Public Policy and the Privacy Avalanche

Fred H. Cate

The open flow of information is under attack in the United States as never before in an effort to protect privacy. This issue has united the far right and far left, Republicans and Democrats, federal and state governments, the Eagle Forum and the ACLU, even Phyllis Schlafly and Ralph Nader. It is an issue that in the last two years has generated an avalanche of litigation, legislation, administrative regulations, hearings, press reports, and proposals for more to come in the future. In the past year alone, we have seen comprehensive financial-privacy legislation enacted by Congress,[1] the first federal law prohibiting access to historically-open public records without individual "opt-in" consent,[2] sweeping health-privacy rules proposed by the Clinton administration,[3] children's online-privacy rules promulgated by the Federal Trade Commission,[4] multimillion-dollar settlements of privacy lawsuits,[5] a multistate attorneys general privacy investigation of major banks,[6] the negotiation of a privacy "safe harbor" with European regulators,[7] the appointment of the first-ever privacy official,[8] 356 privacy laws enacted by states,[9] and, most recently, two proposals from the Federal Trade Commission that Congress enact legislation protecting online privacy and guaranteeing individual access and an opportunity to correct personal information.[10]

This unprecedented attention to privacy both reflects and has contributed to widespread popular concern. People are worried about their privacy; poll after poll tells us this. In one 1999 poll published in *The Wall Street Journal*, 29 percent listed loss of privacy as the issue that most concerns them about the next century—ahead of terrorism on US soil (23 percent), world war (16 percent), global warming (16 percent), or economic depression (13 percent).[11] This concern is prompted largely by extraordinary technological innovations that are dramatically expanding

both the practical ability to collect and use personal data, and the economic incentive to do so. Computers and the networks that connect them have become a dominant force in virtually all aspects of society in the United States and throughout the industrialized world. Information services and products today constitute the world's largest economic sector. Institutions and individuals alike are flocking to the Internet—particularly to the World Wide Web—in record numbers, making it the fastest-growing medium in human history.[12] As a result, information, long the "lifeblood that sustains political, social, and business decisions,"[13] has taken on new and dramatically greater importance.

THE PRIVACY AVALANCHE AND CORE INFORMATION VALUES

The problem is that this new legislative and regulatory approach towards dealing with privacy ignores or repudiates a number of core values, especially those reflected in the US Constitution. I want to address briefly six of these.

Open Information Flows

The first is the concept of a free flow of information. The free-flow concept 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 economy."[14]

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. Federal regulations demonstrate a sweeping preference for openness, reflected in the Freedom of Information Act,[15] Government in the Sunshine Act,[16] and dozens of other laws applicable to the government. There are even more laws requir-

ing disclosure by private industry, such as the regulatory disclosures required by securities and commodities laws, banking and insurance laws, and many others. This is a very basic tenet of the society in which we live.

The importance of an open flow of personal information reflects the very practical benefits that such accessibility brings. 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.[17] 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." The more such information is available, he continued, "the more accurately and efficiently will the economy meet those needs and preferences."[18]

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 Edward 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 [*sic*]. 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.[19]

Unfettered use of personal information benefits consumers not only by allowing businesses to ascertain and meet their needs accurately, rapidly, and efficiently, but also because it:

- enhances customer convenience and service;
- permits consumers to be informed rapidly and at low cost of those opportunities in which they are most likely to be interested;
- improves efficiency and significantly reduces the cost of many products and services;
- facilitates a wide range of payment options, including instant credit;
- allows for real consumer mobility, so that consumers can obtain credit, write checks, enjoy frequent-shopper recognition, return goods or have them serviced, and enjoy a wide range of other benefits when they travel or move;
- promotes competition by facilitating the entry of new competitors into established markets, reduces the advantage that large, incumbent firms have over smaller start-ups, and encourages the creation of businesses specialized in satisfying specific consumer needs; and
- facilitates the detection and prevention of fraud and other crimes.

