld in a variety of contexts involving different uses of information, including the use of intercepted communications from a commercial rival, *inter alia*, to create a competing product,²³² to read a document or listen to a recording obtained as a result of illegal interception,²³³ to invest in securities,²³⁴ to take adverse employment actions against employees or subordinates,²³⁵ to use in family or criminal court proceedings,²³⁶ to use in criminal or administrative investigations,²³⁷ and possibly to use as the basis for blackmail.²³⁸

Information use rules, just like information collection rules, are generally held to be outside the scope of the First Amendment under current doctrine. In *Bartnicki v. Vopper*, the Supreme Court assessed the First Amendment implications of the Wiretap Act's prohibition of the use or disclosure of intercepted communications.²³⁹ The Court drew a sharp distinction between the use of a communication under § 2511(1)(c) of the Act and its disclosure under § 2511(1)(d), reasoning that while disclosures of information could certainly constitute speech, "the prohibition against the 'use' of the contents of an illegal interception in § 2511(1)(d) . . . [is] a regulation of conduct."²⁴⁰ As a content-neutral regulation of conduct, ECPA's information use rule would fall outside the scope of the First Amendment unless, like the information collection rules discussed above, it had a substantial effect upon expressive activity. As the Court strongly implied in *Bartnicki*, virtually all of the activities that prior cases have held to constitute a "use" of intercepted information

231. 18 U.S.C.A. § 2511(1)(c) (West 2000 & Supp. 2004).

232. S. REP. NO. 90-1097, at 67 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154; *see also* *Bartnicki v. Vopper*, 532 U.S. 514, 526-27 & 527 n.10 (2001).

233. *Thompson v. Dulaney*, 838 F. Supp. 1535, 1547 (D. Utah 1993) (holding such activities to constitute a violation of ECPA separate from the interception itself).

234. *See Bartnicki*, 532 U.S. at 527 n.10 (citing Brief for United States at 24).

235. *Dorris v. Absher*, 959 F. Supp. 813, 815-16, 819 (M.D. Tenn. 1997).

236. *Bess v. Bess*, 929 F.2d 1332, 1334 (8th Cir. 1991).

237. *Berry v. Funk*, 146 F.3d 1003, 1011-13 (D.C. Cir. 1998) (knowing use of unlawfully intercepted communications by Inspector General in investigations); *Chandler v. United States Army*, 125 F.3d 1296, 1298-1302 (9th Cir. 1997) (use by military of taped conversation in adultery investigation); *In re Grand Jury*, 111 F.3d 1066, 1068, 1075 (3d Cir. 1997) (disclosure of an illegally recorded conversation to grand jury, even where such disclosure would be in compliance with subpoena).

238. *See Fultz v. Gilliam*, 942 F.2d 396, 400 n.4 (6th Cir. 1991) (envisioning extortory use of intercepted communications as violating ECPA).

239. 532 U.S. 514, 524-27 (2001); *see also* 18 U.S.C. § 2511(1)(c) (2000) (disclosure); § 2511(1)(d) (use).

240. *Bartnicki*, 532 U.S. at 526-27 (footnote omitted).

therefore would be constitutionally unproblematic.²⁴¹ I discuss the disclosure issue (and *Bartnicki*) in Part II.D, but for present purposes, it is important to note the Court's clear distinction between regulating the use of information—nonspeech conduct largely outside the scope of the First Amendment—and regulating the disclosure of information that in some circumstances (like the radio broadcast at issue in *Bartnicki*) may regulate speech.

The issue of whether an information use rule violated the First Amendment was assessed peripherally in *U.S. West, Inc. v. FCC*, in which the telephone companies sought to use customer information they had received for one purpose (providing phone service) for an unrelated purpose (marketing). Laurence Tribe argued on the telephone companies' behalf that their processing of personal data was speech entitled to full First Amendment protection.²⁴² The Tenth Circuit accepted this version of the First Amendment critique and partially agreed. Perhaps unwilling to deal with Tribe's somewhat befuddled argument that the use and processing of data within a company was speech entitled to *greater* protection than commercial speech, the court concluded that the regulations as a whole placed a restriction on U.S. West's "targeted speech to its customers . . . for the purpose of soliciting those customers to purchase more or different telecommunications services."²⁴³ U.S. West's commercial speech rights were therefore unduly burdened.²⁴⁴ The use of the information, the court asserted, was "integral to and inseparable from" the commercial solicitation.²⁴⁵ Applying the *Central Hudson* test for commercial speech restrictions, the court thus invalidated the regulation by determining that the opt-in requirement did not directly and materially advance the state interest in protecting consumer privacy,²⁴⁶ and that the regulation was not narrowly tailored because it failed to consider an available, less-restrictive alternative.²⁴⁷

241. *Id.* at 526–27 & 527 n.10 (citing favorably a long list of such examples proffered by the Solicitor General); see also *id.* at 529. The case states:

The government identifies two interests served by the statute—first, the interest in removing an incentive for parties to intercept private conversations, and second, the interest in minimizing the harm to persons whose conversations have been illegally intercepted. We assume that those interests adequately justify the [use] prohibition in § 2511(1)(d) against the interceptor's own use of information that he or she acquired by violating § 2511(1)(a)

Id.

242. See Brief of Appellant U.S. West, Inc. at 6, *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (No. 98-3451).

243. *U.S. West*, 182 F.3d at 1232.

244. *Id.* at 1232–33.

245. *Id.* at 1233 n.4.

246. *Id.* at 1237–38.

247. *Id.* at 1238–39.

The court also questioned, without deciding, whether a vague interest in protecting consumers from the embarrassment of the disclosure of their data amounted to a substantial government interest.²⁴⁸

The Tenth Circuit's reasoning appears wrong under existing law. The FCC rules allowed the telephone companies to advertise to all of their customers, prohibiting them only from using the information to target the advertisements without approval. The rules were thus an ordinary example of a secondary use prohibition that is common to codes of fair information practices, none of which have been held to violate the First Amendment.²⁴⁹ The only relevant burden placed on the telephone companies was on their ability to use, absent advance customer approval, the information they collected from those customers in the course of their commercial relationship to "target" advertisements to them—that is, to select those most likely to be receptive to such advertisements.²⁵⁰ The rules were thus not a regulation of speech at all, but rather a regulation of information use—the business activity of deciding to whom to market products. The only burden placed upon the telephone companies was that their advertisements had to be sent to all of their customers, thus making those advertisements less cost-effective. Conduct (and economic conduct at that) was thus all that was regulated, and the Supreme Court has made clear that conduct can be regulated without implicating the First Amendment. The *U.S. West* example is thus but another instance of the First Amendment critique persuading courts to ask the wrong questions about the First Amendment—that is, to skip the scope question and ignore whether the activity being regulated is really speech within the scope of the First Amendment.

In sum, under established precedent, the conduct of using information, like the conduct of gathering information, can be regulated through generally applicable laws without implicating the First Amendment in most cases, because information use rules generally regulate nonexpressive conduct rather than speech.

C. Information Disclosure Rules

The third category of information restrictions implicated by fair information practices are restrictions on the disclosure of personal information.

248. *Id.* at 1235–36.

249. See Swire, *supra* note 218, at 1293–1314.

250. 16 C.F.R. § 310.4(b)(1)(iii)(B) (2004) (defining "an abusive telemarketing act or practice" as a "telephone call to a person when . . . that person's telephone number is on the 'do-not-call' registry, maintained by the Commission, of persons who do not wish to receive outbound telephone calls to induce the purchase of goods or services").

Information disclosure rules regulate the ability of persons in possession of information to communicate, sell, or otherwise transfer that information to others. Information disclosure rules can take a variety of forms, including evidentiary privileges, Warren and Brandeis's tort of disclosure of private facts, video rental privacy protection, and duties of confidentiality and nondisclosure placed upon lawyers and financial advisers.

American law is replete with legal obligations placed on one person not to disclose information about another. While parties are of course generally free to create contracts that regulate their ability to disclose information,²⁵¹ public and private law regimes impose numerous mandatory duties of confidentiality that go beyond the contract of the transacting parties to prevent the disclosure of information through speech or other means. For example, doctors,²⁵² lawyers,²⁵³ and other professionals owe their clients duties of confidentiality, and can be punished through administrative and tort law remedies if they breach these duties by telling confidences to third parties. These duties of nondisclosure are buttressed by analogous evidentiary privileges, which give clients the ability to prevent their lawyers²⁵⁴ and doctors²⁵⁵ from speaking against their interests, presumably even when the content of the testimony would be quite newsworthy. Evidence law goes further and grants testimonial privileges to present and former spouses,²⁵⁶ psychotherapists,²⁵⁷ and others.²⁵⁸

In the commercial context as well, many legal rules impose duties of nondisclosure or confidentiality. For example, agency law imposes a general

251. See, e.g., Volokh, *supra* note 3, at 1057.

252. See AM. MED. ASS'N, CODE OF MEDICAL ETHICS § 5.05 (1999) ("The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law.").

253. See *supra* note 222 and accompanying text.

254. See, e.g., *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) ("The attorney-client privilege is the oldest of the privileges for confidential communication known to the common law."); see also CAL. EVID. CODE § 954 (West 1995) (codifying attorney-client privilege); N.Y. C.P.L.R. 4503 (McKinney 1992 & Supp. 2004) (same).

255. See, e.g., CAL. EVID. CODE § 994 (codifying doctor-patient privilege); N.Y. C.P.L.R. 4504 (same); WIS. STAT. ANN. § 905.04 (West 2000 & Supp. 2003) (same).

