FIRST REPORTS

VOL. 4, NO. 1 MARCH 2003

The Privacy Problem

A broader view of information privacy and the costs and consequences of protecting it

BY FRED H. CATE

A FIRST AMENDMENT CENTER PUBLICATION

FIRST AMENDMENT CENTER
FUNDED BY THE FREEDOM FORUM

Fred H. Cate is a distinguished professor, Ira C. Batman Faculty fellow and director of the Center for Applied Cybersecurity Research at the Indiana University School of Law-Bloomington. He specializes in privacy and other information-law issues and appears regularly before Congress, state legislatures and professional and industry groups on these matters.

He has directed the Electronic Information Privacy and Commerce Study for the Brookings Institution and has served as a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He is a visiting scholar at the American Enterprise Institute and a senior policy adviser at the Hunton & Williams Center for Information Policy Leadership.

Cate is the author of many articles and books concerning privacy and information law, including *Privacy in Perspective* (AEI Press), *Privacy in the Information Age* (Brookings Institution Press) and *The Internet and the First Amendment* (Phi Delta Kappa). He is the co-author (with Marc Franklin and David Anderson) of the sixth edition of the best-selling *Mass Media Law* (Foundation Press).

A graduate of Stanford University and Stanford Law School, Cate is a member of the Phi Beta Kappa Senate and of the board of directors of the Phi Beta Kappa Fellows, and is listed in *Who's Who in America* and *Who's Who in American Law*.

The Privacy Problem

A broader view of information privacy and the costs and consequences of protecting it

BY FRED H. CATE

A debate is raging over the privacy of personal information and the role of law in protecting it. Opinion polls report that the public is worried about privacy, believes privacy is threatened as much by businesses as by the government, and does not trust either to protect it. As a result, polls show considerable support for expanding the legal rights of individuals to control data about themselves.

Public concern about privacy is manifesting itself in many forms: press conferences, op-eds, legislative hearings and study commissions, attorneys general and Federal Trade Commission investigations and lawsuits. Angst about privacy has given rise to an entire new industry of corporate privacy officers, consultants, conferences and books.

We have also seen a wave of new laws and regulations. While only a small percentage of the more than 600 privacy bills proposed in Congress and state legislatures during the past four years has been enacted, these new laws are fundamentally altering the ways in which information is collected and used.

The problem, from the perspective of rational policymaking, is that privacy is not a simple or isolated issue. Its protection through law inevitably conflicts with other important values and imposes costs — financial and otherwise. The privacy debate to date has tended to ignore those other values and costs, in part because of the unusual features of the debate.

- Privacy is an unusually broad term, encompassing both fundamental constitutional rights (such as freedom from government intrusions into homes and the right of citizens to make decisions about marriage, contraception and abortion) and less well-defined, and arguably less critical, issues (such as the desire to be free from annoying direct marketing calls and mailings).

- Privacy is a subjective and often emotional issue: What threatens one individual's sense of privacy may not concern another person.

- The role of information flows in markets is a complex subject, usually of greater interest to economists than consumers. Nonetheless, most people believe that they intuitively understand the privacy issues raised by those flows and know, at least, how their own privacy should be protected.

- Most people regard privacy, or at least their own privacy, as deserving of as much protection as possible: If a little is good, more is better.

- The rhetoric of the privacy debate is one-sided. "Just as no one is 'pro-abortion' or 'anti-life,'" former Netscape counsel Kent Walker has written, "No one can be 'anti-privacy,' yet that's the only label left by the rhetoric."[1]

One of the most significant values threatened by new privacy laws is the flow of information necessary to a democracy and a free press. Granting individuals greater control over information about them inevitably means allowing them to restrict access to and use of that information by the public and the press. In recent years privacy concerns have been asserted as a justification for closing traditionally open public records and for blocking or penalizing publication of accurate facts.

The existence of competing values and compliance costs does not mean that the law should not protect privacy. But it does heighten the need to weigh

those values and costs carefully before adopting new restrictions on information flows, even when those restrictions are designed to serve a valuable purpose.