These are real, tangible benefits that consumers enjoy every day and that are not possible without reliable access to personal information. 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.[20] 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 credit 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.[21]

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 impact virtually every facet of American life.…" 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."[22]

Perhaps most importantly, widely-accessible personal information has helped democratize 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, 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 standardized 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, in every sense of the word: Choice as to whether to reveal their identities or not, whether to surf anonymously, whether to disclose information. Choice is taken away if you have legislation that prohibits an activity or makes it unreasonably costly. Direct marketing is a perfect, if mundane, example. I have no particular love for direct-marketing solicitations, but if I am going receive them I had rather get the ones I am most likely to be interested in. Am I better off if direct marketers are prohibited from accessing personal data so that they send me everything or nothing, rather

than offers which are relevant to me? Am I better off if I have to pay more for goods and services because they cannot be target marketed? Am I better off with less choice?—because that is what sweeping privacy laws offer.

The Meaning of "Private"

The Supreme Court has long asked in the context of various constitutional issues, such as 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.[23] There should be no interference with information flows to protect privacy interests that are not reasonable.

The US Court of Appeals for the 4th Circuit highlighted this very point in its decision striking down the 1994 Drivers Privacy Protection Act.[24] 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.[25]

Second, the court found 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."[26] 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."[27]

As the appellate court's language suggests, one long-standing 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. This reflects not only the Supreme Court's interpretation of the Fourth Amendment, but also the common sense that the law should not impose costly or burdensome impediments to the collection and use of information that consumers willingly disclose and that is widely available in the marketplace. To do otherwise results in privacy protections that are nonsensical because they are hopelessly ineffective, contrary to the wishes of individuals, and unnecessary barriers to commerce and customer service.

The Limits of Privacy

The requirement that privacy interests must be reasonable, like the focus on open information flows, reflects an understanding that in a democracy and a market economy privacy is not an unmitigated good. Protecting privacy of information imposes real costs 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.[28]

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 users seeking to verify the accuracy and completeness of information they receive, and the risk of future losses due to 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 First Amendment protection for expression and the Fifth Amendment protection for private property.

As a practical matter, virtually none of us want 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 don't want the pilots to have extensive privacy rights. The Supreme Court has long said that politicians have effectively no privacy rights. There are areas in which each of us intensely believes that we should have privacy rights, but few of us are seriously willing to accord those same privacy rights to others. Across-the-board privacy rights create a situation that is both undesirable and unworkable.

The Concept of Harm

The fourth of these six principles is the concept of harm. We have long recognized that 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. Those instances are actually few and far between, but they nonetheless exist—but only where a specific harm is threatened. This was the view of the US Court of Appeals for the 10th Circuit in *U.S. West, Inc. v. Federal Communications Commission* (which the Supreme Court in June, 2000, declined to review), when it struck down the FCC rules requiring telephone companies to 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.[29]

The harm principle has largely been lost in the flood of privacy legislation. This is a very significant issue, for at least three reasons. The first is that we have historically required 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?

The second concern is that if you don't know what the harm is, you don't know what type of law is necessary to address it or whether a proposed law does in fact address it. For instance, one widely-cited example of the need for greater financial-privacy regulation involves Minneapolis-based U.S. Bancorp, which has been accused of selling customer data to MemberWorks, a telemarketing company, for $4 million. The sale allegedly violated both U.S. Bancorp's promise to its customers not to sell such data and the Fair Credit Reporting Act. Some of U.S. Bancorp's customers also reported fraudulent charges for MemberWorks' products. In July, 1999, U.S. Bancorp settled a suit brought by the Minnesota attorney general, without admitting wrongdoing, by agreeing to new disclosure policies and paying about $3 million to the state and charitable organizations.[30]

But as the outcome of that case shows, what U.S. Bancorp was charged with doing already violated both the federal and state consumer-protection laws. U.S. Bancorp paid $3 million in fines. This case is not a poster child for why more regulation is needed, but rather a shining example of how well existing law works.

Another example of the inadequacy of current privacy law is the fear that information, particularly medical information, will be used to discriminate in a financial or employment context. The merger of Citibank and Travelers Insurance has been widely cited as a key example of the "potential for the risky sharing of financial and medical information for marketing or underwriting purposes."[31] But remember, legitimate, lawful business activities routinely involve using personal information to discriminate among potential consumers. Only consumers meeting certain financial criteria are offered pre-approved credit cards. Only consumers likely to be interested in a given direct-marketing opportunity are targeted to receive a solicitation.

