

Michigan Telecommunications and Technology Law Review

Volume 9 | Issue 1

2002

Constitutional Issues in Information Privacy

Fred H. Cate

Indiana University School of Law-Bloomington

Robert Litan

Brookings Institution

Follow this and additional works at: <http://repository.law.umich.edu/mttlr>



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

Recommended Citation

Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35 (2002).

Available at: <http://repository.law.umich.edu/mttlr/vol9/iss1/2>

This Article is brought to you for free and open access by the Journals at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Telecommunications and Technology Law Review by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

CONSTITUTIONAL ISSUES IN INFORMATION PRIVACY

*Fred H. Cate**

*Robert Litan***

Cite as: Fred H. Cate and Robert Litan, *Constitutional Issues
in Information Privacy*,
9 MICH. TELECOMM. TECH. L. REV. 35 (2002),
available at <http://www.mttl.org/volnine/cate.pdf>

EXECUTIVE SUMMARY	36
INTRODUCTION—THE ABSENT CONSTITUTION.....	36
PART I. CONSTITUTIONAL CONTENDERS	39
A. <i>Constitutional Sources of a Privacy Right</i>	39
B. <i>Constitutional Limits on Protecting Privacy</i>	42
1. The Fourth Amendment.....	42
2. The Fifth Amendment	43
3. The Commerce Clause and the Tenth Amendment	46
4. The Nondelegation Doctrine	47
5. The Compact Clause	48
PART II. THE FIRST AMENDMENT.....	49
A. <i>The Dominance of Freedom of Expression</i>	49
B. <i>The Limited Role of Commercial Speech</i>	50
C. <i>The Problem of “Nonpublic” Uses</i>	52
D. <i>The First Amendment Applied to Privacy Contracts</i>	56
E. <i>Summary</i>	57
PART III. CONCLUDING OBSERVATIONS ABOUT THE CONSTITUTION AND THE PRIVACY DEBATE.....	58
A. <i>The Meaning of Privacy</i>	59
B. <i>The Range of Affected Parties</i>	60
C. <i>Privacy in Context</i>	61
D. <i>Privacy and Change</i>	61
E. <i>Public and Private Spheres</i>	62
CONCLUSION.....	62

* Professor of Law and Ira C. Batman Faculty Fellow at the Indiana University School of Law—Bloomington; senior fellow of the Hunton & Williams Center for Information Policy Leadership; and visiting scholar at the American Enterprise Institute. The authors thank Jean Walker for her able research assistance.

** Co-director of the AEI-Brookings Joint Center for Regulatory Studies, and Vice President and Director of the Economic Studies Program and Cabot Family Chair in Economics at the Brookings Institution; formerly associate director of the Office of Management and Budget, and deputy assistant attorney general, in charge of civil antitrust litigation and regulatory issues, at the Department of Justice.

EXECUTIVE SUMMARY

The U.S. Constitution has been largely ignored in the recent flurry of privacy laws and regulations designed to protect personal information from incursion by the private sector despite the fact that many of these enactments and efforts to enforce them significantly implicate the First Amendment. Questions about the role of the Constitution have assumed new importance in the aftermath of the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon. Recent efforts to identify and apprehend terrorists and to protect against future attacks threaten to weaken constitutional protections against government intrusions into personal privacy. However, these efforts vividly demonstrate the value of information collected in the marketplace and the need for such information in the future.

While there is some suggestion that the First Amendment may be a source of privacy rights applicable to the collection and use of personal information by the private sector,¹ it is clear that the First Amendment restrains the power of the government to enact and enforce privacy laws that curtail expression. The precise extent of that restraint depends on a number of factors, not all of which have been clearly resolved by the Supreme Court. But, as the events of September 11 starkly remind us, the price of privacy may be very high indeed. Legislators, regulators, and prosecutors who ignore the First Amendment when considering privacy laws threaten not only our constitutional rights, but our safety as well.

INTRODUCTION—THE ABSENT CONSTITUTION

The past five years have witnessed a surge in legislation, regulation, and litigation designed to protect the privacy of personal information. In 1998, Congress adopted legislation restricting the collection and use of information from children online,² and the following year enacted both the first comprehensive federal financial privacy legislation, as part of the Gramm-Leach-Bliley Financial Services Modernization Act,³ and the first federal law prohibiting access to historically open public records without individual “opt-in” consent.⁴ Federal regulators not only

1. See FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* 52–56 (1997) and sources cited therein.

2. Children’s Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (1999).

3. Gramm-Leach-Bliley Financial Services Modernization Act tit.V, 12 U.S.C. § 1811 (1999).

4. Driver’s Privacy Protection Act of 1994, 18 U.S.C. § 2721(b) (1994), *amended by* 18 U.S.C. § 2721(b)(11) (1999).

implemented these and other privacy laws, but also adopted sweeping health privacy rules under the Health Insurance Portability and Accountability Act⁵ (“HIPAA”) and negotiated a privacy “safe harbor” for U.S. companies seeking to comply with European privacy law.⁶ The Federal Trade Commission (“FTC”), under former Chairman Robert Pitofsky, reversed its longstanding position and released two proposals for legislation concerning adult online privacy.⁷ Newly installed Chairman Timothy Muris has promised renewed enforcement of existing privacy laws and policies, even while the FTC is re-examining its support for new privacy legislation.⁸ Furthermore, state legislatures have considered more than 400 privacy bills, while state attorneys general have initiated aggressive privacy investigations and litigation.

Largely absent from this surge in federal and state privacy efforts, and from the public and academic debate that has surrounded it, is any discussion of the role of the Constitution. Do public officials have the constitutional authority to restrict the collection and use of information by the private sector in an effort to protect privacy? Do those restrictions implicate the First Amendment and other provisions of the Bill of Rights that restrain government authority? Does the Constitution include a “right to privacy” outside of the context of *government* intrusions? These and many other related questions remain unanswered and are not even addressed in the current privacy debate. However, their resolution goes to the very heart of the government’s power to adopt and enforce laws designed to protect privacy.

These questions have assumed new importance in the aftermath of terrorist attacks on the World Trade Center and the Pentagon. Many observers worry that one long-term effect of the attacks may be to weaken the considerable constitutional protection against government invasions of personal privacy. At the same time, efforts to identify and

5. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 164.502, 164.506 (2000) (final rule); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776 (2002) (HHS, proposed rule, modification); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 43,181 (2002) (HHS, final rule) (to be codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

6. Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000), *available at* <http://www.export.gov/safeharbor/>.

7. FEDERAL TRADE COMM’N, ONLINE PROFILING: A REPORT TO CONGRESS (PART 2)—RECOMMENDATIONS (July 2000); FEDERAL TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS (May 2000).

8. Timothy J. Muris, Protecting Consumers’ Privacy: 2002 and Beyond, Remarks at the Privacy 2001 Conference, Cleveland, Ohio (Oct. 4, 2001), *available at* <http://www.ftc.gov/speeches/muris/privisp1002.htm>.

bring to justice the perpetrators and to protect against future terrorist attacks also vividly demonstrate the value of information collected in the marketplace and the need for such information in the future. To the extent that a “right to privacy” limits the availability of that information, the price of privacy may be very high indeed. As a result, there is a new urgency to determine what the Constitution allows—or requires—with regard to information collection and its use by the private sector.