A HISTORICAL PERSPECTIVE

Privacy law originated in the United States with the 1890 publication of Louis Brandeis and Samuel Warren's article, "The Right to Privacy," in the *Harvard Law Review*.[2] Brandeis and Warren, concerned that the press, armed with "instantaneous photographs" and "numerous mechanical devices," was "overstepping in every direction the obvious bounds of propriety and of decency," proposed the creation of a tort for invasion of privacy by the press. That article and its authors laid the foundation for the two dominant strands of U.S. privacy law: protection against government invasions of citizen privacy, and protection against harmful uses of personal information.

The U.S. Supreme Court's first and best developed concept of privacy emerged from then-Supreme Court Justice Brandeis' 1928 dissent in *Olmstead v. United States*.[3] Five of the nine justices had found that wiretapping of telephone wires by federal officials did not constitute a search or seizure since there had been no physical trespass and nothing tangible had been taken. Justice Brandeis disagreed: "The makers of our Constitution … conferred, as against the Government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men."[4]

Almost 40 years later, the Court adopted Justice Brandeis' reasoning in *Katz v. United States*.[5] The protected zone of Fourth Amendment privacy is defined by the individual's "actual," subjective expectation of privacy and the extent to which that expectation is "one that society was prepared to recognize as 'reasonable.'"[6]

Protection of privacy from government intrusion has expanded beyond the Fourth Amendment area to include a more general constitutional right against government-compelled "disclosure of personal matters"[7] and a variety of statutory provisions limiting the power of the government to compel the disclosure of personal information and protecting against misuse of personal information possessed by the government.

This focus on government intrusion reflects the reality that only the government exercises the power to compel disclosure of information and to impose civil and criminal penalties for noncompliance. Only the government collects and uses information free from market competition and consumer preferences. It is therefore not surprising that the Supreme Court has interpreted the Bill of Rights to restrict the government's collection and use of personal information.

Warren and Brandeis also were influential in the development of the second strand of U.S. privacy law — protection against harmful disclosures of personal information. By 1960, courts in many states had recognized some form of the common-law privacy tort that Warren and Brandeis had advocated.

Three varieties of that tort are relevant to information privacy. The tort of unreasonable intrusion into the seclusion of another requires that the intrusion involve "solitude or seclusion of another or his private affairs or concerns" and that it be "highly offensive to a reasonable person."[8] The tort of "unreasonable publicity given to the other's private life" applies when there is public disclosure of private information that would be "highly offensive to a reasonable person" and is not of "legitimate public concern to the public."[9] These torts are recognized in all but six states.

The third privacy tort is "publicity that unreasonably places the other in a false light before the public." To be actionable under the false light tort, the publication must be both false and highly offensive to a reasonable person.[10] In 1967, the Supreme Court extended the First Amendment privileges previously recognized in the context of defamation to actions for false light privacy.[11] The Court thus requires plaintiffs to show that the defendant knew the publication was false or recklessly disregarded its truth or falsity. Fewer than two-thirds of states recognize this tort.

The privacy torts, then, apply only when the information is "highly offensive to a reasonable person" and either false or of no "legitimate public concern." They are designed to remedy only a narrow category of harmful uses of information. Because the torts restrict expression and therefore must withstand First Amendment review,

they are rarely successful. To date, only one award to a privacy tort plaintiff has ever survived the Supreme Court's First Amendment scrutiny.[12]

Other laws designed to address the collection or use of personal information by the private sector have, until recently, reflected a similarly narrow focus on preventing harms. The Fair Credit Reporting Act, for example, one of the earliest privacy statutes applicable to the private sector, focuses primarily on correcting inaccuracies and assuring that credit information is not used in ways that could harm consumers.[13]

These were the two dominant spheres of privacy law into the early 1990s: protection against invasion by the government and protection against highly offensive, harmful disclosures of personal information to the public.