256. See GRAHAM C. LILLY, AN INTRODUCTION TO THE LAW OF EVIDENCE 442-51 (3d ed. 1996).

257. *Jaffee v. Redmond*, 518 U.S. 1, 15-17 (1996) (recognizing psychotherapist-patient privilege with licensed psychologists, psychiatrists, and "licensed social workers in the course of psychotherapy"); see also CAL. EVID. CODE § 1014 (West 1995 & Supp. 2005) (codifying psychotherapist-patient privilege); FLA. STAT. ANN. § 90.503 (West 1999 & Supp. 2005) (same); MASS. ANN. LAWS ch. 233, § 20B (Law. Co-op. 2004) (same).

258. Some states recognize a priest-penitent privilege. See, e.g., CAL. EVID. CODE § 1033-1034; IND. CODE ANN. § 34-46-3-1 (Michie 1998); MASS. ANN. LAWS ch. 233, § 20A (Law. Co-op. 2000). Others recognize an accountant-client privilege. See, e.g., FLA. STAT. ANN. § 473.316 (West 2001); GA. CODE ANN. § 43-3-32 (2002); 225 ILL. COMP. STAT. ANN. 450/27 (West 1993).

duty of confidentiality upon agents not to disclose their principal's information.²⁵⁹ State trade secret law enforces a mandatory regime of nondisclosure that prohibits, *inter alia*, the disclosure of trade secrets to competitors.²⁶⁰ Furthermore, some states place nondisclosure rules on social security numbers.²⁶¹

Federal statutory law imposes numerous duties of confidentiality under the federal commerce power. The federal Economic Espionage Act also prohibits the disclosure, sale, or receipt of trade secrets, and punishes individual violations with up to fifteen years imprisonment and institutional violations with fines of up to \$10 million.²⁶² Federal securities, antitrust, and labor law impose numerous duties of nondisclosure of truthful information upon corporations.²⁶³ Recent federal statutes place nondisclosure obligations upon banks with respect to customer information,²⁶⁴ and upon hospitals with respect to patient medical information.²⁶⁵ Federal law also imposes duties of confidentiality upon cable companies and video stores, charging them with keeping confidential the videos watched by their customers.²⁶⁶ ECPA provides that the disclosure of an intercepted communication is a separate violation from the interception and use of that communication.²⁶⁷ Another provision of federal wiretapping law places a duty of confidentiality upon Internet Service Providers with respect to the content of e-mails sent and received by their customers.²⁶⁸

Most commercial nondisclosure or confidentiality rules have never been thought to fall within the scope of the First Amendment's protection. Like other commercial regulations, these rules are properly assessed under rational

259. See RESTATEMENT (SECOND) OF AGENCY § 395 (1958) ("Unless otherwise agreed, an agent is subject to a duty to the principal not to use or to communicate information confidentially given him by the principal or acquired by him during the course of or on account of his agency or in violation of his duties as agent . . .").

260. See *supra* note 226.

261. For example, California prohibits any person from "publicly post[ing] or publicly display[ing] in any manner an individual's social security number." CAL. CIV. CODE § 1798.85(a)(1) (West Supp 2005).

262. 18 U.S.C. §§ 1831–1832 (2000).

263. E.g., SEC Regulation FD, 17 C.F.R. § 243.100 (2004) (preventing the selective disclosure of "material nonpublic information" by issuers of securities to selected securities traders rather than to the public as a whole); see also Schauer, *supra* note 98, at 1778–83 (collecting other examples).

264. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2000).

265. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C.); see also Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 164.500–534.

266. Video Privacy Protection Act, 18 U.S.C.A. § 2710–2711 (West 2000 & Supp. 2004); Cable Communications Policy Act, 47 U.S.C.A. § 551 (West 2001 & Supp. 2004).

267. 18 U.S.C.A. § 2511(1) (West 2000 & Supp. 2004).

268. *Id.* § 2702.

basis review.²⁶⁹ However, a few information disclosure rules undeniably restrict speech within the scope of the First Amendment in some circumstances—for example when the tort of publication of private facts is applied to a newspaper that wishes to publish information of public concern that it obtained lawfully.²⁷⁰ Indeed, much of the historical conflict between the privacy tort and the First Amendment has come as a result of litigation over the ability of the media to publish private facts it had received about subjects it felt to be newsworthy. The Supreme Court has consistently upheld the right of the established media to publish even the most intimate private facts regardless of any countervailing privacy interest.²⁷¹ For example, in *Florida Star v. B.J.F.*,²⁷² the Supreme Court held that the First Amendment protected a newspaper that had published the name of a rape victim from liability under a privacy tort action, even though a government employee had violated agency policy by disclosing the name to the reporter.²⁷³ Unsurprisingly, the First Amendment critics rely heavily upon this line of cases to argue that “[w]hile privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.”²⁷⁴ Accordingly, First Amendment critics assert that only market-based solutions to the database problem—that is, contract, self-regulation, or privacy-enhancing technological solutions—are cognizable options given the dictates of the First Amendment.²⁷⁵

The contemporary First Amendment critique is part of a larger tradition of scholarship and jurisprudence regarding the tension between the First Amendment and the classic formulation of the privacy tort. Indeed, to understand the critique properly, as well as to perceive some of its core

269. See Schauer, *supra* note 98, at 1777–84; cf. Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1035–47 (2000) (discussing trade secrets in the First Amendment context).

270. See *Bartnicki v. Vopper*, 532 U.S. 514, 527–28 (2001).

271. See *id.* at 526–28 (holding that a radio station cannot be prohibited from publishing newsworthy information of public concern, even where such information had been illegally obtained by a third party); *Fla. Star v. B.J.F.*, 491 U.S. 524, 526 (1989) (holding that a state statute prohibiting the publication of the name of a rape victim was unconstitutional as applied to a newspaper that had obtained the name from a “publicly released police report”); *Smith v. Daily Mail Publ’g Co.*, 443 U.S. 97 (1979) (holding the First Amendment prohibits a state from punishing a newspaper for publishing the name of a juvenile murder suspect because the press lawfully obtained the information); *Okla. Publ’g Corp. v. Okla. County Dist. Court*, 430 U.S. 308 (1977) (holding the First Amendment prevents a state court from prohibiting the media from publishing the name of a juvenile in a proceeding that a reporter attended); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975) (holding the name of a rape victim obtained by the press from public records cannot be prevented from being published by statute or made the basis for liability under the nondisclosure tort).

272. 491 U.S. 524 (1989).

273. *Id.* at 541.

274. Volokh, *supra* note 3, at 1051; see also CATE, *supra* note 1, at 70.

275. See, e.g., Singleton, *supra* note 54, at 132–53.

assumptions and limitations, a brief exploration of its origins is helpful. Although American law has long protected various aspects of privacy (including what we today would call data privacy),²⁷⁶ modern thinking about the right of privacy is often traced to Warren and Brandeis's privacy article, in which their concern was not primarily data privacy, but rather media use of private information.²⁷⁷ In particular, Warren and Brandeis sought to use common law tort rules as a possible remedy for the collection and publication of personal details about famous persons by newspapers and magazines.²⁷⁸ Although such a clear attempt to regulate the publication of truthful information by the press would appear to be in direct tension with modern First Amendment doctrine, the Supreme Court at that time had yet to begin its project of giving the First Amendment preemptive force over tort law.²⁷⁹ In addition, the tort of privacy was itself immature, with early cases largely involving the right of individuals to protect themselves against the commercial misappropriation of their likeness by businesses,²⁸⁰ a context removed from both the principal concern of Warren and Brandeis and from the core of First Amendment protection. The privacy torts as we know them today were given their modern formulation as a result of the work of William Prosser in the period immediately after the Second World War.²⁸¹ Prosser revised and restated the privacy tort into four separate strands: "appropriation privacy"; intrusion privacy, which dealt with intrusions into the home or personal possessions; unauthorized public disclosure of "private" information; and the tort of "putting the plaintiff in a false but not necessarily defamatory position in the public eye."²⁸² Prosser's categorization of the third strand—the tort punishing the publication of truthful but private information—rejuvenated the argument of Warren and Brandeis. Indeed, Prosser expressly credited Warren and Brandeis with the "origins" of the privacy tort,²⁸³ even though he had done almost as much to establish it as a recognized and refined body of

276. See *The Right to Privacy in Nineteenth Century America*, *supra* note 17 (arguing that the right of privacy identified by Warren and Brandeis was predated by the broad protection given under nineteenth century law to private property, confidential communications, and personal information).

277. Warren & Brandeis, *supra* note 4, at 195.

278. *Id.* at 213–20.

279. See Richards, *supra* note 144, at 781–82 (noting that "between 1937 and 1954 . . . the Court decided a number of critical First Amendment cases that laid the doctrinal and conceptual foundation for much of modern free speech and free exercise of religion jurisprudence").

280. See G. EDWARD WHITE, *TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY* 174 (expanded ed. 2003) (citing *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442 (N.Y. 1902), and *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (Ga. 1904)).

