

The National Retail Federation's
Protecting Privacy in the New Millennium Series

PROTECTING CONSUMER PRIVACY:
TEN QUESTIONS EVERY LEGISLATOR SHOULD ASK

Fred H. Cate*

New laws to protect privacy are seldom necessary and often constitutionally forbidden. Thanks to a well-established array of state and federal privacy laws, an expanding competitive market for privacy protections, and new technologies and services that make real privacy a reality for the first time ever, additional legislation is rarely necessary.

Unfortunately, this has not deterred state and federal legislators from introducing more than 800 new privacy laws during the past two years. Legislators and citizens are increasingly being called on to evaluate an avalanche of new privacy bills, many of which threaten the benefits that result from open information flows, would impose significant costs on consumers and businesses alike, and offer little enhanced protection for personal privacy.

As both a practical and a constitutional matter, new privacy legislation should respond effectively to a specific harm, interfere as little as possible with individual rights and competitive markets, impose the least cost consistent with the level of privacy protection provided, and be easy and intuitive to use. But it is not always easy to figure out which legislation meets these requirements, especially in the face of so many proposed bills.

These ten questions are designed to help legislators and citizens alike critically evaluate proposed privacy laws:

1. *Does the proposed law address a real problem?* This requires both that there be a real problem and that the law respond to it effectively. If the law's proponents don't identify a specific harm, be suspicious.

*Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington. This paper is excerpted from the National Retail Federation's Protecting Privacy in the New Millennium series, which is available from the National Retail Federation, Attn: Privacy Project, 325 7th Street, N.W., Suite 1100, Washington, DC 20004, tel (202) 783-7971, fax (202) 737-2849, privacy@nrf.com.

2. *Does the proposed law duplicate the protection provided by existing federal or state laws or regulations?*
3. *Is existing privacy law being enforced vigorously?* Proposals for new laws often obscure the fact that existing laws aren't being enforced. Enacting new privacy laws costs the government far less than enforcing existing ones, but does nothing to protect the public.
4. *Are the law's proponents addressing the cost of the proposed law explicitly and honestly?* That cost includes not only the expenses associated with implementing and complying with the law, but also its broader economic impact on consumers, businesses, and the economy. It is irresponsible to adopt a law without understanding the full range of costs it imposes. Distrust any proposal that does not include an estimate of its total economic impact.
5. *Does the proposed law create more problems than it solves?* What are the unintended (or intended, but unspoken) side-effects? Is the solution worse than the problem?
6. *Are the law's proponents making impossible claims for the proposed law?* Some advocates of new privacy laws claim that proposed laws will "give consumers control over their own information." These claims are seldom true and their vagueness suggests that the proponents of such laws may not have a clear idea of what harm they are trying to prevent. If a claim sounds too good to be true, it probably is. This is particularly true when a state law is offered as a solution to a national or international problem.
7. *Does the proposed law claim to protect personal information only from private parties or does it also restrict the government's collection and use of personal information?* Laws that exempt the government from privacy protections are seldom effective or fair. Remember, the constitutional right to privacy only applies against the government; public officials and candidates should get their house in order first before telling others what to do. Question the credibility of any privacy law advocate who does not personally follow the same standards he or she is trying to impose on others.
8. *Does the proposed privacy law take away citizen choice?* The most basic privacy principle, recognized in every set of "fair information principles," is *choice*—the individual's right to make his or her own choice about the proper balance between the value of the open flow of information and the value of enhanced privacy protection, and to act on that choice by choosing among different levels and means (and corresponding costs) of privacy protection in the market. Privacy laws have the effect of denying consumers access to services and benefits that

we value; those laws that make everyone pay for a high level of privacy that only a few desire should be avoided.