This Article begins the process of remedying the failure of the policymaking debate to address the role of the Constitution in privacy protection. The Article grew out of a one-day roundtable, hosted by the AEI-Brookings Joint Center for Regulatory Studies in Washington in May 2001. The roundtable brought together constitutional law scholars, economists, privacy advocates, privacy theorists, prominent current and former government officials, and leading privacy law practitioners for a free-wheeling discussion of constitutional issues in information privacy.⁹ The participants addressed the major constitutional provisions that might be applicable to the government’s power to protect privacy from private-sector encroachment, as well as a number of related issues. This Article seeks to capture, and build on, the key substantive issues the participants discussed and the general conclusions they reached, in an effort to further the inquiry into the role of the Constitution in the on-going privacy debate.

Section II provides an overview of the constitutional provisions likely to create or restrict a privacy right applicable to the collection, use,

9. The participants at the Joint Center roundtable were, in addition to the authors: Marty Abrams, Executive Director, Hunton & Williams Center for Information Policy Leadership; Sarah Andrews, Research Director, Electronic Privacy Information Center; Paula Bruening, Staff Counsel, Center for Democracy and Technology; Becky Burr, Partner, Wilmer, Cutler & Pickering; formerly Associate Administrator and Director of International Affairs, National Telecommunications and Information Administration; Amitai Etzioni, University Professor, The George Washington University; founder and Director, The Communitarian Network; Peter Gray, Internet Consumers Organization; Robert W. Hahn, Co-director, AEI-Brookings Joint Center for Regulatory Studies; Resident Scholar, American Enterprise Institute; Oliver Ireland, Of Counsel, Morrison & Foerster LLP; formerly Associate General Counsel for Monetary and Reserve Bank Affairs, Board of Governors of the Federal Reserve System; Duncan MacDonald, formerly General Counsel, European and North American Card Products, Citibank; Adam Clayton Powell, III, Vice President of Technology and Programs, The Freedom Forum; the Hon. Bill Pryor, Attorney General, Alabama; Joel Reidenberg, Professor of Law, Fordham University; Paul Rubin, Professor of Law and Economics, Emory University; formerly Senior Economist, Council of Economist Advisors, and Chief Economist, U.S. Products Safety Commission; Paul Schwartz, Professor of Law, Brooklyn Law School; Peter Swire, Professor of Law, Ohio State University; formerly Chief Counselor for Privacy, Office of Management and Budget; Eugene Volokh, Professor of Law, UCLA; and Alan Westin, Professor of Public Law and Government Emeritus, Columbia University, Co-founder and Publisher, *Privacy & American Business*.

and transfer of personal information in the private sector. Section III focuses on the role of the First Amendment, the constitutional provision most likely to be implicated by such privacy laws. Section IV offers some general observations about, and tensions implicit in, efforts to use law to protect the privacy of personal information. The Article concludes that while there is a suggestion that the First Amendment may be a source of privacy rights applicable to the collection, use, and transfer of personal information by the private sector, it is clear that the First Amendment restrains the power of the government to enact and enforce privacy laws that curtail expression, even when that expression involves personal information. The precise extent of that restraint depends on a number of factors, not all of which have been clearly resolved by the Supreme Court. But the failure of legislators, regulators, and prosecutors to scrutinize privacy laws under the First Amendment calls into question the constitutionality of those laws and disserves the values that the First Amendment protects.

PART I. CONSTITUTIONAL CONTENDERS

Efforts to adopt and enforce legal restrictions on the collection and use of information by the private sector in an effort to protect privacy potentially implicate several provisions of the U.S. Constitution.

A. *Constitutional Sources of a Privacy Right*

In 1965, the Supreme Court decided in *Griswold v. Connecticut* that an 80-year-old Connecticut law forbidding the use of contraceptives violated the constitutional right to “marital privacy.”¹⁰ Justice Douglas, writing for the Court, identified a variety of constitutional sources for this right:

Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one. . . . The Third Amendment in its prohibition against the quartering of soldiers “in any house” in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone

10. 381 U.S. 479 (1965).

of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.”¹¹

Justice Douglas wrote that the “specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.”¹² It was in these penumbras that the Court grounded constitutional protection for the right to marital privacy and, in subsequent cases, other privacy rights.

Constitutional privacy rights, as with virtually all constitutional rights, have been applied to protect against intrusion only by the *government*. For example, courts interpret the Fourth Amendment to apply only to searches and seizures by the government, usually in a criminal context. Some commentators, however, have argued that the existence of a constitutional right to privacy may allow, or require, the government to enact laws to restrict the collection and use of personal information by the *private sector*. The preamble to the recent HIPAA health privacy rules,¹³ for example, discusses at length the Fourth Amendment right to be free from “unreasonable searches and seizures” by the government and the right to protect some information from mandatory disclosure to the government, as recognized by the Supreme Court in *Whalen v. Roe*,¹⁴ as justifications for rules regulating health-related information in the private sector. The effect of such arguments is to extend to the private sector constitutional obligations previously applicable only to the government.

To date, there is little judicial support for this position. Historically, while the Supreme Court on occasion has addressed citizens’ interest in privacy from nongovernmental intrusion, it almost never identifies the Constitution as the source of that interest. Instead the Supreme Court looks to statutory or common law. In fact, the Court has intimated a constitutional right applicable to private-sector acquisition or use of personal information only twice. In *Harper & Row Publishers, Inc. v. Nation Enterprises*,¹⁵ a case involving the “scooping” of President Ford’s memoirs by the *Nation* magazine prior to their publication by Harper & Row, the Court quoted a New York state appellate judge for the proposition:

11. *Id.* at 484.

12. *Id.*

13. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (2000) (HHS, final rule).

14. 429 U.S. 589 (1977).

15. 471 U.S. 539 (1985).

The essential thrust of the First Amendment is to prohibit improper restraints on the voluntary public expression of ideas; it shields the man who wants to speak or publish when others wish him to be quiet. There is necessarily, and within suitably defined areas, a concomitant freedom not to speak publicly, one which serves the same ultimate end as freedom of speech in its affirmative aspect.¹⁶

The Supreme Court used this quote to help justify, in part, why it was not expanding the copyright doctrine of fair use to provide an affirmative First Amendment right to publish newsworthy expression without regard for its copyright. The Court concluded that the *Nation's* unauthorized use of Harper's unpublished manuscript was not sanctioned by the copyright law's fair use doctrine. The issue before the Court was whether the First Amendment required a broader reading of the fair use doctrine, not the right to privacy.

In May 2001, however, the Court quoted this same language for the first, and only, time in a case involving privacy. In *Bartnicki v. Vopper*, decided after the Joint Center Roundtable, the Supreme Court faced the question of whether the broadcast of an illegally intercepted cellular telephone conversation was protected by the First Amendment.¹⁷ The Court repeated the same passage it had quoted in *Harper & Row* 16 years earlier to demonstrate that “[p]rivacy of communication is an important interest.”¹⁸ Nevertheless, the Court found that the First Amendment protected playing the conversation on-the-air because the information at issue was true, was on a matter of public concern, and was obtained by a third party without the knowledge or participation of the radio station that subsequently disclosed it. The privacy interest noted by the Court was insufficient to overcome the free expression interest even in the context of an illegally intercepted telephone conversation.