281. See WHITE, *supra* note 280, at 173–76.

282. WILLIAM L. PROSSER, *HANDBOOK OF THE LAW OF TORTS* 637–40 (2d ed. 1955).

283. WILLIAM L. PROSSER, *HANDBOOK OF THE LAW OF TORTS* 1050–51 (1941).

law.²⁸⁴ Prosser's taxonomy of the tort of privacy in the various editions of his treatise between 1941 and 1960 gave order to the various strands of doctrine at a time when the Supreme Court was beginning to address the role of the First Amendment in tort law. Prosser and others warned of the tension between the First Amendment and the tort of publication of private information,²⁸⁵ and the Supreme Court seemed to confirm this warning in its line of privacy cases, in which the private plaintiffs lost and the media won.²⁸⁶ As a result, there is an enormous literature discussing whether the post-*New York Times v. Sullivan* First Amendment dooms the disclosure tort completely.²⁸⁷

In light of these cases, scholars—and privacy scholars in particular—have been quite gloomy about the prospects of privacy. However, such a prognosis tends again to confuse the outcomes of a handful of reported cases with the full extent of the law in actual practice.²⁸⁸ As noted above, while privacy and speech have been in famous conflict involving the nondisclosure tort as applied to newspapers, privacy and speech have coexisted harmoniously throughout the overwhelming majority of nondisclosure rules, which have never raised constitutional issues.²⁸⁹ The Supreme Court may have held in favor of press immunity from privacy rules in the *Florida Star/Bartnicki* line of cases, but it does not follow from these cases that nondisclosure rules applied in other circumstances—for example, to nonpress entities engaged in ordinary commercial activity—are constitutionally suspect. First, the Court has made quite clear in each of these cases that its ruling was narrow.²⁹⁰ Second, because of the importance of both privacy and the First Amendment, the Court has repeatedly declined to address the issue of “whether truthful publication may ever be punished consistent with the First Amendment.”²⁹¹ Third, all of these cases involve media defendants publishing allegedly newsworthy facts, but the vast majority of

284. See WHITE, *supra* note 280, at 173, 175–76.

285. See Prosser, *supra* note 164, at 389, 422; see also WHITE, *supra* note 280, at 176.

286. See cases cited *supra* note 271.

287. See, e.g., Edward J. Bloustein, *The First Amendment and Privacy: The Supreme Court Justice and the Philosopher*, 28 RUTGERS L. REV. 41 (1974); Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 TEX. L. REV. 1195 (1990); Paul Gewirtz, *Privacy and Speech*, 2001 SUP. CT. REV. 139; Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 366 (1966); Nimmer, *supra* note 137, at 935; Solove, *supra* note 71, at 972–73; Zimmerman, *supra* note 4, at 341–62.

288. See *supra* Part II.B.

289. See *supra* notes 252–269.

290. *Bartnicki v. Vopper*, 532 U.S. 514, 529 (2001) (“[T]he 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.” (quoting *Fla. Star v. B.J.F.*, 491 U.S. 524, 532–33 (1989))).

291. *Id.*

nondisclosure rules do not involve media defendants or newsworthy information, although a few high-profile cases may be produced from time to time.

Where, then, do nondisclosure rules fall under current doctrine? If the privacy tort is dead, why is our law filled with nondisclosure rules that we find constitutionally unproblematic, and, indeed, have never envisioned to fall within the scope of the First Amendment? As Schauer might put it, why have we not perceived the constitutional salience of other nondisclosure rules like the attorney-client privilege or the Video Privacy Protection Act? Some privacy scholars have proffered the concept of "private speech" as a justification for sustaining nondisclosure rules against the First Amendment.²⁹² Building upon Warren and Brandeis's distinction between matters of public and matters of private interest,²⁹³ these scholars suggest that courts should develop a category of speech that is "private" or at least not a matter of public concern.²⁹⁴ By so doing, these scholars hope to rejuvenate the tort of disclosure of private facts to make it applicable in at least egregious cases against media defendants. Although the Supreme Court has declined to hold categorically whether truthful speech on a matter not of public concern may ever be restrained consistent with the First Amendment,²⁹⁵ the "private speech" theory has some support in First Amendment doctrine. For example, in *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,²⁹⁶ a plurality of the Court noted in a private-figure trade libel case that speech not on matters of public concern receives "less stringent" First Amendment protection.²⁹⁷ Even in *Bartnicki v. Vopper*, a case received gloomily by most privacy scholars,²⁹⁸ the Court strongly implied that the First Amendment could only defeat privacy if the speech being regulated was "unquestionably a matter of public concern."²⁹⁹ However, such a theory is mostly unhelpful to the protection of the vast majority of consumer data privacy laws for a couple of reasons. First, by attempting to justify

292. See, e.g., Cohen, *supra* note 47, at 1414, 1417; Edelman, *supra* note 287, at 1229–30; Solove, *supra* note 71, at 1013–30.

293. Cf. Warren & Brandeis, *supra* note 4, at 214–16.

294. See Solove, *supra* note 71, at 1000–30 (collecting sources).

295. See, e.g., *Bartnicki*, 532 U.S. at 529 (noting "this Court's repeated refusal to answer categorically whether truthful publication may ever be punished consistent with the First Amendment").

296. 472 U.S. 749 (1985).

297. *Id.* at 760.

298. See, e.g., Katy J. Lewis, Comment, *Bartnicki v. Vopper: A New Bully in the Schoolyard of Private Expression*, 70 TENN. L. REV. 859, 886 (2003) (arguing that the Court diminished individual privacy rights in *Bartnicki*).

299. *Bartnicki*, 532 U.S. at 535; see also *Glickman v. Wileman Bros. & Elliott, Inc.*, 521 U.S. 457 (1997) (holding the First Amendment analysis inapplicable to businesses' complaint of mandatory assessment used for generic pro-industry advertising); *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557, 561–63 (1980) (granting intermediate scrutiny to "expression related solely to the economic interests of the speaker and its audience").

privacy rules against media disclosures, it lumps the easy case of consumer privacy rules with the hard case of privacy against the press. In so doing, it necessarily concedes that privacy rules are speech rules. Second, requiring courts to determine whether speech is “public” or “private” would be incredibly difficult and likely lead to indeterminate and inconsistent outcomes.

It is not necessary to develop a new jurisprudence of private speech to sustain consumer privacy rules, as existing doctrine is more than adequate to protect such rules without implicating the First Amendment. With the historical context of privacy and speech in mind, I believe that two additional factors help explain not only why consumer privacy rules have not been thought to implicate the First Amendment, but also why such rules do not in fact do so. First, many forms of nondisclosure rules are enforceable through express or implied contracts. Second, generally applicable law can operate to create a kind of “information contraband”³⁰⁰ to which nondisclosure obligations can be attached without encroaching upon the scope of the First Amendment.

1. Contract-based Nondisclosure Rules

Contract as a basis for nondisclosure rules is an uncontroversial proposition in the privacy literature, even among the First Amendment critics.³⁰¹ Two parties can create an information nondisclosure contract that the courts will enforce, even if the party agreeing to keep the information secret is a newspaper and the information is newsworthy. The Supreme Court has made clear that there does not even need to be an enforceable contract to hold the media liable for damages under such circumstances. In *Cohen v. Cowles Media Co.*,³⁰² the Court upheld the application of promissory estoppel principles to allow a plaintiff to recover against a newspaper that had broken its promise of confidentiality to him. The plaintiff had disclosed embarrassing information relating to the state lieutenant governor’s prior criminal record in exchange for the newspaper’s promise to keep his identity secret. The newspaper then published the allegations along with the plaintiff’s name. Writing for the Court, Justice White held that the state’s “law of general applicability” of promissory estoppel could be enforced against the newspaper because “generally applicable laws do not offend the

300. See Rodney A. Smolla, *Information as Contraband: The First Amendment and Liability for Trafficking in Speech*, 96 NW. U. L. REV. 1099 (2002).

301. See Volokh, *supra* note 3, at 1057.

302. 501 U.S. 663 (1991).

First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news.³⁰³

Eugene Volokh reads *Cohen* as merely establishing the principle that the First Amendment does not generally prohibit the enforcement of express or implied speech-restricting contracts against the press.³⁰⁴ Volokh acknowledges that this principle allows government to impose statutory default non-disclosure rules upon a variety of relationships in which ordinary social conventions include an expectation of confidentiality, including relationships between consumers and doctors, lawyers, and even video stores at the outer limits.³⁰⁵ However, he suggests that this general principle is subject to two significant limitations. First, it only allows people to restrict the speech of persons with whom they have a contract, and it does not cover third parties who are outside the scope of contractual or quasi-contractual privacy.³⁰⁶ Second, it does not justify mandatory government-imposed nondisclosure rules that the parties cannot waive.³⁰⁷

Volokh's category of unobjectionable speech restrictions based on a contract theory is significantly broader than it might appear at first blush. First, his use of contracts as a limiting principle is unpersuasive on its own terms. Volokh concedes that implied contracts are also outside the First Amendment. Viewing "implicit" contracts, broadly defined, as falling outside the scope of the First Amendment thus includes not only contracts that can be implied from the circumstances surrounding a transaction, but also default statutes setting up the terms of a transaction but giving parties the option of bargaining around the rule.³⁰⁸ Volokh also admits that the government can supply default rules to relationships that social convention considers confidential, and he suggests that the *U.S. West* case was incorrectly decided on this basis.³⁰⁹ However, this additional concession gives away most of the game, because virtually all nondisclosure rules outside the media context tend to reinforce implicit social conventions of confidentiality—for example, as Volokh recognizes, the Video Privacy Protection Act reflects such a social expectation in requiring video rentals to be kept secret.³¹⁰ But once the law can modify a relationship of

303. *Id.* at 669–70; see also *id.* at 670 (“[T]he publisher of a newspaper has no special immunity from the application of general laws. He has no special privilege to invade the rights and liberties of others.” (quoting *Associated Press v. NLRB*, 301 U.S. 103, 132–33 (1937))).

304. Volokh, *supra* note 3, at 1057–58.

305. *Id.* at 1058–60.

306. *Id.* at 1061.

307. *Id.* at 1061–62.

