2000

Principles of Internet Privacy

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Principles of Internet Privacy

FRED H. CATE*

I. INTRODUCTION

Paul Schwartz's *Internet Privacy and the State* makes an important and original contribution to the privacy debate that is currently raging by beginning the process of framing a new and more useful understanding of what "privacy" is and why and how it should be protected.[1] The definition developed by Brandeis, Warren,[2] and Prosser,[3] and effectively codified by Alan Westin in 1967—"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"[4]—worked well in a world in which most privacy concerns involved physical intrusions (usually by the government) or public disclosures (usually by the media), which, by their very nature, were comparatively rare and usually discovered.

But that definition's exclusive focus on individual control has grown incomplete in a world in which most privacy concerns involve data that we inevitably generate in torrents as we go through our lives in an increasingly computerized, networked environment, and which can be collected and used by virtually anyone, usually without us knowing anything about it. Moreover, in this information economy, data have real value, especially when combined with other data, and the resources required to collect and use data are comparatively inexpensive and widely available. In this world, few of us have the awareness and expertise to consider trying to

* *Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington; Senior Counsel for Information Law, Ice, Miller, Donadio & Ryan, Indianapolis, IN.*

1. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000).

2. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

3. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

4. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

control all of the data we generate. Few of us have the time or frankly, even the incentive to attempt to do so, and the sheer volume of data, variety of sites where they are collected and used, and economic incentive for doing so would make the attempt laughably futile.

So Professor Schwartz's contribution is both valuable and timely as it helps us appreciate the limits of our current understanding of privacy, and the need for developing a more expansive definition. To be sure, I do not agree with all of Professor Schwartz's analysis, but I agree wholeheartedly, even if for sometimes different reasons, with his conclusion that it is time to look for a better definition of privacy.

This is not to suggest that individual control should not be part of our understanding of privacy, but rather that it can no longer reasonably be considered the only part. That "privacy" means more than just individual control of information and the government's involvement in protecting privacy, as Professor Schwartz argues, both says something important about, and significantly influences individual participation in, our democracy and society. Professor Schwartz describes this broader vision of privacy as "constitutive privacy," which, he argues, reflects the understanding that "access to personal information and limits on it help form the society in which we live and shape our individual identities."[5] As a result, Professor Schwartz writes: "The proper social response to information privacy issues cannot be to maximize secrecy about individuals and their pursuits."[6] Rather, our new understanding of privacy should reflect the fact that the State "has a positive role to play in shaping the privacy market and privacy norms"[7] and that those norms will not be bright-line rules but instead "shifting, multidimensional data preserves that insulate personal data from different kinds of observation by different parties."[8] Again, I agree entirely, as will, I suspect, most readers.

But what does this mean, practically, in this new millennium in the context of the Internet? What principles should undergird the government's involvement in attempting to craft privacy norms? These questions remain mostly unanswered in Professor Schwartz's article, in large part because they are beyond the scope of his sophisticated, theoretical analysis. He writes that his definition of "constituitive privacy" argues for the State to "concentrate its activities in two areas: (1) assisting in the creation and maintenance of the conditions for a functioning privacy market, and (2) supporting development of privacy norms that protect against too great a rate of preference falsification."[9] But I am unclear what this would mean

5. Schwartz, *supra* note 1, at 834.
6. *Id.*
7. *Id.* at 859.
8. *Id.* at 834.
9. *Id.* at 854.

in reality, or why it supports his conclusion in passing that Congress' recent rejection of its 1994 requirement that states provide drivers with an opportunity to "opt-out" of the use of state Department of Motor Vehicles drivers' license and motor vehicle records (DMV records) for marketing and surveys, in favor of a new requirement that states prohibit such uses unless drivers "opt-in" to them is "effective action to establish and protect positive feedback for a privacy norm."[10]

I would like to take advantage of the important process that Professor Schwartz has begun of redefining our understanding of what privacy means, especially in the context of the Internet, by considering briefly those principles that undergird the government's efforts to protect privacy and craft privacy norms. Part II of this Article suggests five principles that should guide government legislative and regulatory activities concerning privacy. While this list is necessarily brief and, therefore, likely incomplete, it provides at least a glimpse of what State regulation might be appropriate in the face of the broader, more subtle understanding of privacy that Professor Schwartz has proposed. Finally, in Part III, I apply those principles to Professor Schwartz's specific example of a practical application of "constitutive privacy," cited above, to suggest that far from demonstrating "effective action to establish and protect positive feedback for a privacy norm,"[11] Congress's recent action to close DMV records undermines the creation of thoughtful, rational privacy norms.

II. PRINCIPLES FOR GOVERNMENT POLICYMAKING

Judicial precedent, historical experience, and common sense suggest five principles that have undergirded, and should continue to guide, government policymaking with regard to information.