THE NEW FACE OF PRIVACY PROTECTION

By the mid-1990s, however, a variety of developments prompted new concerns about privacy: the proliferation of new technologies; the spread of privacy law in Europe; public perceptions of increasingly invasive press stories; a new awareness of how much personal information is collected and used; and the growth of identity theft. Although these concerns have not excluded the government, they have focused primarily on information collection and use by the private sector. And the remedy that polls suggest most people favor — and that legislators have sought to provide — is to grant consumers a legal right to control the collection and use of information about them.

In fact, the dominant trend in recent and pending privacy legislation is to invest consumers with control over information in the marketplace, irrespective of whether the information is, or could be, used to cause harm. Public officials and privacy advocates argue that "we must assure consumers that they have full control over their personal information" and that privacy is "an issue that will not go away until every single American has the right to control how their personal information is or isn't used."[14] And virtually all of the privacy bills pending before Congress

reflect this goal: "To strengthen control by consumers" and "to provide greater individual control."[15]

William Safire summed up this movement in 1999 when he wrote in *The New York Times:* "Your bank account, your health record, your genetic code, your personal and shopping habits and sexual interests are your own business. That information has value. If anybody wants to pay for an intimate look inside your life, let them make you an offer and you'll think about it." Safire concluded: "[E]xcepting legitimate needs of law enforcement and public interest, control of information must rest with the person himself."[16]

New privacy laws and regulations reflect the focus on control of information without regard for whether the information could be used to cause harm:

Financial Information. On Nov. 4, 1999, Congress removed decades-old barriers within the financial services industry with passage of the Gramm-Leach-Bliley Financial Services Modernization Act.[17] Title V, which regulates the collection and use of information about customers, took effect on July 1, 2001. The new law permits a financial institution to transfer any "nonpublic personal information" to nonaffiliated third parties only if the institution "clearly and conspicuously" provides consumers with a notice about its information-disclosure policies and an opportunity to opt out of such transfers. That notice, which must be sent at least annually, must include:

- the policies and practices of the financial institution with respect to disclosing nonpublic personal information about current and former customers to nonaffiliated third parties, including the categories of persons to whom the information is or may be disclosed;

- the categories of nonpublic personal information that the financial institution collects;

- the policies and practices that the financial institution maintains to protect the confidentiality and security of nonpublic personal information; and

- any other disclosures required by law.[18]

The act provides certain exceptions to the notice and opt-out requirements when, for example, the use of information is necessary to provide a product or service requested by a customer, maintain a customer's account, to resell a loan, to protect against fraud or other liability, to resolve disputes with the customer, to facilitate a merger, to market the financial institution's own products or services, or to comply with applicable laws or the requirements of self-regulatory organizations, rating agencies, government officials and consumer reporting agencies.[19]

The scope of Gramm-Leach-Bliley is broader than its title might at first suggest. The term "financial services" includes all insurance-related activities, real or personal property leases, investment advisory services, tax planning, management consulting, financial career counseling, the extension of credit to consumers by any institution and any other activity in which a financial holding company is permitted to engage.[20] The law applies to anyone who is "significantly engaged" in one or more of these activities. Moreover, the law restricts anyone, whether or not they provide a financial service, from redisclosing personal information received from a financial institution.

Health Information. In April 2001, the Department of Health and Human Services, as required by the Health Insurance Portability and Accountability Act, adopted rules protecting the privacy of personal health information.[21] The rules proved so complicated and controversial that, even before going into effect, they were the subject of a published "clarification" and then, less than a year later, wholesale amendment.[22]

As amended, the rules regulate the use of information that identifies, or reasonably could be used to identify, an individual and that relates to physical or mental health, the provision of health care to an individual or payment for health care.

The rules apply to "covered entities," namely, anyone who provides or pays for health care in the normal course of business.

A covered entity may use personal health information to provide or obtain payment for health care only after first providing the patient with notice and making a good faith effort to obtain an "acknowledgment."[23] Notices must meet detailed requirements set forth in the rules; proof of providing notice and acknowledgments must be retained for six years after the date on which service is last provided.

A covered entity may use personal health information for purposes other than treatment or payment only with an individual's opt-in "authorization."[24] An authorization must be an independent document that specifically identifies the information to be used or disclosed, the purposes of the use or disclosure, the person or entity to whom a disclosure may be made and other information. A covered entity may not require an individual to sign an authorization as a condition of receiving treatment or participating in a health plan.