Whether the Constitution protects individuals' interests in avoiding collection and use of information about them by private-sector entities is a critical question, but *Bartnicki* is a slender basis for such a claim. Whether the case will prove to mark the first step in the beginning of a real change in the Court's thinking, or whether it is merely an aberration, remains to be seen. This brief reference is the only support for the claim

16. *Id.* at 559 (quoting *Estate of Hemingway v. Random House, Inc.*, 23 N.Y.2d 341, 348, 244 N.E.2d 250, 255 (Ct. App. 1968)).

17. 532 U.S. 514, 535 (2001).

18. *Id.* at 532.

that the Constitution creates a right to privacy applicable to the private sector or protects individuals' privacy from nongovernmental intrusion.

B. *Constitutional Limits on Protecting Privacy*

Because the Constitution establishes the powers of the government and also the limits on those powers, it is not surprising that there are many constitutional provisions that might limit the government's ability to adopt and enforce laws protecting privacy. The most obvious—and, in the view of the participants in the Joint Center Roundtable, the most significant—provisions the First Amendment's protection for freedom of expression. Before turning to the First Amendment, however, we briefly address the six other provisions that the participants discussed and that most concluded were unlikely to impose any substantive limit on the government's power to protect information privacy.

1. The Fourth Amendment

The Fourth Amendment is the basis for the Supreme Court's oldest and most well-developed jurisprudence on a constitutional right to privacy. Although, as noted in the introduction, Fourth Amendment cases involve searches and seizures by the government, the principles developed there might potentially be instructive in other settings. For example, when evaluating wiretaps and other seizures of private information, the Court has protected only those expectations of privacy that were, in the Court's view, "reasonable." The data subject must have actually expected that the information was private, and that expectation must be "one that society is prepared to recognize as 'reasonable.'"¹⁹ The Court adopted this two-part test in 1968 and continues to apply it today, albeit with somewhat uneven results.²⁰

Some courts have borrowed from Fourth Amendment jurisprudence when evaluating privacy restrictions in other settings. For example, in

19. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (attaching a recording device to a public telephone booth without a warrant did not violate petitioner's Fourth Amendment rights).

20. *See Smith v. Maryland*, 442 U.S. 735, 740 (1979) (use of a pen register without a warrant to record telephone numbers dialed did not violate petitioner's Fourth Amendment rights); *Terry v. Ohio*, 392 U.S. 1, 9 (1968) (warrantless search of petitioner's person for concealed weapons did not violate petitioner's Fourth Amendment rights); *CATE*, *supra* note 1, at 58 (the Court has found "reasonable" expectations of privacy in homes, businesses, sealed luggage and packages, and even drums of chemicals, but no "reasonable" expectations of privacy in bank records, voice or writing samples, phone numbers, conversations recorded by concealed microphones, and automobile passenger compartments, trunks, and glove boxes).

Condon v. Reno,²¹ the U.S. Court of Appeals for the Fourth Circuit focused on the “reasonable expectation of privacy” in its decision striking down the 1994 Drivers Privacy Protection Act.²² In that case, South Carolina Attorney General Charlie Condon argued that a federal restriction on the use of state public record data for “marketing, solicitation, or survey” purposes violated the First Amendment. The appellate court agreed, writing that “neither the Supreme Court nor this Court has ever found a constitutional right to privacy with respect to the type of information found in motor vehicle records. Indeed, this is the very sort of information to which individuals do not have a reasonable expectation of privacy.”²³ The court found that it would be unreasonable to prevent the disclosure of such information because “the same type of information is available from numerous other sources. . . . As a result, an individual does not have a reasonable expectation that the information is confidential.”²⁴ The Supreme Court ultimately reversed the Fourth Circuit on unrelated grounds, and therefore never reached the First Amendment issue.²⁵ Few other courts have relied on Fourth Amendment concepts or cases when evaluating privacy protections aimed at nongovernmental intrusions.

As a result, while the Fourth Amendment could prove to be important as a source of principles for evaluating privacy laws regulating private sector activities, it has not played that role to date. Furthermore, the contours of the Fourth Amendment itself are under renewed scrutiny following the September 11 terrorist attacks and subsequent proposals for increased government surveillance, national identification numbers, and passenger profiling.

2. The Fifth Amendment

The Fifth Amendment to the U.S. Constitution prohibits the government from taking private property for public use without both due process of law and just compensation. Historically, the Supreme Court has applied the “takings clause” to require compensation when the government physically appropriated real property, even if only a tiny portion of the property at issue was occupied,²⁶ or if that occupation was

21. *Condon v. Reno*, 155 F.3d 453 (4th Cir. 1998), *rev'd on other grounds*, 528 U.S. 141 (2000).

22. Drivers Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (1994).

23. *Id.* at 464.

24. *Id.* at 465.

25. *Reno v. Condon*, 528 U.S. 141 (2000).

26. *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419 (1982) (explaining that only 1.5 cubic feet of private property is occupied).

only temporary.²⁷ Beginning in 1922, however, the Court has found a compensable taking even when the government does not engage in physical occupation²⁸ and when the property involved is not land or even tangible property, but rather a legal entitlement,²⁹ government benefit,³⁰ or interest in continued employment.³¹

In 1984, the Supreme Court decided *Ruckelshaus v. Monsanto Company*, in which it extended the Fifth Amendment takings clause to protect stored data.³² The Court found that the Environmental Protection Agency's use of proprietary research data that Monsanto was required by regulation to disclose constituted a compensable taking. The Court in *Ruckelshaus*, as in all regulatory takings cases, faced two fundamental questions: whether there was "property" and, if so, whether it was "taken" by the government's action. The first question presented little difficulty, because state law recognizes a property right in "trade secrets" and other confidential business information, and the possessors of such data have long been accorded property-like rights to control access to, and the use of, business information. To answer the second question, the Court focused on Monsanto's "reasonable investment-backed expectation with respect to its control over the use and dissemination of the data," finding that Monsanto had invested substantial resources in creating the data and reasonably believed that the EPA would keep the information secret.³³

The Supreme Court's recognition of this "regulatory taking"—including the taking of stored data—could suggest that privacy regulations that substantially interfere with a private party's use of data that it has collected or processed may require compensation under the Fifth Amendment. As applied to personal information collected in the private sector, even if a privacy law interfered with a "reasonable investment-backed expectation with respect to its control over the use and dissemination of the data," it seems unlikely that a court would find

27. *First English Evangelical Lutheran Church of Glendale v. County of Los Angeles*, 482 U.S. 304 (1987) (denying plaintiff temporary use of his property constitutes a taking requiring just compensation).

28. *Pennsylvania Coal Co. v. Mahon*, 260 U.S. 393 (1922) (finding that the state abrogated the right to remove coal from property).

29. *Logan v. Zimmerman Brush Co.*, 455 U.S. 422 (1982) (property interest in statutorily created cause of action for discrimination against the disabled); *U.S. Trust Co. v. New Jersey*, 431 U.S. 1 (1977) (property interest in common law contract rights).

30. *Mathews, Sec'y of Health, Educ., and Welfare v. Eldridge*, 424 U.S. 319 (1976) (determining plaintiff has a property interest in Social Security benefits).