Medical information may be more sensitive, but even its use, provided such use is within the law, raises similar issues. "Discrimination" is the business of insurance underwriting. So we should hesitate before assuming discrimination is always bad. It is not intrinsically unreasonable for a lender to want to know whether a borrower is likely to pay off a loan, or to require insurance for the loan if she is reasonably unlikely—for whatever reason—to be able to. This is especially true if the borrower possesses, but does not disclose to the lender, relevant information about her health. Even if discrimination is clearly harmful, the most efficient and practical response is to outlaw the discrimination. Restricting information flows to protect against unlawful discrimination is like using a hammer to swat a fly: It may get the job done, but it causes a lot of collateral damage, especially if the fly is resting on your head. Restricting information flows to protect against *lawful* discrimination is nonsensical.

The third concern in this harm concept is that if you cannot identify a specific harm, it raises the specter there may be some other, undisclosed purpose—unrelated to protecting privacy—motivating the regulation. Privacy, as some public officials

have already demonstrated, is often an effective lever to use to obtain some other, unrelated concession from companies.

The Importance of Balance

As suggested by the discussion of a number of principles above, the fifth core principle is the concept of balance. As important as open information flows may be, there are occasions, when a sufficiently-great harm is threatened if information that is reasonably believed to be private is disclosed, that the law will properly protect against its disclosure. But efforts to enhance personal privacy must be weighed against the costs that those efforts impose on the free flow of information, the election and supervision of governments, the development of efficient markets, and the provision of valuable services.

Put simply, privacy protections must be proportional to the interest they are designed to serve. This principle is not only suggested by a common-sense regard for the benefits that flow from open information, but also is mandated by the First Amendment to the US Constitution. 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. For example, when information is true and obtained lawfully, the Supreme Court repeatedly has held that the state may not restrict its publication without showing that the government's interest in doing so is "compelling" and that the restriction is no greater than is necessary to achieve that interest.[32] Under this standard, the Court has struck down laws restricting the publication of confidential government reports[33] and of the names of judges under investigation,[34] juvenile suspects,[35] and rape victims.[36]

Even if the information is considered to be "commercial," its collection and use is nevertheless 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" that interest and is "narrowly tailored to achieve the desired objective."[37] In *U.S. West, Inc. v. Federal Communications*

Commission, the US Court of Appeals for the 10th Circuit specifically found that (1) the FCC's privacy rules limiting the use of personal information about telephone subscribers restricted speech and therefore were subject to First Amendment review; (2) under the First Amendment, the FCC bore the burden of proving its rules were constitutional; and (3) constitutional burden required the FCC to demonstrate that the rules were "no more extensive than necessary to serve [the stated] interests."[38] Specifically, the appellate court found that the government's choice of means to protect privacy must 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.'[39]

Balance is therefore a constitutional obligation.

Moreover, it is important to note the strong historical preference—also reflected in the 10th Circuit's decision in *U.S. West*—for sensitive balances that result in no more information than necessary being restricted in order to protect privacy. Consider just one specific example: The commonwealth of Massachusetts had a statute which required trial-court judges to close all criminal trials when minor victims of sexual offenses testified. In 1982 the Supreme Court struck down the statute as unconstitutional.[40] It is difficult to imagine a stronger privacy interest than that of minor victims of sexual offenses who are having to testify at trial. But even in that instance the Supreme Court said the state may not enact an across-the-board rule closing trials:

> 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.[41]

Laws that put in place broad restrictions on the flow of information, rather than requiring sensitive balances to prevent specified harms, are constitutionally problematic.

Distrust of Government and Preference for Self-Help

Finally, the sixth of these principles at issue in the current rash of legislation is the concept of self-help and a distrust of government. The new quest for government intervention to protect privacy is ironic, because privacy protection in the United States, probably the greatest level of protection in the world, has historically focused on *government* access to information. We have restricted the government from coming into our homes, from invading our cars, from searching our places of work, from tapping our phones. We are now turning that principle on its head, asking the government to intrude into our lives to protect our information. According to Jane Kirtley, former executive director of the Reporters Committee for Freedom of the Press, the expectation 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.[42]

This is not only ironic, it is unprecedented in the United States. Remember, constitutional rights in the United States are generally "negative" and apply only against the government, not private parties.[43] Those rights do not obligate the government to *do* anything, but rather to *refrain* from unnecessarily interfering with individuals' freedom to act. This also explains the very high protection in US law for private agreements.