A. *The Importance of Balance*

The first principle is the concept of balance. This may seem so obvious as to not be worth stating, but the United States has historically balanced competing interests, particularly with regard to information, to determine for what purposes and by what means the government may interfere with private information flows, or engage in the collection and dissemination of information itself. Identifying the constitutional standard by which those balances are achieved has been one of the major tasks of the Supreme Court in the latter half of the twentieth century. The Court has promulgated a plethora of standards to be applied variously, for example, to government regulations that discriminate against a small group of speak-

10. *Id.* at 858.
11. *Id.* at 857.

ers,[12] restrict expression on the basis of viewpoint or prior to its being published,[13] regulate conduct intrinsically intertwined with expression,[14] affect only the time, place, or manner of expression,[15] regulate expression on public property,[16] restrain commercial expression,[17] or compel expression.[18]

All of these and the Court's other information-related standards have one thing in common: They accord considerable protection to expression

12. Such cases typically require "strict scrutiny," under which "the State must show that its regulation is necessary to serve a compelling state interest and is narrowly drawn to achieve that end." Arkansas Writers' Project, Inc. v. Ragland, 481 U.S. 221, 231 (1987). As articulated in *Minneapolis Star & Tribune Co. v. Minnesota Comm'n*, 460 U.S. 575 (1983), the test required that the State assert an interest "of compelling importance that it cannot achieve without" the regulation. *Id.* at 585. Nonetheless, and despite rhetoric to the contrary, the Court does not require that the means be the least restrictive available. Strict scrutiny applies to most "discriminatory restriction[s] or prohibition[s] of speech . . . ." *Arkansas Writers' Project*, 481 U.S. at 236 (Scalia, J., dissenting).

13. *See, e.g.*, New York Times Co. v. United States, 403 U.S. 713 (1971); Near v. Minnesota, 283 U.S. 697 (1931).

14. *See* United States v. O'Brien, 391 U.S. 367 (1968). Chief Justice Warren wrote for the Court that "when 'speech' and 'nonspeech' elements are combined in the same course of conduct," government regulation of that conduct is:

> sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.

Id. at 376-77.

15. Regulations of the time, place, and manner of expression are constitutional if they "are content-neutral, are narrowly tailored to serve a significant government interest, and leave open ample alternative channels of communication." Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983).

16. The Supreme Court has identified three types of public fora: "the traditional public forum, the public forum created by government designation, and the nonpublic forum." Cornelius v. NAACP Legal Defense & Educ. Fund, Inc., 473 U.S. 788, 802 (1985). Traditional public fora are defined by the objective characteristics of the property, such as whether, "by long tradition or by government fiat," the property has been "devoted to assembly and debate." *Id.* (quoting *Perry*, 460 U.S. at 45). The government can exclude a speaker from a traditional public forum "only when the exclusion is necessary to serve a compelling state interest and the exclusion is narrowly drawn to achieve that interest." *Id.* at 800. Designated public fora are created by purposeful governmental action. *See id.* at 802. If the government excludes a speaker who falls within the class to which a designated public forum is made generally available, its action is subject to strict scrutiny. *See id.* at 800. Other government properties are nonpublic fora or effectively not fora at all. *See id.* at 803. The government can restrict access to a nonpublic forum "as long as the restrictions are reasonable and [are] not an effort to suppress expression merely because public officials oppose the speaker's view." *Id.* at 800 (quoting *Perry*, 460 U.S. at 46).

17. "Commercial speech," which the Court has found is accorded less constitutional protection, is evaluated under a four-part test: the expression at issue "must concern lawful activity and not be misleading"; the asserted governmental interest must be "substantial;" the regulation must be one that "directly advances the governmental interest asserted;" Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 566 (1980); and must be narrowly tailored to achieve the desired ends. *See* Board of Trustees v. Fox, 492 U.S. 469, 477-81 (1989).

18. In *West Virginia State Board of Education v. Barnette*, 319 U.S. 624, 639 (1943), *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241, 258 (1974), and *Wooley v. Maynard*, 430 U.S. 705, 716 (1977), the Court required that the government action be reviewed under "strict scrutiny."

and the communication of information, requiring in virtually every case that the government have a "compelling" or "substantial" interest and that its regulation be "narrowly tailored" to achieve that interest. I will return to this point below.

In addition, all of these tests require that courts engage in their own independent balancing. Across-the-board legislative or regulatory assessments are insufficient where constitutional interests are at stake. Consider just one example. The state of Massachusetts adopted a statute which required trial court judges to close all criminal trials when minor victims of sexual offenses testified.[19] In 1982, the Supreme Court struck down the statute, in part, as unconstitutional.[20] It is difficult to imagine a stronger privacy interest than that of minor victims of sexual offenses who must testify at trial. But even in that instance, the Supreme Court said that the State may not enact an across-the-board rule closing trials. It stated that "in individual cases, and under appropriate circumstances, the First Amendment does not necessarily stand as a bar to the exclusion from the courtroom of the press and general public during the testimony of minor sex-offense victims. *But a mandatory rule, requiring no particularized determinations in individual cases, is unconstitutional.*"[21] Laws that put in place broad restrictions on the flow of information, rather than require sensitive balances to prevent specified harms, are constitutionally problematic.