The rules contain a number of exceptions, under which personal health information may be used with neither consent nor authorization, for example, for public health activities; to report victims of abuse, neglect or domestic violence; in judicial and administrative proceedings; and for certain law enforcement activities. The rules actually lower the protection afforded personal health information from government collection and use.

Covered entities must make reasonable efforts to limit the use and disclosure of personal health information to the minimum necessary to accomplish the intended purpose. They may disclose personal health information to a business associate (such as a billing company, third party administrator, attorney or consultant) only if the covered entity has a contract ensuring that the business associate will be bound by all of the obligations applicable to the covered entity, and that at the termination of the contract, the business associate will destroy or return all personal health information.

Children's Information Online. The Children's Online Privacy Protection Act of 1998 applies to operators of Web sites directed to children under 13 or who

knowingly collect personal information from children under 13 on the Internet. Such operators must provide parents with notice of their information practices and obtain prior, verifiable opt-in parental consent for the collection, use and/or disclosure of personal information from children (with certain limited exceptions).[25] The law gives parents the right to review the personal information collected from their children and to prevent the further use of personal information that has already been collected or the future collection of personal information from that child. The law limits the collection of personal information for a child's online participation in a game, prize offer or other activity to information that is reasonably necessary for the activity, and requires that Web site operators have reasonable procedures to protect the confidentiality, security and integrity of the personal information collected from children.

Public Records. Congress enacted the Driver's Privacy Protection Act of 1994 in response to the 1989 murder of actress Rebecca Schaeffer.[26] Schaeffer had been killed by an obsessed fan who reportedly obtained her address, through a private investigator, from her California Department of Motor Vehicles 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 14 exemptions, including use by any government agency, insurance company or licensed private investigator. The law permits states to release information from driver's records if the DMV has provided drivers with the opportunity to opt out of such disclosures.

The DPPA took effect in 1997, by which time a majority of states had enacted 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 authority to compel them to regulate access to their state records. On Jan. 12, 2000, the Supreme Court ruled in *Reno v. Condon* that Congress did possess the necessary authority.[27])

The DPPA had been in effect only two years, however, when Congress amended it to require that states, as a condition of receiving federal highway funds, obtain affirmative opt-in consent from individuals before information about them

contained in motor vehicle records is used for "surveys, marketing, or solicitation" purposes.[28]

A majority of states have adopted other laws and executive orders restricting access to traditionally open public records, such as hunting and fishing license registration forms, autopsy reports, drivers license photos and state employee address information, without first obtaining the consent of the individuals involved.

Collectively, these enactments reflect a much broader view of privacy than previously recognized by U.S. law. They focus on information collection and use by the private sector, not the government — in fact, some would make it easier for the government to access personal information. And they do not purport to restrict or punish only harmful uses of information. Rather, except for a few specific exemptions, they condition the collection and use of broad categories of information on consumer consent. All but the Gramm-Leach-Bliley law require opt-in consent. And they impose broad notice and record-keeping requirements on those who would seek to collect and use personal information.

These enactments clearly respond to widely shared consumer concerns about loss of control over personal information. In the areas in which they apply, they eliminate secret collection and use of data. Moreover, by investing individuals with unprecedented rights to control processing of data about them, the laws create a significant incentive for businesses to educate consumers about how and why they collect and use information, and to avoid uses that would be embarrassing to disclose.

But for all of their advantages, the very breadth of these laws — restricting many private sector uses of personal information as well as access to that information in the first place — increases the extent to which they conflict with other important values and impose unanticipated costs on consumers and on society at large.

THE FIRST AMENDMENT

The most obvious example of that conflict is the impact of new privacy laws on freedom of expression. "The difficulty," Professor Eugene Volokh has written, "is

that the right to information privacy — my right to control your communication of personally identifiable information about me — is a right to have the government stop you from speaking about me."[29] Granting consumers the right to control information inevitably requires restricting the right of others to access and communicate that information.