31. *Perry v. Sindermann*, 408 U.S. 593 (1972) (determining plaintiff has a property interest in continued employment).

32. 467 U.S. 986 (1984).

33. *Id.* at 1011.

that the data user or collector had the requisite “property” interest in the information. *Ruckelshaus* involved trade secrets, which courts have long treated as property, while most privacy laws affect information that is not clearly property owned by anyone, and certainly not clearly owned by a third party data collector or user. In addition, even if this obstacle to a takings claim were overcome, it ordinarily would be difficult to demonstrate that the interference with the ability to use or disclose the information was sufficiently great to constitute a taking.

Finally, even when a government regulation deprives a property owner of all use of his property, the Supreme Court has historically declined to find a taking, and therefore not required compensation, when the regulation merely abated a “noxious use” or “nuisance-like” conduct. Such a regulation does not constitute a taking of private property, because one never has a property right to harm others.³⁴ Laws restricting the use of personal information to protect privacy, it could be argued, are simply preventing a “noxious use” of the data.

In 1992, the Supreme Court retreated somewhat from the “prevention of harmful use” exception, recognizing that the government could virtually always claim that it was regulating to prevent a harmful use.³⁵ Nevertheless, the Court permits the government to adopt regulations depriving property “of all economically beneficial use,” provided that the government can show that its power to promulgate the regulation inheres in the “background principles of the State’s law of property and nuisance.”³⁶ Privacy advocates would likely argue that this is the case with privacy laws: if personal data are to be treated as property, then the state has the inherent power to prevent their being used to cause a nuisance to the data subject.

Given the substantial uncertainty over whether personal information may be considered the property of a third party, and the difficulty of demonstrating both that a regulation poses a sufficiently great interference with a “reasonable investment-backed expectation” and that the interference was not necessary to abate a generally harmful use of that information, the roundtable participants doubted whether the takings clause is likely to play a significant role in future privacy litigation.

34. See Jan G. Laitos, *The Takings Clause in America’s Industrial States After Lucas*, 24 U. Tol. L. Rev. 281, 288 (1993).

35. *Lucas v. South Carolina Coastal Council*, 505 U.S. 1003, 1026 (1992).

36. *Id.* at 1027, 1029.

3. The Commerce Clause and the Tenth Amendment

Two key issues concern Congress' constitutional authority to legislate to protect privacy. The first is grounded in the Commerce Clause.³⁷ Is enacting privacy laws a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause? The other constitutional issue is raised by the Tenth Amendment, which reserves to the states and to the people all powers not explicitly granted in the Constitution to the federal government. Under the Supreme Court's somewhat convoluted Tenth Amendment jurisprudence, Congress can neither compel a state to enact or enforce a federal regulatory program nor achieve the same result by conscripting the state's officers directly. The Tenth Amendment is, therefore, implicated when the federal government prescribes privacy standards that state and local governments must enact or enforce.

Both issues were raised explicitly in the privacy context in *Reno v. Condon*,³⁸ discussed above, in which South Carolina challenged Congress' authority to pass the Drivers Privacy Protection Act—a federal law that mandated that states restrict access to motor vehicle record information. The Supreme Court, by a unanimous vote, rejected the state's Commerce Clause and Tenth Amendment challenges to the statute.

With regard to the Commerce Clause argument, the Court concluded that the law was within Congress' power under the Commerce Clause because (1) motor vehicle information is "used by insurers, manufacturers, direct marketers, and others engaged in interstate commerce;" (2) that information is also "used in the stream of interstate commerce by various public and private entities for matters related to interstate motoring;" and (3) "drivers' information is, in this context, an article of commerce" sold or released into the "interstate stream of business."³⁹

The Supreme Court rejected the Tenth Amendment challenge on the basis that the Act "does not require the States in their sovereign capacity to regulate their own citizens" in the furtherance of a federal regulatory scheme; rather it regulates the states themselves, "as the owners of databases."⁴⁰ This distinction is critical, because the Court had previously held that laws that "regulated state activities," rather than "seeking to control or influence the manner in which States regulate private parties"

37. U.S. CONST. art. I, § 8, cl. 3.

38. 528 U.S. 141 (2000).

39. *Id.* at 148.

40. *Id.* at 151.

were permissible under the Tenth Amendment.⁴¹ As a result, the Supreme Court dismissed the Tenth Amendment challenge to the DPPA.

The breadth of the Court's opinion led most of the participants in the roundtable to conclude that the Court is very likely to find that future privacy laws are within Congress' power and not susceptible to challenges based on the Commerce Clause or the Tenth Amendment.

4. The Nondelegation Doctrine

The roundtable participants also considered and rejected another possible challenge to Congress' authority to enact privacy protections. Article I, Section 1 of the Constitution provides that "All legislative Powers shall be vested in a Congress."⁴² The "nondelegation doctrine" provides that a legislature may not generally confer upon another branch of government or an administrative body broad legislative power; instead, the legislature must provide some degree of direction and some limit on the agency's discretion.⁴³ Some commentators have argued that the privacy provisions of HIPAA violated the nondelegation doctrine by specifying that if Congress failed to enact health privacy rules, the Department of Health and Human Services ("HHS") was to do so.⁴⁴ If Congress engaged in an unconstitutional delegation of its legislative power, then the health privacy rules issued by HHS in December 2000 would likely be unconstitutional.⁴⁵ In July, the South Carolina and Louisiana Medical Societies filed a suit challenging the constitutionality of the health privacy rules on nondelegation, as well as other, grounds.⁴⁶

The success of any nondelegation challenge seems doubtful following the Supreme Court's February 2001 decision in *Whitman v. American Trucking Associations*.⁴⁷ There the Court addressed a nondelegation challenge in another context and concluded, 7-2, that Congress had not violated the doctrine when it delegated extensive rulemaking authority to the Environmental Protection Agency. The

41. *South Carolina v. Baker*, 485 U.S. 505(1988) (upholding a federal law prohibiting states from issuing unregistered bonds).

42. U.S. CONST. art. I, § 1.

43. *Mistretta v. United States*, 488 U.S. 361 (1989).

44. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C.A. § 1320d-3(a) (1996). See generally A. Craig Eddy, *A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of The Health Insurance Privacy and Accountability Act of 1996*, 9 ANNALS HEALTH L. 1 (2000).

45. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

46. *South Carolina Medical Ass'n v. U.S. Dep't of Health and Human Services* (D.S.C. filed July 18, 2001).

47. 531 U.S. 457 (2001).

breadth and recency of the Court's ruling led most of the roundtable participants to believe that a nondelegation doctrine challenge to the health privacy rules issued under the HIPAA would be unlikely to succeed; the barest direction from Congress to administrative agencies is apparently sufficient under Article 1, Section 1.