So, this first principle suggests not only the importance of balance, but also that when that balance involves expression, the government bears an historically great burden, and courts reviewing its actions must engage in a careful, specific weighing of the interests at stake. The remaining principles reflect those interests that the Supreme Court has identified as most relevant.

B. *Open Information Flows*

Perhaps the most important consideration when balancing restrictions on information is the historical importance of the free flow of information. The free flow concept is one that is not only enshrined in the First Amendment, but frankly in any form of democratic or market economy. In the United States, we have placed extraordinary importance on the open flow of information. As the Federal Reserve Board noted in its report to Congress on data protection in financial institutions, "it 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 econ-

19. *See* MASS. GEN. LAWS ch. 278, § 16A (1998).
20. *See* Globe Newspaper Co. v. Superior Court, 457 U.S. 596 (1982).
21. *Id.* at 611 n.27 (emphasis added).

omy."[22]

The significance of open data flows is reflected in the constitutional provisions not only for freedom of expression, but for copyrights—to promote the creation and dissemination of expression, and for a post office—to deliver the mail and the news.[23] Federal regulations demonstrate a sweeping preference for openness, reflected in the Freedom of Information Act,[24] Government in the Sunshine Act,[25] and dozens of other laws applicable to the government. There are even more laws requiring disclosure by private industry, such as the regulatory disclosures required by securities and commodities laws, banking and insurance laws, and many others.[26] This is a very basic tenet of the society in which we live. Laws that restrict that free flow almost always conflict with this basic principle. That does not mean that such laws are never upheld, but merely that they face a considerable constitutional hurdle.

This is done with good reason. Open information flows are not only essential to self-governance; they have also generated significant, practical benefits. The ready availability of personal information helps businesses "deliver the right products and services to the right customers, at the right time, more effectively and at lower cost," Fred Smith, founder and President of the Competitive Enterprise Institute, has written.[27] Federal Reserve Board Governor Edward Gramlich testified before Congress in July 1999 that "[i]nformation about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy."[28] The more such information is available, he continued, "the more accurately and efficiently will the economy meet those needs and preferences."[29]

---

22. Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud*, 2 (1997) <http://www.bog.frb.fed.us/boarddocs/RptCongress/privacy.pdf>.

23. *See* U.S. CONST. art. I, § 8.

24. *See* 5 U.S.C. § 552 (1994 & Supp. IV 1998).

25. *See* 5 U.S.C. § 552b (1994 & Supp. IV 1998).

26. *See, e.g.*, Fair Credit Billing Act, 15 U.S.C. § 1666 (1994)); Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994 & Supp. IV 1998)); Electronic Funds Transfer Act, 15 U.S.C. §§ 1693-1693r (1994 & Supp. IV 1998)); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2520, 2701-2709 (1994 & Supp. IV 1998)); Video Privacy Protection Act, 18 U.S.C. § 2710 (1994)); Family Education Rights and Privacy Act, 20 U.S.C. § 1232g (1994)); Customer Proprietary Network Information provisions of the Telecommunications Act of 1996, 47 U.S.C. § 222 (Supp. III 1997)); and the Cable Communications Policy Act, 47 U.S.C. § 551(a)(1) (Supp. IV 1998)).

27. Fred L. Smith, Jr., *Better to Share Information*, DESERET NEWS (Salt Lake City, Utah), Oct. 14, 1999, at A22, *available in* LEXIS, News Library, Deseret News File.

28. *Financial Privacy, Hearings Before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives*, 106th Cong. (1999) *available at* <http://www.house.gov/banking/72199gra.htm> [hereinafter Financial Privacy Hearings] (statement of Edward M. Gramlich, Member, Board of Governors of the Federal Reserve System).

29. *Id.*

Federal Reserve Board Chairman Alan Greenspan has been perhaps the most articulate spokesperson for the extraordinary value of accessible personal information. In 1998, he wrote to Congressman Ed Markey (D-Mass.):

> A critical component of our ever more finely hewn competitive market system has been the plethora of information on the characteristics of customers both businesses and individuals. Such information has enabled producers and marketers to fine tune production schedules to the ever greater demands of our consuming public for diversity and individuality of products and services. Newly devised derivative products, for example, have enabled financial institutions to unbundle risk in a manner that enables those desirous of taking on that risk (and potential reward) to do so, and those that chose otherwise, to be risk averse. It has enabled financial institutions to offer a wide variety of customized insurance and other products.
>
> Detailed data obtained from consumers as they seek credit or make product choices help engender the whole set of sensitive price signals that are so essential to the functioning of an advanced information based economy such as ours.[30]

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.[31] With outstanding mortgage rates approaching $4 trillion, American consumers save as much as $80 billion a year because of the efficiency and liquidity that information makes possible. Such information further reduces the cost of financial services by facilitating the prevention and early detection of fraud, debt collection efforts, and nationwide competition and consumer mobility, thereby increasing both the availability of, and the range of people who qualify for, credit.