308. See Schwartz, *supra* note 71, at 1569–71.

309. Volokh, *supra* note 3, at 1060 n.37.

310. *Id.* at 1059 n.35.

this sort, it is hard to see where such a principle would stop, other than to render all default rules constitutional. Moreover, to the extent that law can reinforce social norms, a privacy rule applied to an area where there is no existing social convention of confidentiality could, over time, create new such norms. For example, scholars have argued that this is exactly what FTC regulation of privacy policies achieves in the Internet context.³¹¹ It would also seem to follow under this theory that terms should be able to be supplied to constructive “relationships” as well. Just as the law unremarkably can impose duties of confidentiality upon a lawyer when the client reasonably believes that an attorney-client relationship exists, other duties could be prescribed to regulate the ways in which profiling and marketing companies use sensitive customer data, including massive profile databases. Thus, Volokh’s acceptance of implied contracts seems to permit the government to supply a whole range of default rules to any relationship involving privacy that the government thinks reasonable to regulate.

Volokh’s second limiting principle is that while default rules may be permissible, mandatory rules violate the First Amendment. This argument is also unpersuasive. First, Volokh offers little justification for the claim that mandatory rules are somehow different than default rules from a First Amendment perspective, other than to note that the essence of contract is consent, which the Court in *Cohen* recognized.³¹² But other regimes operate to supply mandatory nondisclosure rules without falling within the scope of the First Amendment. For example, trade secret law places a mandatory obligation on those who come across trade secrets not to disclose them to others, even if the person who comes across the secret has no relationship to the trade secret holder.³¹³ Similarly, contract law supplies a whole host of mandatory terms in the consumer context in which there is reason to believe that diminished capacity exists; yet these terms do not raise constitutional issues.³¹⁴ This includes, for example, the legislative prohibition of certain types of transactions where the bargain itself is thought to be unconscionable.³¹⁵ In analogous contexts involving consumer privacy, then, mandatory rules should be equally unproblematic—for example, the Children’s Online Privacy Protection Act, which does not give children the right to waive their privacy rights and

311. See, e.g., Hetcher, *supra* note 193.

312. Volokh, *supra* note 3, at 1058–62 & n.42 (citing *Cohen v. Cowles Media Co.*, 501 U.S. 663, 671 (1991)).

313. See ROGER E. SCHECHTER & JOHN R. THOMAS, *INTELLECTUAL PROPERTY: THE LAW OF COPYRIGHTS, PATENTS AND TRADEMARKS* § 24.3 (2003).

314. See FARNSWORTH, *supra* note 182, § 1.10.

315. See *id.* § 4.28.

prohibits companies from collecting information about children without parental consent.³¹⁶ Similarly, scholars have noted that many consumers do not understand the technology of the Internet, the legal language of privacy policies, or the nature of the trade in personal information. This ignorance leads to a form of “privacy myopia,” in which consumers sell their data too frequently or too cheaply.³¹⁷ For example, some consumers who care deeply about privacy nevertheless sell their information bit by bit for frequent flier miles.³¹⁸ If a legislature were to conclude that consumers were behaving myopically in information transactions, it could also conclude that consumers are incapable of waiving their privacy rights in the context of such a transaction, just as a legislature might police standard-form contracts or consumer credit transactions in the offline context. In all of these examples, economic policing of the risk of unconscionability would be assessed under the rational basis review reserved for economic regulation generally.³¹⁹

Contract thus provides a quite expansive rationale for regulating consumer privacy transactions outside the scope of the First Amendment. Particularly when we recognize the enormous power that legislatures possess to structure and regulate the terms of economic transactions, the regime of contract law grants policymakers a wide variety of regulatory tools, including the power to supply both default and mandatory terms to transactions. Such instances of contractual commercial regulation are well outside the scope of the First Amendment.

2. Creation of Nondisclosure Rules via Generally Applicable Law

The promissory estoppel remedy in *Cohen* is certainly a broader theory of liability than contracts at law. But the remedy is still essentially a contractual one, albeit one that imports concepts of reliance and equity.³²⁰ Another theory under which a wide variety of nondisclosure rules can be justified outside the scope of the First Amendment is the related concept of “generally applicable law.” *Cohen* did not rest for the theory that only contract law can uniquely insulate speech restrictions from First Amendment difficulties. Rather, it stood for the much broader theory that a larger category of generally applicable laws do not violate the First Amendment, at least insofar as they

316. Children’s Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2000).

317. See Froomkin, *supra* note 29, at 1502–03.

318. See *id.* at 1502.

319. See *infra* Part IV.B.

320. See RESTATEMENT (SECOND) OF CONTRACTS § 90 cmt. a (1981) (“Obligations and remedies based on reliance are not peculiar to the law of contracts. This Section is often referred to in terms of ‘promissory estoppel,’ a phrase suggesting an extension of the doctrine of estoppel.”).

do not place a significant burden upon protected, expressive conduct.³²¹ In other words, *Cohen* suggests that “generally applicable laws” comprise a broader category, of which contract is but one doctrinal strand of several. Such a conclusion is confirmed by several other cases. For example, in *Seattle Times Co. v. Rhinehart*,³²² the Court held that a protective order placed on a newspaper involved in litigation could be applied validly to the newspaper to prevent it from disclosing the contents of newsworthy information it learned as a result of the discovery process. Indeed, extrapolating from *Rhinehart*, Lucas Powe—no enemy of the press, to be sure—has argued that “if the press broke into a building and pillaged files—or planted bugs—and later published, then the publication could be taken as insult upon injury,” and the press could be subjected to liability for publication of the wrongfully obtained information.³²³ Such a principle is fully consistent with *Bartnicki* and the other cases in which the Court invalidated public laws and tort actions that interfered with the media’s First Amendment rights, because each of those cases held that the media had *lawfully* obtained the published information.³²⁴ Read together, these cases suggest that information disclosure rules that are the product of generally applicable laws fall outside the scope of the First Amendment. If information is received by an entity in violation of some other legal rule—whether through breach of contract, trespass, theft, or fraud—the First Amendment creates no barrier to the government’s ability to prevent and punish disclosure. This is the case even if the information is newsworthy or otherwise of public concern.³²⁵ In this regard, the information is a kind of contraband, and traffic in it (at least by those with unclean hands) can be regulated.

321. Although it did not say so expressly, the Court’s rejection of the claim made by Justice Souter in dissent that its holding would “inhibit truthful reporting,” *Cohen v. Cowles Media Co.*, 501 U.S. 633, 671 (1991), suggests that the Court determined that promissory estoppel did not have a significant impact on First Amendment values so as to subject it to intermediate scrutiny under *Arcara/O’Brien*. See *supra* notes 213–214 and accompanying text.

322. 467 U.S. 20 (1984).

323. LUCAS A. POWE, JR., *THE FOURTH ESTATE AND THE CONSTITUTION* 176 (1991).

324. For example, in *Cox Broadcasting Corp. v. Cohn*, the Court stated:

Appellee has not contended that the name was obtained in an improper fashion or that it was not on an official court document open to public inspection. Under these circumstances, the protection of freedom of the press provided by the First and Fourteenth Amendments bars the State of Georgia from making appellants’ broadcast the basis of civil liability.

420 U.S. 469, 496–97 (1975); see also *Bartnicki v. Vopper*, 532 U.S. 514, 527–29 (2001) (same); *Fla. Star v. B.J.F.*, 491 U.S. 524, 541 (1989) (same); *Smith v. Daily Mail Publ’g Co.*, 443 U.S. 97, 105–06 (1979) (same); *Okla. Publ’g Co. v. Okla. County Dist. Court*, 430 U.S. 308, 311–12 (1977) (same).

325. Cf. *Bartnicki*, 532 U.S. at 532 & n.19.

Volokh argues that such a principle could be used to justify troubling laws in the name of “privacy,” such as a law providing that all questions by reporters would carry with them an implicit promise of confidentiality, or

a law providing that people who buy a product implicitly promise to give the seller equal space to respond to any negative article they publish about the product, unless the seller consents in writing after being given full disclosure of the true purpose for which the product is being bought.³²⁶

However, unlike the law upheld in *Cohen*, neither of these examples is really a law of general applicability. Because both laws would have a significant impact upon expressive activity on matters of public concern, they would likely trigger intermediate scrutiny under current doctrine.³²⁷ Additionally, because the media confidentiality law singles the media out for special unfavorable treatment, it would be subjected to strict scrutiny.³²⁸ Both examples are thus a long distance from the ordinary nondisclosure rules that permeate American law.

Ordinary nondisclosure rules (even mandatory ones) are less threatening to First Amendment values than the speech restriction upheld in *Cohen* for another reason. *Cohen* did not just involve information that was unlawfully obtained, but also undeniably newsworthy information that was disseminated by the press, the latter of which the Court has long recognized as filling an important social function. From a First Amendment perspective, no such equivalently important social function is provided by database companies engaged in the trade in personal data. Indeed, a general law regulating the commercial trade in personal data by database, profiling, and marketing companies is far removed from the core speech protected by the First Amendment, and is much more like the “speech” outside the boundaries of heightened review.³²⁹

326. Volokh, *supra* note 3, at 1058.

327. See *supra* notes 213–214 and accompanying text.

328. See *supra* note 204.

329. Cf. Schauer, *supra* note 98. In a thoughtful forthcoming article, Eugene Volokh makes the claim that the concept of generally applicable laws is insufficient to protect important First Amendment values from abridgement. In particular, he argues that it is not enough to uphold a law simply because it is content neutral on its face, because such rules can be content based as applied, for example to advocacy of illegal conduct. Volokh, *supra* note 131 (manuscript at 11). It is difficult and perhaps unfair to take issue with arguments that have not yet been published, but I believe that Volokh’s assertion is inapplicable to my arguments here for three reasons. First, to the extent he argues that current doctrine underprotects First Amendment values, this does not conflict with my claim here that ordinary doctrinal tools can be used to sustain the constitutionality of a wide variety of nondisclosure and other privacy rules. Indeed, Volokh’s dissatisfaction with the strictness of current doctrine in this area perhaps supports my claim that the First Amendment critics overstate the power of the First Amendment when they make normative claims about its applicability to privacy rules. Second, because the subversive advocacy cases are some distance removed from commercial database nondisclosure rules in terms of their proximity to the core of what the First Amendment protects, his critique does not speak to the privacy context, but rather to matters of

Thus, even though some information disclosures can be viewed as speech within the scope of the First Amendment, information disclosure rules regulating nonnewsworthy information or disclosures of information that was not lawfully obtained (regardless of whether it is newsworthy or not) are, as a general matter, outside the scope of the First Amendment and are thus constitutionally sound.