9. *Is the proposed law consistent with the Constitution?* Laws that would violate the Constitution, no matter how noble their purpose, are never good laws. The process of debating and enacting them wastes legislatures' time and the public's money. According to the U.S. Court of Appeals for the Tenth Circuit in *U.S. West, Inc. v. Federal Communications Commission*, a decision the Supreme Court declined to review:
 - a. laws restricting the collection and use of personal information to protect privacy restrict speech and therefore are subject to First Amendment review;
 - b. under the First Amendment, the government bears the burden of proving that its rules are constitutional;
 - c. that constitutional burden requires the government to demonstrate that its rules prevent a "*specific and significant harm*"; and
 - d. that the rules reflect "a 'careful calculat[ion of] the costs and benefits associated with the burden on speech imposed by its prohibition.' 'The availability of less burdensome alternatives to reach the stated goal signals that the fit between the legislature's ends and the means chosen to accomplish those ends may be too imprecise to withstand First Amendment scrutiny.'"
10. *Does the law reflect a serious approach to privacy?* Is the proposed law based on inaccurate facts or faulty expectations? Laws that respond to (or worse, encourage) public hysteria, exaggerate the harms they are intended to address or their likely effectiveness in addressing those harms, or fail to provide practical solutions to real problems serve the interests of politicians or advocacy groups, but not of the public.

These questions are by no means exhaustive, but they provide a critical first step toward assuring that proposed privacy laws are necessary, effective, appropriate, and constitutional. Enacting laws that do not meet these criteria threatens not only consumer convenience and economic prosperity, but our very liberty.

*U.S. West, Inc. v. Fed. Communications Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999), *cert. denied*, 120 S. Ct. 1240 (2000) (quoting *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993), and *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 529 (1996) (O'Connor, J., concurring) (citations omitted)) (emphasis added).

The National Retail Federation's
Protecting Privacy in the New Millennium Series

PROTECTING CONSUMER PRIVACY:
TEN QUESTIONS EVERY LEGISLATOR SHOULD ASK

Fred H. Cate*

The Privacy Surge

“Privacy” was the subject of more than 200 bills considered by the 106th Congress and more than 600 introduced in state legislatures during 1999 and 2000. This unprecedented attention both reflects and has contributed to widespread popular concern about privacy and the role of the government in protecting it.

There is no question that privacy is important, both as a political issue and as a basic need of all people. Privacy is critical to our participation in this society and democracy; it is key to the growth and success of commerce online and off; and it is a topic of concern to many people today, as poll after poll demonstrates.

The Cost of Privacy Protection

However, *restricting information flows to protect privacy—as each of the more than 800 legislative proposals identified above would have done—always, inevitably imposes costs on consumers, businesses, and the economy as a whole.* Often those costs are quite significant.

This should come as no surprise to anyone: *Information is the lifeblood of our 21st century economy.* In the words of the Federal Reserve Board: “[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy.”¹ Efforts to restrict the flow of information for whatever purpose inevitably impose costs on us all. Those costs include both the substantive costs of greater privacy (e.g., the costs associated with obscuring relevant information in commercial and personal transactions, impediments to law enforcement, and bad decisions and inefficiencies resulting from inadequate

*Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington. This paper is published by the National Retail Federation as part of its Protecting Privacy in the New Millennium series. For additional information or to order additional copies, contact the National Retail Federation, Attn: Privacy Project, 325 7th Street, N.W., Suite 1100, Washington, DC 20004, tel (202) 783-7971, fax (202) 737-2849, privacy@nrf.com.

information), and the transaction costs of complying with new privacy laws. Perhaps the greatest costs of privacy, however, are the benefits of responsible information-sharing that we no longer enjoy.

The Benefits of Information-Sharing

Laws designed to protect privacy threaten the significant, practical benefits that open information flows bring. Those benefits are shared both by each consumer about whom data are shared and by all consumers in the aggregate because, as Federal Reserve Board Governor Edward Gramlich testified before Congress in July 1999, “[i]nformation about individuals’ needs and preferences is the cornerstone of any system that allocates goods and services within an economy.” The more such information is available, he continued, “the more accurately and efficiently will the economy meet those needs and preferences.”² Without reliable access to personal information, neither government nor business can anticipate and meet citizen and consumer needs, and service and convenience suffer as a result.