In a recent report on public record information, Richard Varn, Chief Information Officer of the State of Iowa, and I examined the critical roles played by public record information in our economy and society. We concluded that such information constitutes part of this nation's "essential infrastructure," the benefits of which are "so numerous and diverse that they

30. Letter from Alan Greenspan, Chairman, Federal Reserve Board, to Edward J. Markey, Representative, U.S. House of Representatives, July 28, 1998, *available at* <http://www.house.gov /markey /980728letter.htm>.

31. *See* WALTER F. KITCHENMAN, U.S. CREDIT REPORTING: PERCEIVED BENEFITS OUTWEIGH PRIVACY CONCERNS 7 (1999), *available at* <http://www.towergroup.com/Search/wkitchen.asp>.

impact virtually every facet of American life. . . ."[32] The ready availability of public record data "facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want."[33]

Perhaps most importantly, widely accessible personal information has helped to create a democratization of opportunity in the United States. Anyone can go almost anywhere, make purchases from vendors they will never see, maintain accounts with banks they will never visit, and obtain credit far from home all because of open information flows. Americans can take advantage of opportunities based on their records, on what they have done rather than who they know, because access to consumer information makes it possible for distant companies and creditors to make rational decisions about doing business with individuals. The open flow of information gives consumers real choice. This is what the open flow of information principle reflect, not just the constitutional importance of information flows, but their significant economic and social benefits as well.

C. *The Meaning of "Private"*

The third principle reflects a complex, but sophisticated understanding of "privacy." Individual privacy is highly protected in U.S. law from intrusions by the government. In fact, it would not be an overstatement to say that the Constitution reflects the conviction that the greatest threat to individual liberty is the government. As a result, rights articulated in the Constitution generally are protected only against government actions. Only the Thirteenth Amendment, which prohibits slavery, applies directly to private parties.[34] All other constitutional rights—whether to speak freely, confront accusers, or be tried by a jury of one's peers—regulate the public, but not the private, sector.

One dominant theme of constitutional rights is the protection of citizens from government intrusion into their privacy. A vigorous First Amendment, for example, permits individuals the privacy of their own thoughts, beliefs, and associations. The Third Amendment keeps government soldiers from being quartered in private homes. The Fourth Amendment prohibits unreasonable searches and seizures. The Fifth Amendment restricts government from interfering with private property, provides for due process and compensation when it does so, and protects citizens from self-incrimination. Collectively, these and other provisions of the Constitution impose extraordinary limits on government authority to intrude on

32. FRED H. CATE & RICHARD J. VARN, THE PUBLIC RECORD: INFORMATION PRIVACY AND ACCESS—A NEW FRAMEWORK FOR FINDING THE BALANCE 10 (1999), *available at* <http://www.cspra.org/The%20Public%20Record.pdf>.

33. *Id.* at 13.

34. *See* Clyatt v. United States, 197 U.S. 207, 216-220 (1905).

private property, compel testimony, or interfere with practices closely related to individual beliefs, such as protest, marriage, family planning, or worship.

Three related points are worth noting. The first is that the extent of that protection is determined by the type of balancing reflected in the first principle. The Supreme Court has long asked in the context of Fourth Amendment challenges to government searches and/or seizures: What expectation of privacy is implicated by access and how reasonable is that expectation? When evaluating wiretaps and other seizures of private information, the Court has inquired into 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.[35] The law only protects expectations of privacy that are real and reasonable.

The U.S. Court of Appeals for the Fourth Circuit highlighted this very point in its decision striking down the 1994 Driver's Privacy Protection Act.[36] The court wrote, first, 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."[37] Second, 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...."[38] Finally, the court concluded that "such information is commonly provided to private parties.... We seriously doubt that an individual has a ... right to privacy in information routinely shared with strangers...."[39]

In the context of information held by the government, the law has traditionally balanced access and privacy by providing for disclosure of all information held by the government, except where such disclosure would offend a specific, enumerated privacy interest. The federal Freedom of Information Act (FOIA), for example, requires disclosure of all records other than (1) "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal pri-

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

36. *See* Pub. L. No. 103-322, 108 Stat. 2099-2102 (1994) (codified at 18 U.S.C. §§ 2721-2725 (1994 & Supp. IV 1998)).

37. Condon v. Reno, 155 F.3d 453, 464-65 (4th Cir. 1998), *rev'd on other grounds*, Reno v. Condon, 120 S.Ct. 666 (2000).

38. *Id.* at 465.