The Supreme Court has decided many cases in which individuals sought to stop or obtain damages for the publication of private information or in which the government restricted expression in an effort to protect privacy. Virtually without exception, the Court has upheld the right to speak, publish or protest under the First Amendment, to the detriment of the privacy interest.

For example, the Court has rejected privacy claims by unwilling viewers or listeners in the context of broadcasts of radio programs in city streetcars, R-rated movies at a drive-in theater and a jacket bearing the phrase "Fuck the Draft" worn in the corridors of a courthouse.[30] It has consistently dismissed claims that unsolicited commercial mail or telephone calls constitute an invasion of privacy: Individuals need only "avert their eyes" or "terminate the call. Invasion of privacy is not a significant concern."[31]

The Court has struck down ordinances that would require affirmative opt-in consent before receiving door-to-door solicitations, Communist literature or even "patently offensive" cable programming.[32]

Plaintiffs rarely win suits brought against speakers or publishers for disclosing private information. When information is true and obtained lawfully, the Supreme Court has virtually eliminated restrictions on its disclosure. Punishing the publication of true expression, the Court has written, is "antithetical to the First Amendment's protection."[33] The Court has struck down laws restricting the publication of confidential government reports[34] and of the names of judges under investigation, juvenile suspects and rape victims.[35]

The historical dominance of the free-expression interests over privacy interests is so great that Professor Peter Edelman has written that "the 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."[36]

This is true even when the expression is commercial. Beginning in 1976, the Court recognized that "the particular consumer's interest in the free flow of commercial information … may be as keen, if not keener by far, than his interest in the day's most urgent political debate."[37]

The Court has found that commercial expression, if about lawful activity and not misleading, is protected from government intrusion unless the government can demonstrate a "substantial" public interest and that the intrusion "directly advances" that interest and is "narrowly tailored to achieve the desired objective."[38] The government must demonstrate that "the harms it recites are real" and that "its restriction will in fact alleviate them to a material degree."[39]

This was the view of the 10th U.S. Circuit Court of Appeals. The court was presented with a First Amendment challenge to Federal Communications Commission rules that required U.S. West to get opt-in consent from customers before using data about their calling patterns to determine which customers to contact or what offer to make them.[40] The court, 2-1, found that the FCC's rules, by limiting the use of personal information when communicating with customers, restricted U.S. West's speech and therefore were subject to First Amendment review. The court determined that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a "specific and significant harm" to individuals, and that the rules were "no more extensive than necessary to serve [the stated] interests":[41]

> 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 [the constitutional test applicable to commercial speech] for it is not based on an identified harm.[42]

The appellate court found that for the commission to demonstrate that the opt-in rules were sufficiently narrowly tailored, it must prove that less restrictive opt-out rules would not offer sufficient privacy protection. The commission proved unable to do so.

The Supreme Court reaffirmed the dominance of free-expression interests in the recent case of *Bartnicki v. Vopper*.[43] There the Court explicitly balanced the constitutional interests in privacy and expression and held that the broadcast of an illegally intercepted cellular telephone conversation was protected by the First Amendment: "Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press."[44]

While this decision reflects the power of the First Amendment over privacy protections, it also suggests the limits of that power and of the role of courts as guardians against laws that restrict expression. The information was conceded to be accurate and on a matter of immediate public significance (public school labor negotiations). Moreover, the Court accepted that the defendants not only had not participated in illegally intercepting the cell phone call, but also had no knowledge of who had intercepted it. But, even on these facts, three justices dissented.

INFORMING THE ELECTORATE AND PROTECTING THE PUBLIC

Laws that allow consumers to control the collection and use of information about them interfere not only with the constitutional protection for expression, but also with valuable uses of personal information central to democratic self-governance and protecting public health and safety.

Law enforcement officials rely on collected personal information to prevent, detect and solve crimes. In the days after the terrorist attacks of Sept. 11, 2001, law enforcement officials sought information on possible hijackers and their

accomplices from hundreds of sources, including credit card companies, banks, airlines, rental car agencies, flight training schools and thousands of private individuals. It rapidly became clear that information was a significant resource in the campaign to track down the perpetrators and prevent future attacks.