Information-sharing:

- makes it possible to ascertain customer needs accurately and meet those needs rapidly and efficiently;
- expands consumer access to a wide range of affordable services and products;
- significantly reduces the cost of many products and services;
- enhances customer convenience and services;
- improves efficiency;
- allows consumers to be informed rapidly and at low cost of those opportunities in which they are most likely to be interested;
- prevents and detects fraud and other crimes; and
- promotes competition by facilitating the entry of new businesses into competitive markets, smaller businesses competing more effectively with larger ones, and the emergence of new, specialized businesses.³

As just one example of these practical benefits, Walter Kitchenman has calculated that mortgage rates in the United States are as much as two full percentage points lower because of the rapid availability of standardized, reliable consumer credit information. American consumers save as much as *\$80 billion a year* because of the efficiency and liquidity that information makes possible.⁴

To provide all of these and other benefits, access to data is essential. Laws restricting information-sharing or requiring “opt-in” consent make the provision of many valuable services, and the convenience and benefits they provide, untenable. It is no answer to condition these services and products on consumer consent, because virtually all beneficial information uses depend upon the routine availability of

standardized, reliable, complete data. Moreover, the sheer cost of seeking consent would act as a dramatic disincentive to investing in innovation.

Widely accessible personal information has helped to create a democratization of opportunity in the United States. Americans can take advantage of opportunities based on their records, on what they have done rather than who they know, because access to standardized consumer information makes it possible for distant companies to make rational decisions about doing business with individuals. The open flow of information gives consumers real choice; sweeping privacy laws restrict that choice.

The authors of a 1999 report on public information concluded that such information constitutes part of this nation's "essential infrastructure," the benefits of which are "so numerous and diverse that they impact virtually every facet of American life. . . ." The ready availability of personal information "facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want."⁵ *Restraints on information flows inevitably interfere with these and other benefits.*

The Basic Requirements for "Good" Privacy Legislation

Privacy laws should balance the benefits of privacy with the benefits of open information flows and impose no cost that does not achieve commensurate increases in privacy protection. Many of the recently adopted and proposed privacy laws have failed to meet these basic requirements; in fact, some have failed to protect privacy at all. For example, in an effort to protect privacy, California prohibited the use of arrestee addresses obtained from law enforcement agencies for marketing products or services, but explicitly permitted such information to be used for "journalistic" purposes.⁶ It is difficult to take seriously the state's claim that sending a letter to an arrestee offering the services of an attorney or private investigator would invade her privacy, while publishing her name and address in the newspaper would not. This "overall irrationality," as Justice Stevens called it in his dissent from the Supreme Court's decision upholding the constitutionality of the statute, "eviscerate[s] any rational basis for believing that the Amendment will truly protect the privacy of these persons."⁷

Similarly, the Gramm-Leach-Bliley Financial Services Modernization Act requires financial institutions to "clearly and conspicuously" provides consumers with a notice about its policies and practices for disclosing personal information. That disclosure must be made "[a]t the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship."⁸ By June 12, 2001, approximately 40,000 financial institutions will be sending as many as 2.5 billion notices to their various customers. Estimates are that individual households will receive an average of 20-50 notices each. Printing and mailing costs alone will be in the 2-5 billion dollar range, if not more. It is difficult to imagine how consumer privacy will be enhanced by this onslaught of legal notices. The same degree of privacy protection could have

been achieved by requiring that financial institutions prominently post their privacy notices or make them available to customers without charge upon request. Instead, Congress opted for a more expensive and burdensome law that achieved no greater level of privacy protection.

The rush to adopt “opt-in” laws poses similar issues. Both “opt-in” and “opt-out” systems give citizens the final, absolute say about the use of personal information about them. The major difference between the two is that, without providing for any greater privacy protection, “opt-in” imposes a far greater restriction on information use, because of the lethargy of most citizens and the practical difficulty of would-be users of information contacting individuals to obtain their “opt-in” consent, as opposed to concerned individuals contacting organizations (which maintain 800-numbers and fixed addresses and business hours) to express their desire to “opt-out.” “Opt-in” laws, therefore, impose a greater obstacle to information flows without achieving any greater privacy protection.

Moreover, “opt-in” systems interfere with information flows in another important way: They raise the cost of communicating. Companies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must rebuild the pipeline by contacting one customer at a time to gain their permission to use information. Consequently, an “opt-in” system for giving consumers control over information usage is always more expensive than an “opt-out” system. “Opt-in” requires that every consumer be contacted to gain explicit permission. Under “opt-out,” contact only occurs for those consumers who wish to withhold permission. “Opt-in” is more costly precisely because it fails to harness the efficiency of having customers reveal their own preferences as opposed to having to explicitly ask them.