Citizens do not have to make promises to one another, but when we do, the government makes available valuable resources to enforce those promises.[44]

This preference for private action and individual responsibility is especially clear when information is involved. The US Supreme 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, "the remedy to be applied is more speech, not enforced silence."[45]

The focus on individual and collective private action inevitably restrains the power of the government to pass sweeping privacy laws. But it also facilitates considerable privacy protection through the use of technologies, markets, industry self-regulation and competitive behavior, and individual judgment. 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 associations 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.[46]

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.

What makes this even more ironic is that the very technologies that we are so worried about, for example the Internet, are precisely the tools that make it possible to shop anonymously, to browse anonymously, to visit a web site without being identified. Even direct marketing, the business we love to hate (although more than two-thirds of US consumers—132 million adults—took advantage of direct-marketing opportunities in 1998,[47] accounting for more than $1.3 trillion in sales of goods and services,[48] the use of personal information for direct marketing attracts nearly universal scorn), allows you to stay at home and shop from offers preselected to be of interest. Think about that from a privacy point of view. You don't even have to expose your face to the light of day in order to engage in this activity. Information technologies, and the services they make possible, make privacy realistically possible for many Americans for the first time ever. Unlike small-town America, where everybody knew everyone's business, these technologies offer the promise of real anonymity and, as is discussed in further detail below, real control over what personal information to disclose, and to whom. Yet this is what we are trying to regulate, and we are asking the government to do it for us.

Laws and regulations designed to protect privacy may actually weaken it by ignoring, and even interfering with, the power of new technologies to protect privacy. 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 facilitates a vibrant market for privacy protection, whether in the form of online privacy certifications like BBB*Online* and TRUSTe, or complete privacy-protecting services like the recently unveiled iPrivacy, making 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.

If privacy enactments make the Internet an inhospitable place for businesses to offer services and for consumers to shop, those opportunities for technological privacy protection will no longer exist. If the law creates a disincentive for developing privacy-protection tools, then consumers will be left with less protection, not more. Remember, technologies can actually and completely protect privacy; law cannot. At best, the law can create disincentives for data collection and use, and then impose penalties for engaging in prohibited practices, but this is only effective if: (a) the illegal use is discovered; (b) the user is identified; (c) the user is subject to the law or regulation and within the jurisdiction of an appropriate court or administrative agency; (d) the aggrieved data subject has the wherewithal or obtains the cooperation of a government agency to pursue the data user in court; (e) the aggrieved data subject can prove her allegations in court; (f) a judge or jury finds the user guilty and assess a fine or other penalty; and (g) the penalty can be enforced. As this litany makes clear, while privacy laws and regulations can cause considerable damage to society and the economy, they often provide very little privacy protection and none whatsoever against data users outside of the country. I would rather have the real privacy that technologies make possible than have a legal right to sue. To the extent we eliminate the incentive for the development of technological protections for privacy, not just online but in many other settings, we diminish the availability of real privacy for everyone.

THE FAILURE OF PUBLIC POLICYMAKING

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. This is especially true in view of the increasing globalization of infor-

mation and information technologies like the Internet. The hundreds of state and local privacy laws that have been adopted in the past year alone are merely the most recent evidence of an expanding phenomenon: the effort to use national or subnational law to deal with fundamentally global issues. Information is inherently global. It is because of its inherently-global character that information has been the subject of some of the earliest multinational agreements, treaties, and organizations—dating back to 1601.[49] In fact, the Postal Congress of Berne in 1874 established a multinational postal regime—administered today by the Universal Postal Union—74 years before the General Agreement on Tariffs and Trade was opened for signature.[50]

Today, when data processing is wholly dominated by networked computers, information is difficult to pinpoint and almost impossible to block, through either legal or technological means. Digital information not only ignores national borders, but also those of states, territories, and even individual institutions. Not surprisingly, the inherently global nature of digital information poses extraordinary challenges to the power of national—much less state—governments, and efforts to use national—much less local—law to regulate information in one jurisdiction often pose substantial legal and practical issues in another. At a time in which we are looking at increasingly global activities—global business, global mergers, global shopping, global travel—Congress' most recent decision on privacy is nonsensical. With the Gramm-Leach-Bliley Financial Services Modernization Act,[51] states are expressly permitted to enact their own, more restrictive privacy laws, devolving privacy regulation to the local level. Inconsistent, local regulation at a time when everything else is moving toward centralization and globalization is by definition ineffective and imposes high costs while providing poor privacy protection.