D. Regulation of Direct Marketing

Regulation of direct marketing—whether junk mail, a telemarketing call, unsolicited spam e-mails, or some other means—is undeniably regulation of speech. Indeed, it may seem odd even to categorize a telemarketing call as the regulation of an information flow, except insofar as the information flowing in this case is an invitation to purchase a product. However, because this issue is tied up in the database problem, in the First Amendment critique and in the larger free speech and database privacy debate, it is worth some examination, if only to show the ways in which it differs from the other stages, and to demonstrate how the First Amendment critique is just as unpersuasive in this context as in the others.

A telemarketing call is an example of the final and most intrusive stage of the database problem, occurring after the collection of personal data by a profiling company, the use of that data to determine which consumers best fit a target profile, and the disclosure of the profile to a telemarketing company that wishes to purchase it. Unlike those previous stages, a telemarketing call is undoubtedly “speech” within the scope of the First Amendment. As discussed above, current doctrine answers the protection question by treating commercial speech restrictions with intermediate scrutiny by applying the four-part *Central Hudson* test, although the trend over the past two decades seems to be that the test is being applied with more heightened scrutiny.³³⁰ The First Amendment interest in telemarketing is thus greater than the corresponding interest in information collection, use, and disclosure rules.

On the other hand, the privacy interests at stake in the telemarketing context are not only stronger and more intellectually coherent than in the

indisputable public concern. Third, to the extent we probably do disagree about the breadth of the *Cohen v. Cowles Media* principle, I believe that my interpretation of this rather murky area of the jurisprudence is sufficiently speech-protective because heightened scrutiny is still retained for generally applicable laws that have a significant impact upon expressive activity. See *supra* notes 203–206 and accompanying text. Our ultimate disagreement may be simply one regarding the expressive content of databases, which I tend to treat as warranting lower scrutiny for reasons I develop further *infra* Part IV.

330. See *supra* notes 150–153 and accompanying text.

collection, use, and disclosure contexts; they are also more likely to resonate with a court. Although scholars have struggled to define “privacy,” there is a consensus that the general term “privacy” encompasses three separate “clusters.”³³¹ “Substantive” or “decisional” privacy is the constitutional right to make certain fundamental decisions free from government scrutiny or interference. Cases like *Roe v. Wade*³³² and *Griswold v. Connecticut*³³³ embody this privacy cluster. “Residential privacy” refers to the privacy interest individuals have in their homes against unwanted surveillance or interference by government, businesses, or other individuals.³³⁴ “Data privacy” (also known as “information privacy”) refers to the notion that the rights of individuals are threatened by detailed private-sector databases containing profiles of their preferences, including information about which consumer products they use, as well as potentially embarrassing information about their health, political views, or sexual predilections.³³⁵

While telemarketing implicates data privacy, it also implicates residential privacy, because telemarketing disturbs individuals in the enjoyment of their homes. And unlike data privacy, which is a poorly articulated right, residential privacy is a robust right of constitutional magnitude that can hold its own against free speech. Indeed, the Supreme Court has long been solicitous of residential privacy as a substantial regulatory and societal interest, not just in the Fourth Amendment context,³³⁶ but also as a bulwark supporting other constitutional privacy rights.³³⁷ And whereas the data privacy right embodied in the disclosure tort has traditionally failed to compete with the First Amendment in cases in which the two rights have come into conflict, the privacy interests inherent in the home have long been able to defeat even core First Amendment speech. As early as 1943, the Supreme Court reaffirmed the right

331. See Kang, *supra* note 10, at 1202.

332. 410 U.S. 113 (1973).

333. 381 U.S. 479 (1965).

334. See Kang, *supra* note 10, at 1202.

335. *Id.* at 1205–17.

336. See, e.g., *Kyllo v. United States*, 533 U.S. 27 (2001) (holding that the well-established residential privacy of the home embodied in the Fourth Amendment prevents police from using thermal imagers from public streets to view into homes); *Wilson v. Layne*, 526 U.S. 603, 610 (1999) (“The Fourth Amendment embodies th[e] centuries-old principle of respect for the privacy of the home . . .”).

337. See, e.g., *Lawrence v. Texas*, 539 U.S. 558, 562 (2003). The *Lawrence* Court stated: In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct. *Id.*; see also *Griswold*, 381 U.S. at 485–86 (“Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.”).

of homeowners to exclude unwanted speakers from their property,³³⁸ although it invalidated a municipal ordinance prohibiting door-to-door distribution of handbills. The Court was more explicit in *Frisby v. Schultz*,³³⁹ in which it declared:

One important aspect of residential privacy is protection of the unwilling listener. Although in many locations, we expect individuals simply to avoid speech they do not want to hear, the home is different. . . . [A] special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions. Thus, we have repeatedly held that individuals are not required to welcome unwanted speech into their own homes and that the government may protect this freedom.³⁴⁰

As a result, when the Court in *Rowan v. United States Post Office Dep't*³⁴¹ assessed a First Amendment challenge to the constitutionality of a federal law allowing homeowners to prevent companies from sending them sexually explicit junk mail and to have their names removed from the mailing lists, it upheld the law on residential privacy grounds.

It should therefore be no surprise that even the Tenth Circuit—which had not previously held data privacy in high regard³⁴²—recently upheld the FCC's Do-Not-Call regulations of telemarketers against a First Amendment challenge. Although the district court in that case had been swayed by the First Amendment critique,³⁴³ the Court of Appeals, relying on the tradition of residential privacy, upheld the Do-Not-Call Registry³⁴⁴ against the same *Central Hudson* challenge that had felled the FCC's data privacy regulations in the *U.S. West* case.³⁴⁵ Indeed, other Supreme Court precedent suggests that the intrusiveness of telemarketing makes for a cognizable harm that can be regulated under the First Amendment, despite the fact that telemarketing is commercial speech.³⁴⁶

338. *Martin v. City of Struthers*, 319 U.S. 141, 147 (1943).

339. 487 U.S. 474 (1988).

340. *Id.* at 484–85 (citations omitted).

341. 397 U.S. 728 (1970).

342. *See, e.g., U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999) (“We have some doubts about whether this interest, as presented, rises to the level of ‘substantial.’”).

343. *Mainstream Mktg. Servs. Inc. v. FTC*, 283 F. Supp. 2d 1151, 1168 (D. Colo. 2003) (holding Do-Not-Call Registry unconstitutional under *Central Hudson*), *rev'd*, 358 F.3d 1228 (10th Cir. 2004).

344. *Mainstream Mktg. Servs.*, 358 F.3d at 1242.

345. *Cf. U.S. West*, 182 F.3d at 1239 (holding the regulations were not narrowly tailored and thus failed the fourth prong of the *Central Hudson* analysis).

346. *See, e.g., Illinois ex rel. Madigan v. Telemarketing Assocs., Inc.*, 538 U.S. 600 (2003) (holding the First Amendment does not bar a fraud claim against telemarketers who make misleading statements about the way donations would be used); *see also Telephone Consumer Protection Act of 1991*, 47 U.S.C. § 227 (2000) (regulating telemarketing).

* * * *

My argument to this point has hopefully demonstrated that the First Amendment critique rests on both an unpersuasive conception of the structure of First Amendment protection, and a cramped reading of the sorts of information regulations that are reconcilable with our commitment to free speech. The previous part has suggested that ordinary doctrinal tools can be used to demonstrate the constitutionality of a wide variety of privacy rules both applied to the database context and other contexts. However, simply because the law is a certain way does not mean that it should remain so. In the next part, I develop a normative account explaining why I believe that the interpretation of both First Amendment and data privacy law that I have sketched up to this point is in fact superior to the account put forth by the First Amendment critics.

IV. THE PERILS OF VOLOKHNER

Although information flows can be regulated in the consumer privacy context under current doctrine, the First Amendment critique has nevertheless attracted many adherents. Despite its simplicity (or perhaps because of it), scholars and judges tend to find it persuasive. After all, given the central importance of the First Amendment in American political and legal culture, who wants to be against the First Amendment, in any context?³⁴⁷ I have suggested that one of the dangers of the First Amendment critique is that it represents a constitutionalization of data privacy rules, placing a thorny and tremendously important social issue beyond the regulatory authority of elected legislatures. In this respect, the First Amendment critique can be located within the broader strand of First Amendment thought that believes, drawing upon libertarian theory, that the First Amendment guarantees not just freedom of speech for individuals, but also for business interests, and that many economic regulations conflict with the First Amendment. But free speech doctrine is malleable and often indeterminate, and although the First Amendment critique is shaky under current First Amendment doctrine, it is neither absurd nor lacking in facial appeal. In light of this observation, it is essential to articulate justifications against both the constitutionalization of information policy and the stretching of First Amendment doctrine into areas where it does not fit.