5. The Compact Clause

The Compact Clause was the final constitutional provision that the participants in the Joint Center roundtable considered and rejected as only remotely implicated by the adoption and enforcement of privacy rules. The Compact Clause provides that “[n]o state shall, without the consent of Congress, . . . enter into any agreement or compact with another state, or with a foreign power”⁴⁸ Compared to the other constitutional provisions outlined above, the Compact Clause has been the subject of little judicial discussion. As a general matter, the Supreme Court has held that the application of the Compact Clause is limited to agreements that increase the power of the states such that the combined state's power impinges on the “just supremacy of the United States.”⁴⁹ Thus the relevant question is the impact of the agreement on the “federal structure.”⁵⁰ Some commentators have suggested that the recent trend by states attorneys general to band together in common investigations, litigation, and settlements concerning the privacy practices of banks, pharmaceutical companies, and other institutions reflect a compact among states that is prohibited if not sanctioned by Congress.

The Compact Clause is unlikely to be implicated by these actions because they merely involve the common management of litigation, an activity routinely pursued by state attorneys general collectively, rather than the states acting pursuant to a compact to increase their political power vis-à-vis Congress or other states.⁵¹

By the conclusion of the roundtable, most of the participants had reached the conclusion that whatever the relevance of these six constitutional provisions—the Fourth and Fifth Amendments, the Commerce Clause, the Tenth Amendment, the nondelegation doctrine, and the Compact Clause—none appear likely to impose any practical limit on the government's power to adopt and enforce laws designed to restrict the collection and use of personal information by the private

48. U.S. CONST. art. I, § 10, cl. 3.

49. *United States Steel Corp. v. Multistate Tax Comm'n*, 434 U.S. 452, 471 (1978).

50. *Id.* at 478.

51. See *Cuyler v. Adams*, 449 U.S. 433 (1981); *Virginia v. Tennessee*, 148 U.S. 503 (1893).

sector. This may not be the case in the future, but it appears to be the case today for all practical purposes.

However, the situation appears to be very different for the First Amendment, and it is this constitutional provision to which we now turn.

PART II. THE FIRST AMENDMENT

A. *The Dominance of Freedom of Expression*

The First Amendment is not only a potential source—albeit a weak one—of privacy rights, as discussed above,⁵² but also a significant restraint on the government's power to restrict the publication or communication of information. The Supreme Court has decided many cases in which individuals sought to stop, or obtain damages for, the publication of private information, or in which the government restricted expression in an effort to protect privacy. Virtually without exception, the Court has upheld the right to speak or publish or protest under the First Amendment, to the detriment of the asserted privacy interest. For example, the Court has rejected privacy claims by unwilling viewers or listeners in the context broadcasts of radio programs in city streetcars,⁵³ R-rated movies at a drive-in theater,⁵⁴ and a jacket bearing an the phrase "Fuck the Draft" worn in the corridors of a courthouse.⁵⁵ The Court has struck down ordinances that would require affirmative opt-in consent before receiving door-to-door solicitations,⁵⁶ Communist literature,⁵⁷ or even "patently offensive" cable programming.⁵⁸

Plaintiffs rarely win suits brought against speakers or publishers for disclosing private information. When information is true and lawfully obtained, the Supreme Court has repeatedly held that "strict scrutiny"—the highest level of constitutional scrutiny—applies and, thus, the government may not restrict its disclosure without showing a narrowly tailored, compelling governmental interest. Under this requirement, the Court has struck down laws restricting the publication of confidential

52. *See supra* Part I.A.

53. *Pub. Utilities Comm'n v. Pollack*, 343 U.S. 451 (1952).

54. *Erznoznik v. City of Jacksonville*, 422 U.S. 205 (1975).

55. *Cohen v. California*, 403 U.S. 15 (1971).

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

57. *Lamont v. Postmaster General*, 381 U.S. 301 (1965).

58. *Denver Area Educ. Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727 (1996).

government reports,⁵⁹ and names of judges under investigation,⁶⁰ juvenile suspects,⁶¹ and rape victims.⁶²

Even when the information is false, the Supreme Court has been loathe to allow restrictions on its collection and dissemination. Under the Court's interpretation of the First Amendment, plaintiffs cannot recover for the harm caused by the publication of false and defamatory expression—if that expression is on a matter of public interest—unless the plaintiff can prove its falsity.⁶³ Public officials and public figures may not recover for damage caused by false expression, no matter how personal, unless they can demonstrate with “convincing clarity” that the publisher knew of the falsity or was reckless concerning it.⁶⁴ The Court has eliminated entirely any recourse by public plaintiffs for the publication of true information, even if highly defamatory or personal.⁶⁵

The historical dominance of the free expression interests over the privacy interests is so great that Peter Edelman has written:

[T]he Court [has] virtually extinguished privacy plaintiff's chances of recovery for injuries caused by truthful speech that violates their interest in nondisclosure. . . . If the right to publish private information collides with an individual's right not to have that information published, the Court consistently subordinates the privacy interest to the free speech concerns.⁶⁶

B. *The Limited Role of Commercial Speech*

Free expression has trumped privacy under the First Amendment irrespective of whether the speaker is an individual or an institution. Beginning in 1976, when the Supreme Court first extended the protection of the First Amendment to wholly commercial expression, the judicial system recognized that readily available information and the legal right to express it are critical to the functioning of competitive markets. In *Virginia State Board of Pharmacy v. Virginia Citizens*

59. See *New York Times Co. v. United States*, 403 U.S. 713 (1971).

60. See *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978).

61. See *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97 (1979).

62. See *Florida Star v. B.J.F.*, 491 U.S. 524 (1989); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975).

63. See *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767 (1986).

64. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974); *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).

65. *Monitor Patriot Co. v. Roy*, 401 U.S. 265 (1971).

66. Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 *TEX. L. REV.* 1195, 1198 (1990).

Consumer Council, Inc.,⁶⁷ the Court struck down a Virginia statute that prohibited the advertising of pharmaceutical prices, the Court wrote:

It is clear . . . that speech does not lose its First Amendment protection because money is spent to project it, as in a paid advertisement of one form or another. Speech likewise is protected even though it is carried in a form that is “sold” for profit, and even though it may involve a solicitation to purchase or otherwise pay or contribute money. . . . [T]he particular consumer’s interest in the free flow of commercial information . . . may be as keen, if not keener by far, than his interest in the day’s most urgent political debate.⁶⁸

The Court has found that wholly commercial expression, if about lawful activity and not misleading, is protected from government intrusion unless the government can demonstrate a “substantial” public interest, and that the intrusion “directly advances” that interest and is “narrowly tailored to achieve the desired objective.”⁶⁹

Moreover, the Court does not subject government regulations of expression to intermediate scrutiny just because the speech occurs in a commercial context. The speech of corporations is routinely accorded the highest First Amendment protection, “strict scrutiny” standard, unless the Court finds that the purpose of the expression is to propose a commercial transaction⁷⁰ or that the expression occurs in the context of a highly regulated industry or market (such as the securities exchanges), where the regulation of expression is essential to the government’s regulatory objectives.⁷¹

Even if the expression is “commercial,” the Court requires that the government demonstrate that “the harms it recites are real” and that “its restriction will in fact alleviate them to a material degree.”⁷² As a result, to the extent that privacy laws restrict expression, even if that expression is commercial, the First Amendment imposes a considerable burden on the government to demonstrate the need and effectiveness of those laws.

67. 425 U.S. 748 (1976).

68. *Id.* at 761–63 (omitting footnote and citations).

69. *Board of Trs. v. Fox*, 492 U.S. 469, 480 (1989); *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 566 (1980).