The Drivers Privacy Protection Act 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 Department of Motor Vehicles record, the law

restricts the public's access to motor vehicle records, but not the access 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.[52] 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."[53]

The flood of legislation and regulation suggests this important subject, which touches on core values at the heart of our democracy and economy, is not getting the thoughtful consideration it needs. As a result, everybody suffers. Privacy suffers, because these ill-considered laws do not provide effective protection, while their proponents falsely encourage the public to believe that they do, thereby discouraging the development and use of self-help privacy protections. 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.

THE VIEW FORWARD

Taking Privacy Seriously

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, as 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.

Putting Privacy in Perspective

Privacy is important, but it is not the only value the public and this society treasure. Privacy is always in tension with other values—the benefits that come from the open flow of information, freedom from government intrusion in private markets and private lives, the prevention and detection of crime, consumer convenience, and countless other values we seek and increasingly expect every day. If protecting privacy means we no longer enjoy these and other benefits, the cost of privacy may simply be too great. And if the means we use to protect privacy are overly broad or intrusive, much of the cost of that protection will have been unnecessary.

The goal of all privacy law and regulation, therefore, should be achieving a balance between the value of open flow of information and the value of enhanced privacy protection to guarantee for consumers the maximum practicable benefit. 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. Therefore, privacy-protection tools should give maximum control to individual consumers rather than require the government to decided an appropriate level of privacy protection for all. 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.

Most privacy advocates regard "choice" as the foundation of consumer privacy protections. Unfortunately, the current privacy debate has largely reduced "choice" to the issue of whether a consumer consents to the collection and use of personal information and the method by which that consent is sought. While choice certainly includes consent, the choice principle is actually much broader. It includes the consumer'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 businesses offering different privacy protections. As we have already seen, choice is most often facilitated, not restricted, by the open flow of information. Choice requires that consumers have the right to choose among competing privacy policies, and obligates the government to preserve to the greatest degree possible a competitive market offering a variety of levels and means (and corresponding costs) of privacy protection.

Legislation that proposes a one-size-fits-all approach to privacy should therefore be avoided as posing constitutional problems, interfering with consumer choice, and taking privacy out of its proper perspective.

The Need for Education

We have done a poor job of educating the public, the press, and policymakers about privacy issues and the significant ramifications of regulating information flows inappropriately or unnecessarily. Researchers and organizations that work with information and study its use and regulation have sat back and allowed privacy extremists to come forward with horror stories which often have little to do with privacy or which involve the clear violation of existing laws. The pro-information community has remained lamentably silent or has merely reacted to these anecdotes. As a result, privacy extremists have largely defined the agenda for political and public debate.

It is time that the users of information and the people who study information step forward and begin educating people about the value of open information flows, the danger of letting the government protect your privacy, and the risks posed by overly-broad privacy laws and regulations. Some new educational initiatives are underway—such as the Privacy Leadership Initiative[54] and Privacy Partnership 2000[55]—but we need to do more to refocus attention on the core values that have historically undergirded this information society and demonstrate the continuing vitality of, and need for, those principles, before we lose them entirely.

The Need for Research

We need to develop more and better data to demonstrate the value of open information flows and quantify the costs of restricting those flows to protect privacy. One of the reasons that Congress and state legislatures have done such a poor job balancing privacy with open information flows is that both industry and academia have done an even worse job providing the data necessary for crafting that balance. I recognize this is always the academic's cry: We need more data. But this is an area where we have surprisingly little, and the stakes of policymaking in the absence of those data are, as we have seen, very high. What is the value of information in the economy? What does a privacy bill cost? How much does an accessible public record contribute to the economy? There is some exciting new research just beginning, but there is much more work to be done and it needs to be started now, *before* further legislative and regulatory action, not after.

Standing Firm

Finally, while many businesses do and must make the political compromises necessary to survive, it is essential the business community and other institutions recognize that core values and principles are at stake, as well as the health of the most robust information economy in the world, in the debate over the government's role in protecting privacy. It is vital that we stand

firm on these key issues—that we not give away these basic rights, not compromise these constitutional values, not cut a deal to stave off one particularly bad bill that ultimately erodes our entire information infrastructure.