Personal information is used to elect and monitor public officials and to facilitate public oversight of government employees and contractors. A 2001 study by Professor Brooke Barnett found that journalists routinely use public records not merely to check facts or find specific information, but to actually generate stories in the first place. According to that study, 64% of all crime-related stories, 57% of all city or state stories, 56% of all investigative stories and 47% of all political campaign stories rely on public records. Access to public-record databases, according to Barnett, is "a necessity for journalists to uncover wrongdoing and effectively cover crime, political stories and investigative pieces."[45]

Political parties rely heavily on personal information to identify and contact voters and potential supporters. With 16% of the U.S. population — about 42 million Americans — changing addresses every year, just being able to locate people requires extensive sharing of personal information. Political parties historically relied on motor vehicle records to identify people of voting age and obtain current addresses for past supporters and party members. Yet the 1994 Drivers Privacy Protection Act, as well as other laws limiting use of public records, provides no exemptions for access by political parties or journalists.

In fact, few privacy laws exempt the press. As a result, key sources of information are beginning to be threatened. Both the Society for Professional Journalists and the Reporters Committee for Freedom of the Press have noted the serious threat that the health-privacy regulations pose to reporting about health-related matters.[46]

Medical researchers rely on personal information to conduct "chart reviews" and perform other research critical to evaluating medical treatments, detecting harmful drug interactions, uncovering dangerous side effects of medical treatments and products, and developing new therapies. Such research cannot be undertaken with wholly anonymous information, because the detailed data that researchers require will always include information that could be used to identify a specific person.

Moreover, when that information indicates that a given therapy or drug poses a significant health risk, researchers are required by law to notify the affected individuals.

Health-privacy rules threaten medical research and the development of new drugs and treatments. Helena Gail Rubinstein has written that proponents of such rules refuse to recognize that "as individuals rely on their right to be let alone, they shift the burden for providing the data needed to advance medical and health policy information. Their individualist vision threatens the entire community."[47]

OTHER BENEFITS OF OPEN INFORMATION FLOWS

Privacy laws also run the risk of restricting the greater convenience, lower prices and other benefits that depend on accessible personal information. While these interests may be of less constitutional significance than the impact of privacy laws on freedom of expression and democratic self-governance, they nevertheless represent real costs to the public.

The Federal Reserve Board has written that "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."[48] The result is, in the words of FTC Chairman Timothy Muris, "enormous benefits for consumers." Because of accessible personal information, "the average American today enjoys access to credit and financial services, shopping choices, and educational resources that earlier Americans could never have imagined."[49] Consider four categories of the benefits that privacy laws put at risk:

Consumer Credit. The routine sharing of reliable, standardized personal information has greatly expanded the availability, increased the speed and reduced the cost of consumer credit. When a consumer applies for a mortgage or car loan, the lender makes its decisions about whether, how much and on what terms to lend based on information collected from a wide variety of sources over time. The lender can have confidence in that information because it has been assembled routinely — not just for the purpose of one loan application and presents a complete picture of

the borrower's financial situation — not just one moment in time or information from a selective sample of the businesses with which the borrower deals.

Because of that confidence, lenders provide more loans to a wider range of people than ever before. Between 1956 and 1998, the number of U.S. households with mortgage loans more than tripled. Loan applications are reviewed and approved faster. Virtually all car loan applicants receive a decision within an hour, and most retailers open new charge accounts for customers at the point of sale in less than two minutes. This is unheard of in countries where restrictive laws prevent credit bureaus and other businesses from routinely collecting the information on consumer activities required to maintain the accurate, up-to-date files necessary to support rapid and accurate decision making.

The greater accuracy, speed and efficiency of the credit system, and the greater confidence of lenders also drives down the cost of credit. Lenders don't have to charge higher interest rates and fees to guard against bad or missing information, and it is easier for lenders to pool loans according to risk and sell them in the secondary market. This makes more capital available for new loans and further reduces the cost of credit in the United States by as much as $100 billion per year for mortgages alone. Recent and proposed privacy laws threaten these benefits by limiting the availability of the information on which they depend.