70. *Central Hudson*, 447 U.S. 557.

71. *Lowe v. Sec. & Exch. Comm’n*, 472 U.S. 181 (1985). See generally 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 (2000).

72. *Edenfield v. Fane*, 507 U.S. 761, 770–71 (1993).

C. The Problem of "Nonpublic" Uses

Virtually all of the Supreme Court's cases involving the tension between the First Amendment's protection for expression and an individual's interest in privacy involve the publication of information in which there is legitimate public interest. An important and unresolved issue is how the Court, when balancing privacy and freedom of expression, will weigh the First Amendment interest in expression that does not involve the public interest or that is not being disclosed to the public.

This issue was highlighted, but not resolved, in the recent case of *Bartnicki v. Vopper*,⁷³ discussed above, in which the Supreme Court reasserted, and perhaps even expanded, the dominance of free expression interests. There the Court explicitly balanced the constitutional interests in privacy and expression, and held that the broadcast of an illegally intercepted cellular telephone conversation was protected by the First Amendment. The Court quoted from its earlier cases on the importance of expression:

Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press. "Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period."⁷⁴

As this suggests, the Court in *Bartnicki* based its holding on the fact that the intercepted cellular telephone conversation involved a matter of public interest—labor negotiations over public school teacher salaries. It is not clear how the Court will weigh the First Amendment interest in expression that does not involve publication or expression on a matter of public interest.

In 1985, in *Dun & Bradstreet v. Greenmoss Builders*, the Supreme Court determined that the considerable constitutional obstacles to allowing plaintiffs to recover for false and defamatory expression in the mass media did not apply where the defamation occurred in a credit report distributed under a confidentiality agreement to only five

73. See 532 U.S. 514 (2001).

74. *Id.* at 534 (quoting *Time, Inc. v. Hill*, 385 U.S. 374, 388 (1967) (quoting *Thornhill v. Alabama*, 310 U.S. 88, 102 (1940))).

subscribers.⁷⁵ Although a majority of the Justices could not agree on a single rationale for their decision, a majority seemed to share the view that the First Amendment interest in expression on matters of private concern is less than that for matters of public concern.

However, it must be remembered that *Dun & Bradstreet* involved false speech and a claim of harm resulting from the falsity, where privacy cases by definition involve true speech and claims of harm resulting from the truth of the information collected or disclosed. The Court went out of its way to clarify that its decision was not intended to reduce the First Amendment protection afforded to commercial or economic expression: “We also do not hold . . . that the report is subject to reduced constitutional protection because it constitutes economic or commercial speech.”⁷⁶

Moreover, in *Bartnicki*, while focusing on the fact that the expression at issue did concern a matter of great public interest, the Court nevertheless added in a footnote: “Moreover, ‘our decisions establish that absent exceptional circumstances, reputational interests alone cannot justify the proscription of truthful speech,’” citing to a long line of prior decisions.⁷⁷ This suggests that even expression not on a matter of public importance, if truthful, would be constitutionally difficult to restrain.

This was certainly the view of the U.S. Court of Appeals for the Tenth Circuit when presented with a First Amendment challenge to Federal Communications Commission rules that required U.S. West to get “opt-in” consent from customers before using data about their calling patterns to determine which customers to contact or what offer to make them.⁷⁸ The appellate court, 2–1, found that the FCC’s rules, by limiting the use of personal information when communicating with customers, restricted U.S. West’s speech and therefore were subject to First Amendment review. Although the court applied intermediate scrutiny, it determined that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a “specific and significant harm” to individuals, and that the rules were “‘no more extensive than necessary to serve [the stated] interest[s].’”⁷⁹

75. *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 763 (1985).

76. *Id.* at 762 n.8.

77. 532 U.S. at 534 n.21 (quoting *Butterworth v. Smith*, 494 U.S. 624, 634 (1990)).

78. *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999), *cert. denied*, 528 U.S. 1188 (2000).

79. *See id.* at 1238 (quoting *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 486 (1995)).

Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under *Central Hudson* [the test applicable to commercial speech] for it is not based on an identified harm.⁸⁰

The court found that for the Commission to sufficiently demonstrate that the “opt-in” rules were narrowly tailored, it must prove that less restrictive “opt-out” rules would not offer sufficient privacy protection, and it must do so with more than mere speculation:

Even assuming that telecommunications customers value the privacy of [information about their use of the telephone], the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.⁸¹

The court found that the FCC had failed to show why more burdensome “opt-in” rules were necessary, and therefore struck down the rules as unconstitutional. The fact that the information was being used for purposes other than publication was irrelevant. The Supreme Court declined to review the case.⁸²

The Supreme Court has not yet decided a case in which a party sought to apply the First Amendment to overturn a privacy law or regulation that restricted the *private-interest use* of truthful personal information in the market, but did not otherwise restrain publication or public expression. It is therefore unclear how the Court might evaluate the constitutionality of such a law.

The Court came close to addressing such a situation in two recent cases involving privacy laws, but for important reasons neither case was directly on point. They may nevertheless be instructive.

80. *Id.* at 1235.

81. *Id.* at 1239.

82. *U.S. West, Inc. v. FCC*, 528 U.S. 1188 (2000).

In the first case, *Los Angeles Police Department v. United Reporting*, the Court upheld the constitutionality of a California law that prohibited the release of arrestee addresses to anyone, unless permitted by the statute, for the purpose of using the information to sell a product or service.⁸³ In the Court's discussion of whether the statute was subject to "facial" challenge under the First Amendment, Chief Justice Rehnquist wrote:

This is not a case in which the government is prohibiting a speaker from conveying information that the speaker already possesses. The California statute in question merely requires that if respondent wishes to obtain the addresses of arrestees it must qualify under the statute to do so. Respondent did not attempt to qualify and was therefore denied access to the addresses. For purposes of assessing the propriety of a facial invalidation, what we have before us is nothing more than a governmental denial of access to information in its possession.⁸⁴

And that "denial of access," in the Court's view, raised no constitutional issues. In fact, the Court wrote, "California could decide not to give out arrestee information at all without violating the First Amendment."⁸⁵ This did little more than restate the Court's longstanding position that the First Amendment does not give rise to a general right to access information held by the government. By focusing on the "facial" nature of the challenge, and by construing the case as a case involving *access to government* information, the Court avoided addressing the question of whether a similar limit on using information obtained from nongovernmental sources would be constitutional under the First Amendment.

In the second case, *Reno v. Condon*, discussed above, the Court upheld the constitutionality of the Drivers Privacy Protection Act, a law requiring states to restrict the disclosure of personal information contained in motor vehicle records.⁸⁶ The unanimous Court, in its discussion of whether the Commerce Clause gave Congress the authority to adopt the law, wrote that "the personal, identifying information that the DPPA regulates is a 'thing in interstate commerce,'" and referred to that information throughout its opinion simply as "an article in interstate

83. *Los Angeles Police Dep't v. United Reporting Publ'g Corp.*, 528 U.S. 32 (1999).

84. *Id.* at 40 (citations omitted).

85. *Id.*

86. 528 U.S. 141 (2000).

commerce,”⁸⁷ like a truckload of coal or steel. This case involved no First Amendment challenge at all and, even if it had, the Court would likely have treated it as another “access to government information” case.