347. Cf. Schauer, *supra* note 95, at 176 (describing the First Amendment as an “argumentative showstopper[]”). One possible exception to this rule is child pornography, which forces even zealous First Amendment absolutists to get off the bus. For an explanation of this phenomenon, see generally Amy Adler, *Inverting the First Amendment*, 149 U. PA. L. REV. 921 (2001); Amy Adler, *The Perverse Law of Child Pornography*, 101 COLUM. L. REV. 209 (2001).

In this part, I explore some of the ramifications of the First Amendment critique for free speech and rights jurisprudence generally. I have argued that much of the confusion in the law at the intersection of privacy rights and the First Amendment comes from the conceptual murkiness at the core of both privacy law and (counterintuitively) the First Amendment itself. First Amendment critics are quick to apply seemingly applicable or analogous doctrinal tests to privacy rules, but are less able to supply jurisprudential values advanced by the critique other than a vague notion of the “freedom of information.” In fact, when viewed from the perspectives of both privacy law and First Amendment law, the First Amendment critique of data privacy rules threatens serious and pernicious jurisprudential consequences.

In Part IV.A, looking at the issue from the perspective of privacy law, I examine the broader implications of the First Amendment critique and its “freedom of information” principle for information policy. In so doing, I assess the argument that the First Amendment critique is merely *Lochner*ism in another guise. I conclude that although there are parallels between the First Amendment critique and the traditional understanding of *Lochner*, recent scholarship by legal historians has complicated this sort of claim, revealing that *Lochner* in practice was not as doctrinally illegitimate as its critics have charged. Nevertheless, to the extent that the First Amendment critique resembles the traditional view of *Lochner*, this remains a fairly significant criticism, suggesting that the First Amendment critique is out of step with many basic assumptions about the First Amendment. In Part IV.B, I look at the critique from the other side—from the perspective of First Amendment law. I argue that examining the revisionist intellectual history of *Lochner* reveals the real jurisprudential threat of the movement of which the First Amendment critics are a part—an obliteration of the distinction between economic and political rights that represents the core of modern constitutionalism.

A. The First Amendment Critique and “Freedom of Information” as *Lochner*

Although much is contested at the intersection of data privacy and the First Amendment, one thing at least is clear: First Amendment critics assert that because data privacy rules violate the First Amendment, the regulation of data privacy should be placed beyond the scope of normal regulatory policy and politics. They may couch the constitutional mandate apologetically because of the need to protect other, more important values,³⁴⁸ or they may assert

348. See, e.g., Volokh, *supra* note 3, at 1050–51; sources cited *supra* notes 57–59.

unapologetically that freedom of information is both a constitutional command and good policy,³⁴⁹ but the claim is stated unequivocally. Privacy scholars have failed to point out the similarities between this freedom of information theory of the First Amendment and the freedom of contract theory of due process embodied in the *Lochner* line of cases.³⁵⁰ This is somewhat surprising given the striking parallels between the traditional understanding of *Lochnerism* and the First Amendment critique.

The traditional view of *Lochner* goes something like this: Technological advances inherent in the industrialization of America around the turn of the last century created a series of serious social and economic dislocations, such as unsafe working conditions, unfairly low wages, child labor, sweatshops, and monopolistic trade practices. Reformers including Populists and Progressives sought to remedy these problems of poor working conditions and unequal bargaining power by enacting social legislation.³⁵¹ Unfortunately, Supreme Court Justices interpreted the word "liberty" in the Due Process Clauses to mean "freedom of contract," an inalienable right possessed by both workers and employers to buy and sell their labor in a marketplace unfettered by government controls. In so doing, the judges illegitimately read their own pro-business laissez-faire views of political economy into the Due Process Clauses. This interpretation of "liberty of contract," the story continues, erected a constitutional barrier to most early twentieth century state or federal legislation directed at hours, wages, and working conditions.³⁵² However, less activist judges in the mid-twentieth century consigned *Lochner* to the doctrinal scrapheap, and today *Lochner* is one of the worst charges that can be leveled against a doctrine or constitutional interpretation, an unequivocal normative repudiation of "courts that appear to be substituting their own view of desirable social policy for that of elected officials."³⁵³

From this perspective, there are some fairly strong parallels between the traditional conception of *Lochner* and the First Amendment critique of data

349. See sources cited *supra* notes 53–56.

350. See *Lochner v. New York*, 198 U.S. 45 (1905) (invalidating a New York statute setting maximum hours for bakers on due process grounds). Scholars in the analogous areas of cyberlaw and intellectual property have, however, identified a resurgence of *Lochner*-style arguments in those areas of law. See Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462 (1998); Paul M. Schwartz & William Michael Treanor, *Eldred and Lochner: Copyright Term Extension and Intellectual Property as Constitutional Property*, 112 YALE L.J. 2331 (2003).

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

352. WHITE, *supra* note 8, at 241–42.

353. Friedman, *supra* note 351, at 1385; see also David E. Bernstein, *Lochner's Legacy's Legacy*, 82 TEX. L. REV. 1, 2–4 (2003) (collecting sources); Friedman, *supra* note 351 (same).

privacy legislation. Both theories are jurisprudential responses to calls for legal regulation of the economic and social dislocations caused by rapid technological change. Lochnerism addressed a major socio-technological problem of the industrial age—the power differential between individuals and businesses in newly industrial working conditions—while the First Amendment critique addresses a major socio-technological problem of our information age—the power differential between individuals and businesses over information in the newly electronic environment. Both theories place a libertarian gloss upon the Constitution, interpreting it to mandate either “freedom of contract” or “freedom of information.” Both theories seek to place certain forms of economic regulation beyond the power of legislatures to enact. And both theories are eagerly supported by business interests keen to immunize themselves from regulation under the aegis of constitutional doctrine.³⁵⁴ To the extent that the First Amendment critique is similar to the traditional view of *Lochner*, then, its elevation of an economic right to first-order constitutional magnitude seems similarly dubious.

Although it might be both tempting and rhetorically effective to accuse the critics of Lochnerism and move on, in the interests of fairness and intellectual honesty it is important to admit that the conventional view of *Lochner* is probably quite erroneous, at least as a description of the jurisprudence in its actual operation. Legal historians examining the intellectual history of the late nineteenth and early twentieth centuries have significantly revised our understanding of not just *Lochner*, but also the orthodox legal epistemology that produced it and the ways in which that jurisprudential worldview evolved into the radically different vision of the Constitution, and ultimately law itself, that animates orthodox modern legal thought.³⁵⁵ Scholarship by these so-called “*Lochner* revisionists” has significantly revised our understanding of the intellectual contexts in which the cases were decided. Specifically, these scholars have uncovered and made great strides towards reconstructing a coherent vision of law that constituted jurisprudential orthodoxy during the late nineteenth and early twentieth centuries. Termed variously “legal orthodoxy,”

354. See, e.g., Jack Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1 (2004); Julie E. Cohen, *Lochner in Cyberspace*, 97 MICH. L. REV. 462 (1998).

355. See, e.g., BARRY CUSHMAN, *RETHINKING THE NEW DEAL COURT* (1998); WHITE, *supra* note 8; Michael Les Benedict, *Laissez-Faire and Liberty: A Re-Evaluation of the Meaning and Origins of Laissez-Faire Constitutionalism*, 3 LAW & HIST. REV. 293 (1985); Charles W. McCurdy, *The Roots of “Liberty of Contract” Reconsidered: Major Premises in the Law of Employment, 1867–1937*, 1984 Y.B. SUP. CT. HIST. SOC’Y 20. For a more detailed overview of such efforts, see generally Friedman, *supra* note 351, at 1397–1402 (collecting sources).

“classical legal thought,” or “legal formalism,”³⁵⁶ this jurisprudential worldview was an interlocking system of doctrines³⁵⁷ that represented a functioning classical intellectual engine not unlike the estates system in land law. Formalist legal theory posited that the Constitution had a fixed, essentialist, immanent meaning; that judges could uncover this meaning through ordinary common law modes of inquiry; and that such a mode of inquiry resulted in the judge applying an existing, determined law to new circumstances.³⁵⁸ Most fundamentally, legal formalism drew a sharp separation between the sources of law and the judges who interpreted those sources; unlike the legal realists, whose view of law ultimately triumphed over formalism over the course of the first four decades of the twentieth century, formalist judges believed that they discovered law but did not make it.³⁵⁹

Revisionist scholarship has described the formalist judges as engaging in “guardian review” in constitutional cases, glossing constitutional text with meaning derived from external sources in order to mark out the boundaries between public authority such as the police power and private rights like the liberty protected by the Due Process Clauses. Guardian review was quite different from the modern regime of bifurcated review, according to which courts do not believe that they divine law from external sources, but rather believe that they create it in many instances. Mindful of their countermajoritarian role under an epistemology in which they create rather than divine law, modern courts applying bifurcated review generally treat legislative enactments regarding economic policy with deference, and closely scrutinize only those enactments that interfere with political rights and thus threaten the operation of ordinary democratic processes.³⁶⁰ In the context of the Due Process Clauses at issue in the *Lochner* line of cases, the revisionists have demonstrated persuasively that these cases were not merely injections of reactionary pro-business politics into the constitutional text, but were rather interpretations of the Constitution that were consistent with legitimate authority. Such decisions are, the revisionists argue, best explained as determined by settled existing doctrine rather than judges behaving as political actors.³⁶¹ Thus, as a descriptive explanation of *Lochner*, the behavioralist theory of “laissez-faire constitutionalism” is unpersuasive.³⁶²

356. WILLIAM M. WIECEK, *THE LOST WORLD OF CLASSICAL LEGAL THOUGHT: LAW AND IDEOLOGY IN AMERICA, 1886-1937*, at 3 (1998).