39. *Id.*

vacy,"[40] and (2) records compiled for law enforcement purposes "to the extent that the production of such [information] . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."[41] Under the FOIA, these records *may* be withheld if the agency believes that the privacy risk justifies it. The laws of the states and the District of Columbia follow a similar pattern: disclosure is the rule; privacy is an exception.

Second, as the appellate court's language suggests, one longstanding corollary of the principle that the law should protect as "private" only information that one actually and reasonably believes is private, is the concept that private should necessarily mean "nonpublic." No expectation of privacy may be reasonable if it involves information that is routinely disclosed or available publicly.

The third point that should be noted is that the high level of privacy protection is directed only against government, not private, incursions. This does not mean that there is not, or should not, be any protection from invasions of privacy carried out by private parties, but it does suggest that such incursions are less constitutionally suspect than government actions. There are a variety of possible explanations for this. One focuses on the power of the government to compel disclosure of information, and the fact that individuals have no alternative but to comply: the market, which can reflect consumer demand for privacy, does not apply to information processing by the government. So laws may be necessary to control government invasions of privacy that are not necessary in the private sector.

Another explanation is the constitutional importance of open flows of information. Regulating privacy in the private sector necessarily means interfering with information flows, something the Supreme Court is historically loathe to allow.

Still another explanation is the recognition that restricting the power of one citizen to engage in activity that might be construed as invading the privacy of another may simply impose too great a cost on citizens individually and collectively. Again, this is not to suggest that there is no value in privacy or no legal protection for privacy in the private sector. One of the cornerstones of the American legal system is respect for private property: the laws that attend private property are what empower one person to exclude another from her land and home and papers and possessions, and to call upon the State to protect those objects from physical intrusion and interference.

But I believe this does reflect the understanding that privacy is not an unmitigated good. Protecting the privacy of information imposes real costs

40. 5 U.S.C. § 552(b)(6).
41. *Id.* § 552(b)(7)(C).

on individuals and institutions. Judge Richard Posner has written:

> Much of the demand for privacy . . . concerns discreditable information, often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is . . . to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit . . . .[42]

Privacy facilitates the dissemination of false information, protects the withholding of relevant true information, and interferes with the collection, organization, and storage of information on which businesses and others can draw to make rapid, informed decisions. The costs of privacy include both transactional costs incurred by information users seeking to determine the accuracy and completeness of the information they receive, and the risk of future losses resulting from inaccurate and incomplete information. Privacy, therefore, may reduce productivity, lead to higher prices for products and services, and make some services untenable altogether. The protection of privacy may also interfere with other constitutional values, such as the protection for expression in the First Amendment and the protection for private property in the Fifth Amendment.

As a practical matter, virtually none of us wants as much privacy for others as we do for ourselves. When we hire people to take care of our children, few of us are very interested in the caregivers' privacy rights. When we board an airplane, we do not want the pilots to have extensive privacy rights. The Supreme Court has long lent an unsympathetic ear to individuals seeking redress from the government against other individuals' collection and use of information. When privacy rights conflict with free expression rights before the Court, the latter prevail, virtually without exception. When information is true and obtained lawfully, the Supreme Court has repeatedly held that the State may not restrict its publication without showing a very closely tailored, compelling governmental interest. Under this requirement, the Court has struck down laws restricting the publication of confidential government reports,[43] and of the names of judges under investigation,[44] juvenile suspects,[45] and rape victims.[46] Moreover, there is no recovery for invasion of privacy unless the informa-

42. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 399 (1978).

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

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

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

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

tion published is highly offensive to a reasonable person, and either false[47] or not newsworthy.[48] The 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 plaintiffs' 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.[49]

These stricture apply irrespective of whether the speaker is an individual or an institution. Even wholly commercial expression is protected by the First Amendment. The 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, and that the intrusion "directly advances"[50] that interest and is "narrowly tailored to achieve the desired objective."[51] The Court does not characterize expression as "commercial"—and therefore subject government regulations concerning it to "intermediate scrutiny"—just because it occurs in a commercial context. The speech of corporations is routinely accorded the highest First Amendment protection—"strict scrutiny" review—unless the Court finds that the purpose of the expression is to propose a commercial transaction[52] or that the expression occurs in the context of a regulated industry or market (such as the securities exchanges) and concerns activities which are, in fact, being regulated (the sale of securities).[53] Even if considered commercial, such expression is still accorded intermediate scrutiny, requiring that the government's interest be "important or substantial" and that the regulation be "no greater than is essential to the furtherance of that interest."[54]

What we are left with, then, is a complicated and, outside of the context of government action, restrictive view of privacy.

D. *The Concept of Harm*

One of the key elements used when balancing privacy with other interests is the concept of harm. The Supreme Court has long recognized that

47. *See* Cantrell v. Forest City Publ'g Co., 419 U.S. 245 (1974).

48. *See Florida Star*, 491 U.S. at 536.

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

50. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 566 (1980).