Consider the practical experience of U.S. West, one of the few U.S. companies to test an “opt-in” system. In obtaining permission to utilize information about its customer’s calling patterns (e.g., volume of calls, time and duration of calls, etc.), the company found that an “opt-in” system was significantly more expensive to administer, costing almost \$30 per customer contacted. To gain permission to use such information for marketing, U.S. West determined that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts.⁹ Consequently, customers received more calls and faced higher prices than in an “opt-out” system, and one-third of customers were denied the opportunity to even consider whether they wished to receive information about valuable new products and services. It is little wonder that even countries that have adopted “opt-in” laws, such as the 15 member states of the European Union, have resorted to legal maneuvers such as “implied consent” to turn “opt-in” into “opt-out.”

Constitutional Requirements

Enacting laws that restrict information without enhancing privacy protection or that fail to anticipate and explicitly consider the cost of privacy protection hurts consumers, businesses, and the entire economy. But such laws also raise constitutional issues. When the government restricts information flows—for whatever purpose—it must do so as narrowly or, in some cases, in the least restrictive way possible. Under this standard, the Court has struck down laws restricting the publication of confidential government reports,¹⁰ and of the names of judges under investigation,¹¹ juvenile suspects,¹² and rape victims.¹³

Even if the information is considered to be “commercial,” its collection and use is nevertheless protected by the First Amendment. The Supreme Court has found that such expression, if about lawful activity and not misleading, is protected from government intrusion unless the government can demonstrate a “substantial” public interest, the intrusion “directly advances” that interest, and is “narrowly tailored to achieve the desired objective.”¹⁴

The Supreme Court has long held that the constitutional protections for privacy—which, to start with, only apply against the government, not private parties—protect *reasonable* expectations of privacy and only then if necessary to prevent *specific harms*. When evaluating wiretaps and other seizures of private information under the Fourth Amendment, the Supreme Court has long asked whether the data subject in fact expected that the information was private and whether that expectation was reasonable in the light of past experience and widely shared community values.¹⁵ There should be no interference with information flows to protect privacy interests that are not reasonable.

To be reasonable, courts have held that *an expectation of privacy could not attach to public information*. No expectation of privacy may be reasonable if it involves information that is routinely and voluntarily disclosed or is available publicly. This reflects not only the Supreme Court’s interpretation of the Fourth Amendment, but also the common sense that the law should not create costly or burdensome impediments to the collection and use of information that consumers willingly disclose and that is widely available in the marketplace.

The law has also historically required that the government protect privacy interests *only when a specific harm is actually threatened*. This was the view of the U.S. Court of Appeals for the Tenth Circuit in *U.S. West, Inc. v. Federal Communications Commission*. The court’s decision, which the Supreme Court declined to review, struck down the Federal Communications Commission’s “opt-in” rules, discussed above, requiring that telephone companies obtain affirmative consent from their customers before using data about their customers’ calling patterns to market products or services to them. The court wrote:

In the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict *specific and significant harm* on individuals such as undue embarrassment or ridicule or intimidation or harassment or misappropriation of sensitive personal information for the purposes of assuming another's identity. 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.¹⁶

This principle is justified not only by the need to avoid unnecessary restraints on valuable information flows, but also because it is only by identifying the harm that a law is designed to prevent or remedy that a legislator, reviewing court, or citizen can judge whether the law is necessary and whether it does, in fact, respond to that harm. The harm principle has largely been lost in the flood of proposed privacy legislation.

The Limits of Privacy Law

Moreover, much of the avalanche of privacy laws and regulations ignores the basic fact that law seldom can provide effective privacy protection. It misleads the public by promising something that law simply cannot deliver. At best, a law gives a consumer the right to sue or complain to a federal regulator; it does not keep information private. Moreover, U.S. laws do not affect the behavior of persons, institutions, and Web sites outside of the United States—more than half of all Internet users and Web sites—nor does it deter bad actors who are unconcerned with the requirements of the law.