357. See CUSHMAN, *supra* note 355, at 6-7.

358. See WHITE, *supra* note 8, at 167-70.

359. See *id.* at 168-74.

360. See *id.* at 3-4.

361. See Friedman, *supra* note 351, at 1399-1400 (collecting sources).

362. CUSHMAN, *supra* note 355, at 3, 7; WHITE, *supra* note 8, at 241-46.

Nevertheless, even in light of the tremendously valuable insights provided by the *Lochner* revisionists, the First Amendment critique retains enough similarities to the traditional view of *Lochner* to be normatively questioned from a modern perspective as a jurisprudentially sound application of the First Amendment. Even if *Lochner* was not an illegitimate injection of pro-business libertarian ideology into constitutional decisionmaking by judges, it was widely condemned as such. Such critiques were made both by contemporaries who accused judges of importing their policy preferences and class biases into their decisions, and by later judges and scholars who replaced guardian review with bifurcated review, in part in reaction to the perceived illegitimacy of *Lochner*.³⁶³ Thus, merely because the *Lochner* line of cases appears to have been legitimate under existing doctrine as a descriptive matter, it does not follow as a normative matter that judges should nevertheless be free to inject their view of good social and economic policy into constitutional interpretation. The realists may have been wrong that “liberty of contract” was an empty vessel into which the policy preferences of conservative judges were poured, but this does not mean that judges today can legitimately pour ideological content into the Constitution to void the economic policy of elected representatives. To the extent that the First Amendment critique suggests judges should do something similar in the database context by treating the First Amendment as embodying a “freedom of information” rationale, such an assertion would be similarly illegitimate. In this regard, the modern normative commitment against placing social and economic problems beyond the reach of democratic regulatory politics would still counsel against taking the First Amendment critique at face value.

Alternatively, for a couple of other reasons, one could accept the insights of the *Lochner* revisionists and still decide quite rationally that *Lochnerism* (and thus the First Amendment critique) is as illegitimate as the conventional view would suggest. First, as William Wiecek has argued, legal formalism presented a worldview that was attractive to lawyers because it protected wealth and placed the regulation of property rights beyond the power of legislatures to redistribute.³⁶⁴ Thus, the reconstruction of the doctrinal coherence of *Lochner* would not displace the suggestion that lawyers could find formalist jurisprudence attractive as a purely instrumental matter because it produced outcomes they favored. To the contrary, it would merely confirm

363. See Friedman, *supra* note 351, at 1420–28.

364. WIECEK, *supra* note 356; see also William M. Wiecek, *The Rise and Fall of Classical Legal Thought: Preface to the Modern Constitution*, in CONSTITUTIONALISM AND AMERICAN CULTURE: WRITING THE NEW CONSTITUTIONAL HISTORY 64, 66 (Sandra F. VanBurkleo et al. eds., 2002).

that the elite lawyers who subscribed to and articulated *Lochner*ism were merely good advocates who had thought through the intellectual clarity of their position. It would not, however, say anything about the merits of that position other than its intellectual elegance.

Second, even if *Lochner* were legitimate under established doctrine, it could nevertheless be illegitimate for other reasons. Barry Friedman has argued that even though the *Lochner* line of cases was consistent with formalist doctrine, the jurisprudence was widely criticized as illegitimate by the larger public.³⁶⁵ Like Wiecek's lawyers, who found *Lochner* attractive because of its outcomes, progressive critics also repudiated it because it created outcomes they found unjust. In this context, Barry Friedman draws a distinction between "legal legitimacy"—whether legal decisions have "an established jurisprudential basis"—and what he calls "social legitimacy"—an inquiry that "looks beyond jurisprudential antecedents of constitutional decisions and asks whether those decisions are widely understood to be the correct ones given the social and economic milieu in which they are rendered."³⁶⁶ Friedman points to the widespread contemporary popular disagreement with the outcomes of liberty of contract cases as an example of such illegitimacy.³⁶⁷ And in the modern context, the enormous public outcry and prompt congressional action surrounding the judicial invalidation of the FCC's Do-Not-Call Registry similarly suggests that there is little tolerance today for constitutionalizing information policy.³⁶⁸

The parallels between the First Amendment critique and the traditional view of *Lochner* are not perfect, but they should at least serve to caution us against an uncritical acceptance of the First Amendment critique. The database problem represents a particularly thorny instance of a social problem created by rapid advances in technology. Just as no simple regulatory solution is likely to produce an optimal result, so too is no simple constitutional solution likely to do the same. Because both coverage of the First Amendment and its doctrine are unclear, facile constitutional mantras like "freedom of information" are particularly ill-suited to resolve a complex problem in a means

365. Friedman, *supra* note 351, at 1453–56.

366. *Id.* at 1386–87.

367. *Id.*

368. In only a few months after the creation of the Do-Not-Call Registry, over fifty million phone numbers were registered. When on September 23, 2003, a federal district court invalidated the Registry as lacking sufficient congressional authorization, *United States Sec. v. FTC*, 282 F. Supp. 2d 1285, 1290–91 (W.D. Okla. 2003) (holding that Congress had not given the FTC sufficient authorization to implement the Registry), there was an enormous public outcry. In response, Congress took the almost unprecedented step of reversing the district court by passing a statute in little more than a day. See Adam Zitter, Note, *Good Laws for Junk Fax? Government Regulation of Unsolicited Solicitations*, 72 *FORDHAM L. REV.* 2767, 2767 (2004).

that is satisfactory to society as a whole. As I have argued above, it would be a great tragedy for the continued ascendance of the First Amendment critique to handicap or prohibit elected policymakers from exploring such a difficult question of social and economic policy.³⁶⁹

B. The First Amendment Critique and the Bifurcated Review Project

If the jurisprudential problems caused by the First Amendment critique seem significant from the perspective of privacy law, they are even more dire from the perspective of First Amendment law. Indeed, the same intellectual history of rights jurisprudence that complicates the traditionalist view of *Lochner* brings the real jurisprudential threat of the First Amendment critique into sharp focus. At stake in the database debate is not merely whether data privacy rules can be enforced consistent with the First Amendment, but rather what sorts of rights the First Amendment protects at all. At bottom, the First Amendment critique proffers a robust rationale of freedom of information that threatens the very structure of modern rights jurisprudence—the bifurcated system of judicial review that defers to legislatures with respect to economic rights but treats laws infringing upon political rights with greater scrutiny.

Modern legal historians have devoted significant attention to the task of reconstructing the jurisprudential universe of legal formalism that produced *Lochnerian* rights jurisprudence, but they have spent far less time examining the ways in which the Supreme Court laid the foundations for the rights jurisprudence that replaced it.³⁷⁰ As I have suggested elsewhere, much of this work was done by the Court in a series of cases that roughly corresponded with the Second World War, many of which involved free speech and free exercise challenges brought by the Jehovah's Witnesses.³⁷¹ Only a handful of modern scholars have devoted much serious effort to reconstructing this critical episode in the intellectual history of American law, but the work they have done sheds significant light on the origins of modern rights jurisprudence.

This revisionist rights scholarship has shown how the Supreme Court used the First Amendment as a bridge between the old regime of guardian review and the modern regime of bifurcated review.³⁷² The Court outlined this new approach in “famous footnote four” of the 1938 case of *United States v.*

369. See *supra* notes 31–45.

370. See Richards, *supra* note 144, at 781–82. For exceptions, see WHITE, *supra* note 8, and Freyer, *supra* note 144.

371. See Richards, *supra* note 144, at 781–82.

372. See WHITE, *supra* note 8, at 128–63; G. Edward White, *The First Amendment Comes of Age: The Emergence of Free Speech in Twentieth-Century America*, 95 MICH. L. REV. 299 (1996).

Carolene Products Co.,³⁷³ which posited a relaxed standard of review for economic regulation but a more stringent standard of review for laws that infringed upon rights guaranteed by the text of the Bill of Rights or otherwise interfered with the democratic process.³⁷⁴ As G.E. White explains, this system of “bifurcated review” embodied two of the central assumptions of the new jurisprudence:

By fostering judicial deference in the area of economic regulation, the project embraced the perceived truth that unregulated economic activity actually infringed on the freedom of a significant number of actors in the economic marketplace and reinforced rational regulatory policies that were based on that truth. By fostering judicial scrutiny of legislative restrictions on speech and other noneconomic liberties, the project underscored the centrality of the modernist freedom premise when that premise could be associated with the goals of democratic theory.³⁷⁵

Central to the dualism at the core of the new system of judicial review was a strict separation between economic and political rights. Thus, as noted above,³⁷⁶ the Supreme Court initially excluded commercial speech from heightened First Amendment protection in *Valentine v. Chrestensen*³⁷⁷ and *Breard v. Alexandria*,³⁷⁸ in order to maintain this separation. In another case involving the distribution of literature, Justice Douglas drew a sharp distinction between religious texts covered by “the privileges protected by the First Amendment” and advertising, which he dismissed as “the wares and merchandise of hucksters and peddlers.”³⁷⁹

The sharp line between economic and political rights critical to the intellectual coherence of bifurcated review has persisted, though it perhaps has not endured with the precise clarity that its drafters intended. Indeed, it is in the advertising cases that the greatest blurring of the line between political and economic rights has occurred. After a series of cases indicating that certain forms of advertising associated (quite ironically) with the privacy rights protected in *Griswold* and *Roe* warranted heightened protection, the Court in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*³⁸⁰ brought “commercial speech” within the scope of the First Amendment. In drafting the opinion of the Court, Justice Blackmun was confronted with

373. 304 U.S. 144, 152 n.4 (1938).