51. Board of Trustees v. Fox, 492 U.S. 469, 480 (1989).

52. *See Central Hudson*, 447 U.S. at 562-63.

53. *See* Lowe v. SEC, 472 U.S. 181 (1985).

54. United States v. O'Brien, 391 U.S. 367, 376-77 (1968).

the law should restrict information flows to protect privacy only when a specific harm is actually threatened. When information poses a demonstrable harm, we measure the value of that flow of information against the severity of the harm threatened, and in some instances allow the legal system to restrict the flow of information to protect against that harm, but only where a specific harm is threatened. The U.S. Court of Appeals for the Tenth Circuit recently struck down the Federal Communication Commission's rules requiring that telephone companies obtained 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, 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.[55]

The harm principle is a very significant issue for at least three reasons. One is that we have historically required that there be a realistic possibility of harm to justify regulation. If there is no harm threatened, then what is the justification for the regulation, especially if the regulation interferes with the free flow of information? Second, the effectiveness with which a law prevents or remedies a specific harm is the measure of that law's success and the basis for determining whether new laws are necessary. Finally, if you cannot identify a specific harm, it raises the specter that there may be some other, undisclosed purpose—unrelated to the supposed harm—motivating the regulation. So the harm principle is at the very core of our evaluation of privacy interests.

E. *Preference for Self-Help*

The fifth and final principle reflects the longstanding preference for private, market-based solutions, especially to issues involving information. There are many reasons for this. One is a general distrust of government. Jane Kirtley, former Executive Director of the Reporters Committee for

55. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999) (emphasis added).

Freedom of the Press, has written that the expectation that the government will protect privacy "ignore[s], or repudiate[s], an important aspect of the American democratic tradition: distrust of powerful central government. . . . [W]hen it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart."[56] I believe this undergirds the Supreme Court's preference for self-help remedies where information harms are involved. As noted, the Court has repeatedly interpreted the First Amendment to deny plaintiffs aggrieved by even false and harmful speech any remedy, stressing instead, in the words of Justice Brandeis, that "the remedy to be applied is more speech, not enforced silence."[57]

But I believe this principle also reflects the belief that nongovernmental measures often provide more effective and sensitive means for protecting privacy. This has certainly proved true in the case of privacy, where considerable protection is available through the use of technologies, markets, industry self-regulation and competitive behavior, and individual judgment. For example, technological innovations such as adjustable privacy protection settings in both Netscape and Microsoft Explorer, encryption software, anonymous remailers, and, in fact, the Internet itself all facilitate privacy and individual control over the information we disclose about ourselves. The widespread availability, increased power, and decreased price of many technologies also facilitate a vibrant market for privacy protection, whether in the form of online privacy certifications like BBBOn-line and TrustE, or complete privacy protecting services like the recently unveiled iPrivacy, that make it possible for an individual to browse, make purchases online, and even ship goods to her home or a drop-off location without ever disclosing her real identity, address, e-mail address, or credit card number to anyone. These technologies can actually and completely protect privacy in a way that the law cannot.

In addition, many companies are actively competing for customers by promoting their privacy policies and practices. If enough consumers demand better privacy protection and back up that demand, if necessary, by withdrawing their patronage, virtually all competitive industry sectors are certain to respond to that market demand. In fact, consumer inquiries about, and response to, corporate privacy policies are an excellent measure of how much the society really values privacy.

Many industry associations have adopted privacy standards and principles. Corporate compliance with privacy standards constitutes an increasingly important accolade in competitive markets. Moreover, industry asso-

56. Jane E. Kirtley, *The EU Data Protection and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 648-49 (1995).

57. Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring); *see also* 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 498 (1996); Texas v. Johnson, 491 U.S. 397, 419 (1989).

ciations can help persuade member organizations to adopt and adhere to industry norms for privacy protection. The majority of the individual reference services group industry has agreed to abide by the IRSG Principles, which not only establish data protection standards, but also require annual compliance audits by third parties and a commitment not to provide information to entities whose practices are inconsistent with the IRSG Principles.[58]

These more flexible, more contextual, more specific tools often provide better privacy protection than broad laws, and that protection is achieved at potentially lower cost to consumers, businesses, and the society as a whole. These responses are exactly what we would expect from the market if consumers value privacy protection in the private sector.

III. THE PRINCIPLES APPLIED

These five principles—the requirement that government restrictions on information be balanced on an individual basis, taking into account the value of open information flows, the limited understanding of privacy applied to the private sector (requiring, at minimum, that the privacy interest be real and reasonable), the focus on specific harms, and the broad preference for individual action and self-help—reflect more than a half-century of judicial thinking, yet they are more relevant than ever as technologies give individuals new power to communicate, to access, and to use information.

I think that Congress's recent legislation imposing an "opt-in" system on state DMV records demonstrates these principles' continuing vitality. When judged against these principles, the bill establishes a "privacy norm" that, far from being "effective" and "positive,"[59] is weak, duplicitous, expensive, and politically expedient.