Fortunately, there are often less intrusive, more effective alternatives than government regulation for protecting privacy. These measures more sensitively measure privacy interests and therefore more precisely allow consumers to value their own privacy against the cost and inconvenience of not allowing the use of data about them. Moreover, this approach recognizes that the cause of many privacy invasions, including identity theft, rests solely within the control of the individual.

The role of self-help is especially clear in the Internet environment, where there are readily available, easy-to-use, low- or no-cost technologies and services for browsing anonymously, shopping anonymously, even downloading, printing, and shipping anonymously. Moreover, the technologies of the Internet expand the potential for open, competitive markets, and allow privacy-concerned users to easily search out and compare privacy terms.

Yet, ironically, enacting sweeping privacy laws creates a tremendous disincentive for the development and use of private-sector privacy protections, and a false expectation on the part of many consumers. To the extent we eliminate the incentive for the development of technological and other protections for privacy, we diminish the availability of real privacy for everyone.

The Importance of Balance

Privacy is important and needs to be protected, but these constitutional and practical considerations require that laws that protect privacy be balanced—as consumers do with our personal efforts to protect privacy everyday—with the cost of privacy protection and the benefits that flow from the responsible use of personal information.

This balance is most likely to be reached if each consumer defines that balance for himself or herself. Consumers who value rapid, convenient service more highly than absolute privacy should be free to make that choice and thereby forego the costs imposed by privacy protections that they do not desire. Therefore, privacy protection tools should give maximum control to individual consumers rather than require the government to decide an appropriate level of privacy protection for all. The government must therefore seek to protect each individual's ability to make his or her own choice about the proper balance between the value of the open flow of information and the value of enhanced privacy protection, and to act on that choice by choosing among businesses and other institutions offering a variety of levels and means (and corresponding costs) of privacy protection. *Maximizing consumer benefit, then, requires not only that privacy protection be balanced against the benefits that flow from accessible information, but also that the government avoid substituting its judgment for that of individual consumers.*

Given the extraordinary benefits that information-sharing contributes to consumers, businesses, and the economy and society as a whole, the significant and often unanticipated costs of enacting laws to protect privacy, and the importance of protecting individual choice, legislators should hesitate before restricting the responsible collection and use of personal information even for the most apparently worthwhile purpose.

The Role of Government

When government intervention is necessary—and there are occasions when it is necessary, for example, when very sensitive information is used in a context where no competitive alternatives exist, or when young children are involved—*the government's action should respond effectively to a specific harm; it should interfere with individual rights and competitive markets as little as possible; it should impose the least cost; and*

it should be easy or intuitive to use so that citizens can actually take advantage of the new protection.

Given these important constitutional and practical considerations, here are ten questions that every legislator (and journalist and citizen) should ask about any proposed privacy law:

1. *Does the proposed law address a real problem?* This requires both that there be a real problem and that the law respond to it effectively. If the law's proponents don't identify a specific harm, be suspicious.
2. *Does the proposed law duplicate the protection provided by existing federal or state laws or regulations?*
3. *Is existing privacy law being enforced vigorously?* Proposals for new laws often obscure the fact that existing laws aren't being enforced. Enacting new privacy laws costs the government far less than enforcing existing ones, but does nothing to protect the public.
4. *Are the law's proponents addressing the cost of the proposed law explicitly and honestly?* That cost includes not only the expenses associated with implementing and complying with the law, but also its broader economic impact on consumers, businesses, and the economy. It is irresponsible to adopt a law without understanding the full range of costs it imposes. Distrust any proposal that does not include an estimate of its total economic impact.
5. *Does the proposed law create more problems than it solves? What are the unintended (or intended, but unspoken) side-effects? Is the solution worse than the problem?*
6. *Are the law's proponents making impossible claims for the proposed law?* Some advocates of new privacy laws claim that proposed laws will "give consumers control over their own information." These claims are seldom true and their vagueness suggests that the proponents of such laws may not have a clear idea of what harm they are trying to prevent. If a claim sounds too good to be true, it probably is. This is particularly true when a state law is offered as a solution to a national or international problem.
7. *Does the proposed law claim to protect personal information only from private parties or does it also restrict the government's collection and use of personal information?* Laws that exempt the government from privacy protections are seldom effective or fair. Remember, the constitutional right to privacy only applies against the government; public officials and candidates should get their house in order first before telling others what to do. Question the credibility of any privacy

law advocate who does not personally follow the same standards he or she is trying to impose on others.