374. See Richards, *supra* note 144, at 900.

375. White, *supra* note 372, at 309.

376. See *supra* note 150 and accompanying text.

377. 316 U.S. 52 (1942).

378. 341 U.S. 622 (1951).

379. *Murdock v. Pennsylvania*, 319 U.S. 105, 115 (1943).

380. 425 U.S. 748 (1976).

the conceptual problem that as an economic right, the right to advertise was not supported by any of the existing justifications for free speech. He solved this problem by making one up:

As to the particular consumer's interest in the free flow of commercial information, that interest may be as keen, if not keener by far, than his interest in the day's most urgent political debate. . . . Generalizing, society also may have a strong interest in the free flow of commercial information. Even an individual advertisement, though entirely "commercial," may be of general public interest.³⁸¹

Blackmun went on to add:

Advertising, however tasteless and excessive it sometimes may seem, is nonetheless dissemination of information as to who is producing and selling what product, for what reason, and at what price. So long as we preserve a predominantly free enterprise economy, the allocation of our resources in large measure will be made through numerous private economic decisions. It is a matter of public interest that those decisions, in the aggregate, be intelligent and well informed. To this end, the free flow of commercial information is indispensable.³⁸²

Taken at face value, Blackmun's rationale for heightened constitutional protection for commercial advertising threatened to dissolve the line between economic and political speech—and with it any distinction between economic and political rights. In so doing, he opened the door to the resuscitation of *Lochner*-style economic rights (or at least the traditional understanding of those rights). This fact was not lost on a few contemporary observers, be they dissenting members of the Court³⁸³ or scholarly commentators.³⁸⁴ Indeed, in the aftermath of the decision, observers predicted the expansion of First

381. *Id.* at 763–64.

382. *Id.* at 765.

383. For example, Justice Rehnquist argued in dissent that:

The Court speaks of the importance in a "predominantly free enterprise economy" of intelligent and well-informed decisions as to allocation of resources. While there is again much to be said for the Court's observation as a matter of desirable public policy, there is certainly nothing in the United States Constitution which requires the Virginia Legislature to hew to the teachings of Adam Smith in its legislative decisions regulating the pharmacy profession.

Id. at 783–84 (Rehnquist, J., dissenting); see also *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557, 591 (1986) (Rehnquist, J., dissenting) (arguing that the Court had, "by labeling economic regulation of business conduct as a restraint on 'free speech,' gone far to resurrect the discredited doctrine of cases such as *Lochner*").

384. See, e.g., Thomas H. Jackson & John Calvin Jeffries, Jr., *Commercial Speech: Economic Due Process and the First Amendment*, 65 VA. L. REV. 1, 40 (1979) (characterizing the case as "the revivification of economic due process in the guise of commercial speech").

Amendment analysis to other areas of business speech regulation like securities law.³⁸⁵ However, the fears raised by these commentators failed to materialize.

The line between economic and political rights has persisted, and it remains central to the continued coherence of the modern system of bifurcated review. An expansive reading of *Virginia Pharmacy* as opening the floodgates to heightened review for other economic speech rights besides advertising was rejected, and the dividing line between economic and political rights was shored up in its new location, with commercial advertising placed upon the political rights side of the line. Thus, the feared treatment of securities speech as commercial speech did not come to pass, and the large categories of speech that fall outside the scope of the First Amendment have not been subjected to heightened constitutional review.³⁸⁶ Although the balance is a delicate one, nonadvertising speech in the commercial context continues to be assessed properly under the rational basis review afforded to the other economic rights by the bifurcated review project.³⁸⁷

Looking at the issue from the perspective of free speech law allows a better appreciation of the threat to the modern scheme of rights jurisprudence represented by the First Amendment critique. The critics' attempt to clothe economic rights with the garb of political rights would destroy the basic dualism on which the edifice of modern rights jurisprudence is built. This may not be their intent, but it would be the likely effect of their success. In the database context, this might mean only that nondisclosure rules are treated with heightened scrutiny, but the advancement of a principle of freedom of information as a full-blooded rationale for heightened First Amendment scrutiny would not be limited merely to that context. Every regulation that could be classified as restricting "speech" or information flows would be brought within the scope of First Amendment heightened review. Indeed, much of Volokh's own First Amendment scholarship, in addition to his influential privacy article, has tracked such a prediction, subjecting previously nonsalient areas of speech regulation to more searching doctrinal analysis.³⁸⁸

385. See Schauer, *supra* note 98, at 1780 (collecting sources).

386. See *id.*

387. See *id.* at 1777-84.

388. See, e.g., Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147 (1998); Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. (forthcoming Feb. 2005); Eugene Volokh, *Freedom of Speech and Intellectual Property: Some Thoughts After Eldred*, 44 LIQUORMART, and BARTNICKI, 40 HOUS. L. REV. 697 (2003); Eugene Volokh, *Freedom of Speech and the Right of Publicity*, 40 HOUS. L. REV. 903 (2003); Volokh, *supra* note 131; Eugene Volokh, *What Speech Does "Hostile Work Environment" Harassment Law Restrict?*, 85 GEO. L.J. 627 (1997); Eugene Volokh & Brett McDonnell, *Freedom of Speech and Independent Judgment Review in Copyright Cases*, 107 YALE L.J. 2431 (1998).

A reasonable person could certainly argue that the First Amendment should apply to everything that the dictionary might deem to be “speech.” It might also be reasonable to argue that information flows generally should be treated to heightened constitutional protection, although this would complicate regulation of not only the database problem but also the entire information economy, with spillover effects into areas such as intellectual property.³⁸⁹ It might even be reasonable to argue that the distinction between political and economic rights is unwise, unworkable, or even illegitimate, as some prominent scholars have recently asserted.³⁹⁰ However, such a system would not be our system, and it would likely mean the end of bifurcated review’s distinction between political and economic rights. If we are to make such a change legitimately and coherently, it should come overtly, not by allowing the *Virginia Pharmacy* rationale of freedom of information gradually to undermine the distinction between political and economic rights.

CONCLUSION

Over four decades ago, before the advent of the Internet or the introduction of freedom of information as a theoretical justification for the First Amendment, Thomas Emerson examined the intersection of privacy and the First Amendment. Emerson noted:

Any society sincerely interested in protecting the right of privacy is hardly likely to be at the same time hostile to the right of free expression. Both interests tend to have the same friends and the same enemies. The chief danger is that the right of privacy will be used as a screen, by those not really interested in either interest, to infringe upon legitimate expression. This danger can be met if the courts actively insist upon a careful definition of a genuine right of privacy and upon a fair accommodation of the two interests.³⁹¹

389. Perhaps recognizing this tension, the Supreme Court in the recent case *Eldred v. Ashcroft* rejected the assertion of public interest groups that federal copyright statutes regulate speech and thus warrant intermediate First Amendment scrutiny. *Eldred v. Ashcroft*, 537 U.S. 186, 218–21 (2003). Justice Ginsburg’s opinion for the Court rested on a number of justifications, including the fact that copyright law includes a number of internal speech-protective mechanisms, but implicit in its treatment of the issue seems to be a judgment that heightened scrutiny would unduly handicap Congress in its formulation of information policy more generally. *Id.* at 218–22.

390. See, e.g., RANDY E. BARNETT, *RESTORING THE LOST CONSTITUTION: THE PRESUMPTION OF LIBERTY* 253–54 (2004) (arguing for a rejection of “the pure Footnote Four approach” in favor of a constitutionalism that protects economic as well as political liberties); Walter Dellinger, *The Invisibility of Economic Rights and Personal Liberty*, in 2003–2004 *CATO SUPREME COURT REVIEW* 9, 13–16 (Mark K. Moller et al. eds., 2004).

391. EMERSON, *supra* note 70, at 76.

Emerson had in mind the same paradigmatic privacy case as his contemporary Prosser—the case against a newspaper for publishing private facts.³⁹² However, the data privacy cases envisioned by the First Amendment critics are in some respects the mirror image of what Emerson describes. In these cases, the First Amendment is being used as the screen, to infringe upon legitimate modes of government privacy regulation.

This Article has attempted to follow Emerson's advice in the modern context, arguing that when we subject both data privacy regulations and the First Amendment to careful scrutiny, they can be reconciled without sacrificing either. Furthermore, the real danger presented by the tension between privacy and the First Amendment is not that we must choose one over the other, but that we must instead avoid constitutionalizing important public law issues. Lurking behind the façade of seemingly neutral arguments by First Amendment critics is a theory of free speech and rights jurisprudence more generally that has the potential to topple the edifice of modern constitutionalism. If we do not reject such a theory, we may lose both our "genuine right of privacy" and our system of bifurcated review, under which civil and political rights are protected from legislatures, but economic rights generally are determined by the political process.

At the level of policy, however, resolving the conceptual problem does little to reduce the complexity of the database problem. Indeed, looking at the constitutional issues in the way I propose only allows policymakers to face the true challenges of the database problem and the regulation of information flows. Such a challenge likely will be as thorny in the information age as the problem of regulating industrial capitalism has been for over a century. And there are likely to be no easy answers to this new problem. In fact, in many instances freedom of information may well be the best policy; in others, privacy regulation may produce unacceptable social costs or be technically infeasible. Indeed, we may well determine that more privacy regulations are a really bad idea. However, this calculus should be made at the level of policy rather than at the abstract level of constitutional theory. Anything else would be inconsistent with the basic premises upon which modern rights jurisprudence rests.

392. See *supra* note 285.