The Driver's Privacy Protection Act of 1994 (DPPA)[60] was enacted by Congress as part of a package of anti-crime legislation[61] in response to the 1989 murder of actress Rebecca Schaeffer. Schaeffer had been killed by an obsessed fan who reportedly obtained her address, through a private investigator, from her California DMV record. The law prohibits state DMVs and their employees from releasing "personal information" from any person's driver's record, unless the request fits within any of fourteen

58. *See* FTC, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS (1997), *available at* <http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm>.

59. Schwartz, *supra* note 1, at 857.

60. Pub. L. No. 103-322, 108 Stat. 2099-2102 (1994) (codified at 18 U.S.C. §§ 2721-2725 (1994 & Supp. IV 1998)).

61. *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (codified as amended in scattered sections of 18, 28, and 42 U.S.C.).

exemptions,[62] including, for example, use by any government agency,[63] insurance company,[64] or licensed private investigator;[65] any use related to vehicle safety, emissions, or research;[66] and any use at all if the relevant DMV has provided drivers with the opportunity to waive their statutory rights in non-disclosure, i.e., to "opt-out."[67] The Drivers Privacy Protection Act took effect three years later, in 1994, by which time a majority of states had enacted their own laws complying with the Act, including "opt-out" provisions. (A number of states also challenged the constitutionality of the law, arguing that Congress lacked the constitutional authority to compel them to regulate access to their state records. On January 12, 2000, the Supreme Court determined that Congress did possess the necessary authority.[68])

The Drivers Privacy Protect Act had been in effect only two years, however, when Senate Richard Shelby (R-Ala.), Chairman of the Senate Transportation Committee, introduced a last-minute amendment to the 1999 Transportation Appropriations Act.[69] The amendment eliminated federal highway funds for states that do not require affirmative "opt-in" consent from individuals before information about them contained in driver's and motor vehicle records is used for "surveys, marketing, or solicitation" purposes, thus reversing the position taken by Congress in 1994. With billions of highway funds at stake, no member of Congress wanted to challenge the powerful committee chairman, and the following week, without hearings or opportunity for public comment on the amendment, the bill passed.

No one would argue that this is good legislative process, but it is not unusual for Congress, and good laws have been enacted before through deficient processes. But is this a good law? Is the privacy norm it establishes "effective" and "positive" in light of the five principles identified earlier?

The law certainly reflects a balance: Congress did not prohibit the disclosure of state DMV records for marketing and solicitation purposes, it merely required states to adopt affirmative "opt-in" consent before allowing those records to be used for such purposes. The limited record does not suggest that the Appropriations Committees of either the House or the Senate engaged in any explicit balancing, however, trying to reconcile the need

62. *See* 18 U.S.C. § 2721(a) (1994 & Supp. III 1997).
63. *See id.* § 2721(b)(1).
64. *See id.* §§ 2721(b)(6), (9).
65. *See id.* § 2721(b)(8).
66. *See id.* § 2721(b)(2).
67. *See id.* § 2721(b)(11).
68. *See* Reno v. Condon, 120 S. Ct. 666, 671-72 (2000).
69. *See* Department of Transportation and Related Agencies Appropriations Act of 2000 § 350, Pub. L. No. 106-69; 113 Stat. 986 (1999).

for the restriction with its costs.[70] In fact, anecdotal reports suggest that when the Conference Committee charged with reconciling the House and Senate versions of the Transportation Appropriations bill first considered the Shelby amendment, it was initially opposed by every member, until Senator Shelby threatened to stall the entire bill if the amendment was not included. In any event, there is no record of a specific, individualized balance.

Does the amendment further open information flows? Hardly. Of course, that will be true of most, if not all, laws designed to protect privacy. However, recall that the Shelby amendment replaced the existing "opt-out" system for such uses of DMV records with an "opt-in" system. Both systems give citizens the final, absolute say about the use of DMV data 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 (typically businesses, charities, and alumni/ae organizations that use drivers' license data for marketing and surveys) contacting individuals to obtain their "opt-in" as opposed to concerned individuals contacting organizations (which maintain 800-numbers and fixed addresses and business hours) to express their "opt-out." The amendment, therefore, imposes 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 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 customers' 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 thirty dollars per customer contacted.[71] To gain permission to use such information for mar-

70. *See id.*

71. *See* Brief for Petitioner and Intervenors at 15-16, U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).

keting, 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.[72] In one-third of households called, U.S. West never reached the customer, despite repeated attempts.[73] Consequently, customers received *more calls* than in an "opt-out" system, and many customers were denied opportunities to receive information about valuable new products and services.