As a result, neither of these cases is directly on point. Moreover, both were decided on fairly technical issues concerning the availability of facial challenges and the power of Congress under the Commerce Clause and the Tenth Amendment. But it is nonetheless important to note that in both cases the Court demonstrated no special solicitude for the fact that information was involved, but instead almost casually dismissed the information in question as just another “thing” that legislatures may regulate. This stands in stark contrast to the considerable protection that the Court has interpreted the First Amendment as applying to expression, so there is some confusion as to the Court’s future direction when faced with direct First Amendment challenges to privacy statutes.

D. *The First Amendment Applied to Privacy Contracts*

Another important First Amendment issue is the extent to which the First Amendment is implicated by privacy agreements such as contracts or privacy policies. Because they are agreements between private parties, contracts are usually thought to raise few if any constitutional issues. However, the government often provides procedural or default rules for contracts and the question of whether it is constitutionally free to do so in the privacy arena generated considerable debate.

For example, may the government constitutionally require that consumer consent to privacy contracts be manifest in writing or through some other mechanism indicating explicit, “opt-in” consent? The answer is not clear, but appears to turn on how burdensome those requirements would be to expression. In *Cohen v. Cowles Media Company*, for example, the Supreme Court faced the question of whether a newspaper should pay damages for failing to keep its promise to a confidential source not to disclose his identity, even though those damages would undoubtedly interfere with the newspaper’s ability to publish and would create a future disincentive for disclosing newsworthy information on matters of great public concern.⁸⁸ The Court concluded that a law imposing penalties for breaking promises should be enforced even against the press:

Respondents and amici argue that permitting Cohen to maintain a cause of action for promissory estoppel will inhibit truthful

87. *Id.* at 148 (quoting *United States v. Lopez*, 514 U.S. 549, 558–559 (1995)).

88. *See* 501 U.S. 663 (1991).

reporting because news organizations will have legal incentives not to disclose a confidential source's identity even when that person's identity is itself newsworthy. . . . But if this is the case, it is no more than the incidental, and constitutionally insignificant, consequence of applying to the press a generally applicable law that requires those who make certain kinds of promises to keep them.⁸⁹

In other cases, however, the Court has struck down procedural burdens that had the effect of restricting expression,⁹⁰ and laws that affect expression and are more restrictive than necessary to serve their stated purpose.⁹¹ So the extent to which the First Amendment will impose any limit on the government's ability to impose procedural requirements for privacy contracts, or default rules that apply in the absence of such contracts, is unsettled but critically important.

E. Summary

To the extent privacy laws restrict the communication of information, they certainly implicate the First Amendment. And most privacy laws would appear to restrict communication, either directly or indirectly, as was the case in *U.S. West*. But this conclusion, while significant and widely shared among the roundtable participants, belies a number of important questions:

1. Under what standard should privacy laws be reviewed: "intermediate scrutiny," typically applied to "commercial speech" and cases in which expression is mixed with conduct; or, "strict scrutiny," which is usually applicable to direct government restraints on truthful expression, prior restraints, restraints based on the viewpoint or, in many cases, on the content of the expression?

89. *Id.* at 671.

90. *Lorillard Tobacco Co. v. Reilly and Altadis U.S.A. Inc. v. Reilly*, 533 U.S. 525 (2001) (striking down a state law prohibiting outdoor advertising of cigarettes, smokeless tobacco, and cigars within 1,000 feet of schools and playgrounds and requiring that point-of-sale displays be placed no lower than five feet from the floor if located within 1,000 feet of a school or playground); *Denver Area Educ. Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727 (1996) (striking down a federal law requiring cable operators to segregate and block indecent programming); *Martin v. Struthers*, 319 U.S. 141 (1943) (striking down a state law requiring "opt-in" consent for the door-to-door distribution of religious literature).

91. *Reno v. ACLU*, 521 U.S. 844 (1997) (striking down the Communications Decency Act for "unprecedented" overbreadth); *Sable Communications of Cal., Inc. v. FCC*, 492 U.S. 115 (1989) (striking down a federal law regulating "dial-a-porn" services for burdening protected expression).

2. Does the First Amendment apply (and, if so, does it apply with equal force?) to privacy laws that restrict the collection and private use of personal information in the market but do not otherwise restrain publication or public expression?
3. If personal information is collected or disclosed in violation of a law or contract, is the First Amendment implicated when the government seeks to restrict the use of that personal information by an “innocent” third party, where the use does not implicate matters of general public concern?
4. While the Court has tended to assume that the protection of privacy is a “compelling” or “substantial” state interest, given the ubiquity and amorphousness of information flows, can any law be designed to protect privacy and be considered “narrowly tailored” or the “least restrictive means” for achieving the privacy protection goal?

It is also unclear to what extent the public’s reaction to the September 11 terrorist attacks, the use of personal identification to identify and locate witnesses and suspects, and the threat of future terrorist attacks will influence the debate over the extent to which the First Amendment restrains the power of the government to enact privacy laws applicable to the private sector. Three possible public reactions could be: these developments could have no lasting impact on this debate; they could diminish the importance courts attach to privacy interests by explicitly giving new credence to countervailing interests, such as the prevention and prosecution of terrorism; or they could exercise a more subtle, but nevertheless powerful, influence on judicial thinking about privacy. Some of these implications are discussed in greater detail below. But the uncertainty in the aftermath of September 11 should not obscure the fact that privacy laws applicable to private sector collection and use of personal information unavoidably implicate First Amendment interests.

PART III. CONCLUDING OBSERVATIONS ABOUT THE CONSTITUTION AND THE PRIVACY DEBATE

The role of the Constitution in evaluating privacy laws is influenced by more than legal doctrine. Practical, contextual factors concerning the nature of the privacy debate itself and the settings in which privacy laws are applied significantly affect whether the application of those laws is likely to prove constitutional. We conclude by noting five particularly

important—but also controversial—themes raised during the Joint Center roundtable.

A. *The Meaning of Privacy*

The term “privacy” is used to convey many different meanings. The Supreme Court has interpreted the Constitution to protect under the rubric of “privacy” an individual’s constitutional right to be free from unreasonable searches and seizures by the government;⁹² the right to make decisions about contraception,⁹³ abortion,⁹⁴ and other “fundamental” issues such as marriage, procreation, child rearing, and education;⁹⁵ the right not to disclose certain information to the government;⁹⁶ the right to associate free from government intrusion;⁹⁷ the right to enjoy one’s own home;⁹⁸ sexually explicit mail,⁹⁹ radio broadcasts,¹⁰⁰ or other intrusions.¹⁰¹ Interestingly, none of these understandings of privacy are at issue in the current privacy debate.

In common parlance and political debate, the term “privacy” has even more meanings, including individual autonomy (the right to make decisions without undue interference); self-definition (the right to define one’s self to others); solitude and intimacy (the desire to limit access to a place or to oneself); confidentiality (trade secrets and information disclosed subject to a promise of confidentiality); anonymity (the desire not to be identified); security (for oneself or one’s information); freedom from physical or technological intrusion; freedom from annoyance (such as the distraction or harassment of unsolicited mail or telephone calls); freedom from crime (such as identity theft or financial fraud); freedom from embarrassing disclosures; freedom from discrimination (whether legal or illegal); profit (the desire to share in the proceeds from disclosing or using valuable information); and trust (protection against breaches of fiduciary and other professional duties).