I believe that today we are looking only at a tidal swell that will ultimately turn into a giant wave of privacy legislation, regulation, investigations, and lawsuits. We think the 356 state privacy bills enacted in 1999 is a large number, but I fear that it will pale in comparison to the number to come. Today we are debating "opt-in" versus "opt-out." It won't be long before we are facing restrictions on any use of personal information whatsoever. Today, we are fighting over grocery stores' use of their frequent shoppers' data; it won't be long before we are fighting laws that restrict the right of grocery stores to even identify frequent shoppers or to offer them discounts—laws that have precious little to do with privacy, but that will be carried along, caught up in its powerful rhetoric.

I am not arguing against meaningful discussion of important privacy issues, or efforts to understand better the privacy risks posed by new technologies and applications. But the stakes are simply too great to compromise away the core values and principles that undergird our economy, our democracy, and our society.

Notes

[1] Gramm-Leach-Bliley Financial Services Modernization Act (S. 900), 106 Pub. L. No. 102, 113 Stat. 1338, 1436-1450, Title V (1999).

[2] Department of Transportation and Related Agencies Appropriations Act, 2000 (H.R. 2084), Pub. L. No. 106-69, 113 Stat. 986, 1025-1026, § 350 (1999).

[3] Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (November 3, 1999; HHS, proposed rule), 64 Fed. Reg. 69,981 (December 15, 1999; extending deadline for comment), 65 Fed. Reg. 427 (January 5, 2000; correcting original notice).

[4] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (November 3, 1999; FTC, final rule; codified at 16 C.F.R. pt. 312).

[5] In 1998, NationsBank, without admitting fault, paid $7 million in civil penalties for sharing information about maturing-CD holders with an affiliate, which then marketed risky derivative funds to those customers without

disclosing the risks and other material terms of the transaction. See In the Matter of NationsSecurities and NationsBank, N.A., Securities Act of 1933 Release No. 7532, Securities Exchange Act of 1934 Release No. 39947, Admin. Proceeding File No. 3- 9596 (May 4, 1998; SEC, finding and order), available at http://www.sec.gov/enforce/adminact/337532.txt. In July, 1999, U.S. Bancorp settled, without admitting wrongdoing, a suit brought by the Minnesota attorney general which accused the company of illegally selling customer data; U.S. Bancorp agreed to new disclosure policies and payed about $3 million to the state and charitable organizations. See Holden Lewis, "The devil you *don't* know: Strange banks are selling your private information, too," bankrate.com, October 8, 1999, available at http://www.bankrate.com/brm/news/bank/19991008.asp; Jeff Leeds, "Bank Sold Credit Card Data to Felon," *Los Angeles Times*, September 11, 1999.

[6] Robert O'Harrow, Jr., "A Postscript on Privacy; Bank Bill's Late Change Gives States Last Word," *The Washington Post*, November 5, 1999; Marcy Gordon, "States Challenge Information-Sharing in New Banking Measure," *The Commercial Appeal* (Memphis, Tennessee), November 6, 1999.

[7] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666, July 24, 2000 (International Trade Administration, Department of Commerce, Notice), available at: http://www.ita.doc.gov/td/ecom/menu.html.

[8] "White House Hires Aide To Guide Privacy Policy," *The New York Times*, March 4, 1999.

[9] "Privacy Legislation in the States—1999 Trends," *Privacy & American Business* (September/October 1999), at 1, 3.

[10] Federal Trade Commission, "Online Profiling: A Report to Congress (Part 2)—Recommendations" (July 2000), available at http://www.ftc.gov/os/2000/07/onlineprofiling.pdf; Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress" (May 2000), available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[11] Christine Harvey, "American Opinion (A Special Report): Optimism Outduels Pessimism," *The Wall Street Journal*, September 16, 1999.

[12] Only five years after its creation, it reached more than 50 million homes in the United States. By comparison, it took 38 years for radio to reach 50 million US homes, 13 years for television, and 10 years for cable.

[13] Anne W. Branscomb, "Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition," 36 *Vanderbilt Law Review* 985, 987 (1983).

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

[15] 5 U.S.C. § 552.

[16] 5 U.S.C. § 552b.