8. *Does the proposed privacy law take away citizen choice?* The most basic privacy principle, recognized in every set of “fair information principles,” is *choice*—the individual’s right to make his or her own choice about the proper balance between the value of the open flow of information and the value of enhanced privacy protection, and to act on that choice by choosing among different levels and means (and corresponding costs) of privacy protection in the market. Privacy laws have the effect of denying consumers access to services and benefits that we value; those laws that make everyone pay for a high level of privacy that only a few desire should be avoided.

9. *Is the proposed law consistent with the Constitution?* Laws that violate the Constitution, no matter how noble their purpose, are never good laws. The process of debating and enacting them wastes legislatures’ time and the public’s money. According to the U.S. Court of Appeals for the Tenth Circuit in *U.S. West, Inc. v. Federal Communications Commission*, a decision the Supreme Court declined to review:
 - a. laws restricting the collection and use of personal information to protect privacy restrict speech and therefore are subject to First Amendment review;
 - b. under the First Amendment, the government bears the burden of proving that its rules are constitutional;
 - c. that constitutional burden requires the government to demonstrate that its rules prevent a “*specific and significant harm*”; and
 - d. that the rules reflect “a ‘careful calculat[ion of] the costs and benefits associated with the burden on speech imposed by its prohibition.’ ‘The availability of less burdensome alternatives to reach the stated goal signals that the fit between the legislature’s ends and the means chosen to accomplish those ends may be too imprecise to withstand First Amendment scrutiny.’”¹⁷

10. *Does the law reflect a serious approach to privacy?* Is the proposed law based on inaccurate facts or faulty expectations? Laws that respond to (or worse, encourage) public hysteria, exaggerate the harms they are intended to address or their likely effectiveness in addressing those harms, or fail to provide practical solutions to real problems serve the interests of politicians or advocacy groups, but not of the public.

These questions are by no means exhaustive, but they provide a critical first step towards assuring that proposed privacy laws are necessary, effective, appropriate, and constitutional. Enacting laws that do not meet these criteria threatens not only consumer convenience and economic prosperity, but our very liberty.

¹Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud 2* (1997).

²*Financial Privacy*, Hearings Before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, U.S. House of Representatives, 106th Cong. (1999) (statement of Edward M. Gramlich).

³*See generally* Fred H. Cate, *Personal Information in Financial Services: The Value of a Balanced Flow* (Financial Services Coordinating Council, 2000).

⁴Walter F. Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns 7* (The Tower Group, 1999).

⁵Fred H. Cate and Richard J. Varn, *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (Coalition for Sensible Public Records Access, 1999).

⁶Cal. Gov't Code § 6254(f)(3).

⁷*Los Angeles Police Department v. United Reporting*, 120 S. Ct. 483, 492 (1999) (Stevens, J., dissenting).

⁸Gramm-Leach-Bliley Financial Services Modernization Act, 106 Pub. L. No. 102, § 503(a), 113 Stat. 1338 (1999).

⁹Brief for Petitioner and Intervenors at 15-16, *U.S. West, Inc. v. Fed. Communications Comm'n*, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).

¹⁰*New York Times Co. v. United States*, 403 U.S. 713 (1971).

¹¹*Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978).

¹²*Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97 (1979).

¹³*Florida Star v. B.J.F.*, 491 U.S. 524 (1989); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975).

¹⁴*Central Hudson Gas & Electric Corp. v. Public Service Comm'n*, 447 U.S. 557, 566 (1980); *Board of Trustees v. Fox*, 492 U.S. 469, 480 (1989) (emphasis added).

¹⁵*Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *Terry v. Ohio*, 392 U.S. 1, 9 (1968); *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

¹⁶*U.S. West, Inc. v. Fed. Communications Comm'n*, 182 F.3d 1224, 1235 (10th Cir. 1999), *cert. denied*, 120 S. Ct. 1240 (2000) (emphasis added).

¹⁷*Id.* (quoting *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993), and *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 529 (1996) (O'Connor, J., concurring) (citations omitted)) (emphasis added).