Moreover, many privacy surveys and opinion polls appear to reflect a general angst about privacy, rather than a specific concern. This angst

92. See *Katz v. United States*, 389 U.S. 347 (1967).

93. See *Griswold v. Connecticut*, 381 U.S. 479 (1965).

94. See *Roe v. Wade*, 410 U.S. 113 (1973).

95. See *id.* at 152–53.

96. See *Whalen v. Roe*, 429 U.S. 589 (1977).

97. See *NAACP v. Alabama*, 357 U.S. 449 (1958).

98. See *Stanley v. Georgia*, 394 U.S. 557 (1969).

99. See *Rowan v. Post Office*, 397 U.S. 728 (1970).

100. See *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978).

101. See *Frisby v. Schultz*, 487 U.S. 474 (1988); See also *Carey v. Brown*, 447 U.S. 455 (1980).

is likely the result of many factors, including the pace of change and lack of knowledge and understanding about how information is collected, used, and protected. It is therefore important to avoid over-categorizing types of privacy or over-rationalizing privacy concerns.

The breadth and variety of privacy definitions raise significant issues. They help explain why “privacy” has been so popular in legislative contexts—because the term can mean almost anything to anybody— and yet the risk is run of emotionalizing and confusing political responses by ignoring the substantial benefits of open information flows. Reliable, readily available information increases economic efficiency, reduces crime, and may even serve other “privacy” interests, such as cutting down on identity theft and junk mail. Moreover, in light of the recent terrorist attacks, the very breadth and malleability of the term “privacy” may undercut support for new privacy laws of all forms as legislators fear supporting legislation that might appear, even if mistakenly, to impede the search for clues and the prevention of future terrorist acts.

The diversity of definitions also heightens the extent to which laws may purport to operate under one definition but in fact serve an entirely different purpose. For example, while the rhetoric of the current political privacy debate is to invest individuals with “control” over information about them, recent privacy laws such as Title V of the Gramm-Leach-Bliley Financial Services Modernization Act provide individuals with very little control over such information.¹⁰² Most information collection and use in the financial services industry takes place under exemptions in the Act.

The most relevant risk to understanding constitutional issues raised by privacy laws, however, is that the failure to differentiate between meanings of privacy skews the constitutional analysis. It is impossible to know how important a privacy interest is, or whether a law or regulation serves that interest, if that interest is never identified with specificity.

B. The Range of Affected Parties

Who is affected by privacy laws? Although the political debate often refers only to people about whom information is collected or used and the people who want to collect or use the information, the impact of most laws is much broader. There are broader societal interests that should be considered, such as the protection of children, as

102. Gramm-Leach-Bliley Financial Services Modernization Act tit. V, 106 Pub. L. No. 102, 113 Stat. 1338 (1999) (codified at various sections of 15 U.S.C.).

communitarian Professor Amitai Etzioni has written,¹⁰³ or the protection of the public from terrorism, as we have recently been reminded. There are broader economic interests, especially if the presence or absence of privacy protection raises the cost of goods and services that everyone must pay. And there are broader political interests, as the Supreme Court has often noted, to justify the denial of public officials' privacy rights.¹⁰⁴

Recognizing the wide range of people affected by privacy laws is especially important when considering the role of the Constitution, because constitutional values often reflect a broader range of interests than just those of the parties before the Court.

C. Privacy in Context

A meaningful evaluation of the constitutionality of privacy laws requires that those laws be examined in context—not just the context of other issues and values, but also the specific context in which a constitutional challenge is raised. In each of the Supreme Court's privacy cases, how the privacy issue was evaluated and how the case was decided were almost always determined by the legal context in which the issue was presented. For instance, the case holdings have varied depending upon whether the analysis was based on the Commerce Clause, the First Amendment, a restriction on government release of private information, or the tension between important press freedoms and individual privacy. The context will significantly affect both the outcome of the case and the development of constitutional doctrine applicable to privacy interests in commercial settings.

D. Privacy and Change

Change may be the only constant in the ongoing privacy debate. The public's expectations of privacy are changing, as are the many influences that shape those expectations, such as technology, law, and experience. For example, the flood of privacy notices generated by Gramm-Leach-Bliley Act, however significant their direct effect on consumer control over the release of personal information, also serve to heighten consumer awareness and may increase or diminish concerns.

More than any other single factor, computers seem to be playing a major role in influencing and changing privacy concerns. Computers and the networks that connect them are dramatically expanding both the practical ability to collect and use personal data and the economic

103. AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 43–74 (1999).

104. *See, e.g., Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978).

incentive to do so. Some privacy advocates argue that the information revolution is making everything different—that the constitutional protection for information flows in the 1970s and 80s was in part made possible by the practical difficulty of collecting and disseminating information. Now that anyone can affordably and easily access technologies that assemble and disseminate data about millions of people, there is growing pressure for law to help create what was once a practical obscurity.

However, the exact opposite may be true as well; the explosion in information technologies decreases both the ability of, and the need for, law to protect privacy. Instead, we should recognize the democratic promise of technologies that help equalize our access to information and our ability to speak and that provide technological protections for privacy that were never dreamed of before.

E. Public and Private Spheres

The Constitution traditionally limits only actions by the government. However, as technologies give anyone the power to capture information, and create incentives for large private-sector databases that can then be accessed by the government, it is easy to question whether the constitutional distinction between public and private will retain the same significance. However, as the events of September 11 and the subsequent search for witnesses and suspects have reminded us, there can be tremendous value to the public for the government to have access to private-sector records, such as credit card receipts, rental car records, and airline reservation information.

This blurred line may be a red herring, however, because important distinctions remain between government and private-sector information processing. For example, only the government has the power to compel the disclosure of information free from market pressures. Moreover, there may be a distinction because it would be nonsensical to have the government enact laws restricting the creation of private-sector databases as a way to discourage itself from accessing those databases.

The real issues may be the terms under which access to private sector databases is provided and the uses to which the government may put that information, not whether there should be access or whether the information should be collected at all.

CONCLUSION

The current privacy debate's failure to consider the constitutional implications of enacting laws to protect personal information from

incursion by the private sector is problematic, especially in view of the significant limits imposed on the government by the First Amendment. Under those limits, the government bears the burden of demonstrating that privacy laws interfering with expression serve a “compelling” or “substantial” state interest, and are “narrowly tailored” or the “least restrictive means” for achieving that purpose. This is a considerable burden for the government to bear.

The precise extent of the restraint imposed by the First Amendment depends on the specific requirements of those laws and the contexts in which those laws operate and are enforced. The role of the First Amendment will also be influenced by broader factors such as the changing definitions and expectations of “privacy,” the magnitude of the threats posed by too much or too little privacy protection, and the object of privacy laws and their impact on expression, commerce, individual behavior, and society. These and other related issues are intrinsically intertwined with the discussion about the role of the Constitution itself and the power of the government to adopt and enforce laws to protect private information from intrusion by the private sector. Legislators, regulators, and prosecutors who ignore the First Amendment or these broader issues when considering privacy laws do so at their—and our—peril.