[17] Fred L. Smith, Jr., "Better to Share Information," *Desert News* (Salt Lake City, Utah), October 14, 1999.
[18] Financial Privacy Hearings before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Banking and Financial Services, House of Representatives, 106th Congress, 1st Session, July 20, 1999 (statement of Edward M. Gramlich), available at http://www.house.gov/banking/72199gra.htm.
[19] Letter from Alan Greenspan to Edward J. Markey, July 28, 1998, available at http://www.house.gov/markey/980728letterr.htm.
[20] Walter F. Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns*, 7 (The Tower Group 1999).
[21] See Fred H. Cate, *Personal Information in Financial Services: The Value of a Balanced Flow* (2000).
[22] Fred H. Cate and Richard J. Varn, *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance*, 10, 13 (1999).
[23] *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).
[24] Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified at 18 U.S.C. §§ 2721-2725).
[25] *Condon v. Reno*, 155 F.3d 453, 464 (4th Cir. 1998), reversed on other grounds, *Reno v. Condon*, 120 S. Ct. 666 (2000).
[26] Ibid. at 465.
[27] Ibid.
[28] Richard A. Posner, "The Right of Privacy," 12 *Georgia Law Review* 393, 399 (1978).
[29] *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999) cert. denied, 120 S. Ct. 1240 (2000) (emphasis added).
[30] Lewis, "The devil you *don't* know," supra.
[31] Financial Privacy Hearings, supra (statement of Edmund Mierzwinski).
[32] *Florida Star v. B.J.F.*, 491 U.S. 524 (1989); *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979); *Landmark Communications Inc. v. Virginia*, 435 U.S. 829 (1978); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975).
[33] *New York Times Co. v. United States*, 403 U.S. 713 (1971).
[34] *Landmark Communications, Inc. v. Virginia*, supra.
[35] *Smith v. Daily Mail Publishing Co*., supra.
[36] *Florida Star v. B.J.F.*; *Cox Broadcasting Corp. v. Cohn*, supra.
[37] *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).
[38] 182 F.2d at 1235, quoting *Rubin v. Coors Brewing Co*., 514 U.S. 476, 486 (1995).
[39] Ibid., 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).
[40] *Globe Newspaper Company v. Superior Court*, 457 U.S. 596 (1982).
[41] Ibid. at 611 n. 27.
[42] Jane E. Kirtley, "The EU Data Protection and the First Amendment: Why a 'Press Exemption' Won't Work," 80 *Iowa Law Review* 639, 648-49 (1995).
[43] Only the 13th Amendment, which prohibits slavery, applies to private parties. *Clyatt v. United States*, 197 U.S. 207, 216-220 (1905).
[44] See *e.g.* 15 U.S.C. § 57b-1.
[45] *Whitney v. California*, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring). See *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 498 (1996); *Texas v. Johnson*, 491 U.S. 397, 419 (1989).
[46] Federal Trade Commission, "Individual Reference Services: A Report to Congress" (1997), available at http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.
[47] Direct Marketing Association, *Economic Impact: U.S. Direct Marketing Today*, 4th ed. (1998).
[48] Financial Privacy Hearings, supra (statement of Richard A. Barton).
[49] Ludwig Weber, "Postal Communications, International Regulation," 5 *Encyclopedia of Public International Law* 238 (1983).
[50] Ibid.; General Agreement on Tariffs and Trade, opened for signature January 1, 1948, 61 Stat. (5), (6), T.I.A.S. No. 1700, 55 U.N.T.S. 188. See generally Fred H. Cate, "Introduction—Sovereignty and the Globalization of Intellectual Property," 6 *Ind. J. Global Leg. Stud*., 1 (1998).
[51] Gramm-Leach-Bliley Act, §§ 507, 524 (1999).
[52] Cal. Govt. Code § 6254(f)(3).
[53] *Los Angeles Police Department v. United Reporting Publishing Corp*, 528 U.S. 32, 120 S. Ct. 483 (1999) (Stevens, J., dissenting).
[54] The initial members are AT&T, Compaq Computer, Dell Computer, DoubleClick, E*TRADE, Eastman Kodak Company, Engage, Experian, Ford Motor Company, Harris Interactive, IBM, Intel Corporation, Network Solutions, Procter & Gamble, Sony, Travelocity.com, and US Bank.
[55] The Partnership is comprised of 36 companies including America Online, Intel, AltaVista, Microsoft, Excite@Home, IBM, and Yahoo.