The Shelby amendment also fails to reflect the historical understanding of privacy reflected in the Supreme Court's jurisprudence, in that it applies to an expectation of privacy that I doubt is real and I am certain is not reasonable. DMV records have been available to the public virtually without limit since their inception. Even under the DPPA, the permitted uses of those records are vast. Moreover, since the DPPA took effect in 1997, DMVs in the majority of states have displayed notices informing citizens that their records are available for any purpose if they do not "opt-out" of that availability. It therefore seems unlikely that most people thought those records were confidential and even if that was the expectation of some, it was patently unreasonable.

Moreover, while the Shelby amendment applies to government information use, it only restricts one government use of these data—providing them to private parties for marketing or solicitation. The government is still free to collect whatever data it wishes and to use it in any way not regulated by the DPPA or the Shelby amendment. The amendment imposes a far greater restraint on private sector use of data, for example, for alumni associations to locate members, for charities to raise funds, and for direct marketing solicitations. And that restraint comes with no additional privacy protection; the citizens have no greater privacy rights than we did under "opt-out."

Closely related to these concerns is the clear incongruity of the Shelby amendment with the fourth principle—the concept of harm. What is the harm that the Shelby amendment is designed to protect against? Direct marketing? To be sure, few Americans claim to like direct marketing, but more than two-thirds of U.S. consumers—132 million adults—took advantage of direct marketing opportunities in 1998,[74] accounting for more than $1.3 trillion in sales of goods and services.[75] The Direct Marketing Association has long provided a convenient way for consumers to "opt-out" of the use of their personal information by member companies, but

72. *See id.* at 16.

73. *See id.*

74. *See* DIRECT MARKETING ASSOCIATION, ECONOMIC IMPACT: U.S. DIRECT MARKETING TODAY (4th ed. 1998).

75. *See* Financial Privacy Hearings, *supra* note 28, § I ¶ 2 (July 20, 1999) (statement of Richard A. Barton) <http://www.house.gov/banking/72099rba.htm>.

fewer than three percent of U.S. adults avail themselves of that opportunity. The conclusion is inescapable: the vast majority of the public does not believe that direct marketing poses a demonstrable harm.

Finally, does the Shelby amendment reflect the preference for self-help and individual action that we have long favored? The answer is clearly no, especially since it creates a presumption that is contrary to demonstrated consumer behavior, and it substitutes an "opt-in" system for one that allowed citizens to "opt-out" of the use of DMV information about them for direct marketing.

In sum, the DPPA—which, to be fair, Professor Schwartz only uses as a passing example of a practical application of "constituitive privacy"—strikes me as a poor demonstration of the advantages of the more subtle and sensitive, "shifting, multidimensional" understanding of privacy that Professor Schwartz is proposing. Quite the contrary, this scenario suggests that "opt-in" laws will rarely, if ever, be justified, however we define privacy.

IV. CONCLUSION

We need to take privacy seriously. My point is not at all to suggest that privacy is not a real issue; rather, it is to suggest that the political process thus far has not treated it as one. Where the collection and use of nonpublic, personal information poses a real risk of a serious harm, Congress should enact well-drafted, carefully targeted legislation. For example, rather than worry about the use of public information to market valuable products and services, I would like to see Congress consider the issue of whether the mass of information stored in commercial databases is used on an individual basis, for example, when one enterprising snoop obtained Judge Robert Bork's video rental records following his nomination to the Supreme Court. This type of individual use of information, as opposed to broad use for marketing, raises serious issues that Congress has not yet addressed.

Moreover, not all privacy issues require government action. As discussed above, nongovernmental solutions, which are often best facilitated by government *in*action, are the most effective and appropriate protections for privacy. But there can be no doubt that privacy involves real issues and we must consider them seriously, whether or not that consideration ultimately leads to legislation or regulation.

What we are increasingly witnessing is Congress and state legislatures responding to a politically popular issue with poor policy and with poor process. There are regrettably many examples of this. Absence of preemption is perhaps the best one. If Congress really cared about privacy, it would not have allowed every state to enact its own set of privacy standards. The DPPA provides another sad example. Supposedly enacted in

response to the 1989 murder of actress Rebecca Schaeffer, who was stalked by an obsessed fan using information provided by a private investigator from her California DMV record, the law restricts the public's access to motor vehicle records, but not that of private investigators.

California provides another all-too-common example. In an effort to protect privacy, California enacted a statute that 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.[76] 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."[77]

The flood of legislation and regulation suggests that this important subject, which touches on core values at the heart of our democracy and economy, is not getting the thoughtful consideration that it needs. As a result, everybody suffers. Privacy suffers because these ill-considered laws do not provide effective privacy protection. The economy suffers because these restrictions act as a tax, slowing the economy and eroding the benefits of open information flows. And, most importantly, we as individuals and as a society suffer.

76. *See* CAL. GOV'T CODE § 6254(f)(3) (West Supp. 2000).

77. Los Angeles Police Dep't v. United Reporting, 120 S. Ct. 483, 492-93 (1999) (Stevens, J., dissenting).