Customer Convenience and Service. Businesses and other organizations use personal information to identify and meet customer needs. According to Federal Reserve Board Governor Edward Gramlich: "Information 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, "the more accurately and efficiently will the economy meet those needs and preferences."[50]

For example, consumers enjoy the convenience of going to a single institution to obtain the services of many separate affiliates or companies. A customer may have a checking account, a savings account, a credit card and an investment account all with the same bank, but the four services will likely be provided by four completely separate affiliates. The customer's checks will be printed by a separate company altogether. Billing for the credit card may be handled by still another company.

Because of information-sharing, the customer can deal with all six entities as if they were one. A high savings balance may be used to qualify the customer for free checking. Overdrafts on a checking account can be covered automatically with a credit card. The customer can call one number with questions, and if his or her credit card or checks are stolen, a single call is all that is needed to protect all of his or her accounts.

Targeting Interested Customers. Information-sharing also allows consumers to be informed rapidly, and at low cost, of those opportunities in which they are most likely to be interested. Target marketing increases the likelihood that only people interested in an offer get one. This means that fewer people who are not likely to be interested receive one, thereby saving the business and its customers money, reducing unwanted mail (and the waste it involves), and minimizing the burden on consumers having to sort through solicitations in which they clearly have no interest. This also means a higher response rate so the business, political party, or charity generates more revenue for every dollar it invests in the solicitation.

More than two-thirds of U.S. consumers — 132 million adults — take advantage of direct marketing opportunities each year. In 2000, direct marketing accounted for $938 billion in sales to consumers — 13% of all consumer sales or an average of $3,478 for every U.S. citizen. Millions of other Americans respond to political and charitable appeals.

In the absence of accessible information, these organizations either could not afford to communicate with potential customers or members, or they would need to contact even more households to find people interested in their offer. This means that the public would be peppered with more mail, e-mail and telephone calls, a higher percentage of which is likely to be of no interest to the recipient.

Promoting Competition and Innovation. Information-sharing is especially critical for new and smaller businesses, which lack extensive customer lists of their own or the resources to engage in mass marketing. By restricting the availability of information about their customers, privacy laws help to protect established businesses from competition.

For a practical example, consider AOL Time Warner. As a start-up company, AOL mailed free copies of its software to people likely to be interested in Internet access. Prohibiting the fledgling AOL access to information about consumer addresses and computer ownership would have denied consumers information about an opportunity that many of them obviously valued, increased the volume of marketing material that AOL would have been required to distribute and threatened the financial viability of a valuable, innovative service. Open access to third-party information helps level the playing field for new market entrants.

Laws designed to protect privacy act as barriers to that information-sharing, and therefore, writes Robert E. Litan, director of the economic studies program and vice president of the Brookings Institution, "raise barriers to entry by smaller, and often more innovative, firms and organizations."[51]

These examples are not exhaustive; they are mere illustrations of the extent to which personal information constitutes part of this nation's essential infrastructure, the benefits of which impact virtually every facet of American life. These benefits are threatened by new privacy laws that broadly restrict the availability of information without regard for its potential to cause harm.

THE ILLUSION OF CONSENT

Privacy advocates often answer that if consumers really value the benefits that information-sharing makes possible, they will consent to those uses of their information. This is the premise of recent privacy laws: Disclose to consumers what information you want to collect and why, and then seek their consent.

This intuitively sensible prescription rarely works in practice. On the one hand, consumers often have no choice but to consent, because of the impossibility of providing the service or product they want without the requested information. Or they consent automatically, ignoring privacy policies and consent requests clicking through or signing them without reading them if necessary to proceed. In fact, the chief privacy officer of Excite@Home told an FTC workshop on profiling that the day after "60 Minutes" featured his company in a segment on Internet privacy, only 100 out of 20 million unique visitors accessed that company's privacy pages.

According to an independent research firm's analysis, in 2002 an average of .3% of Yahoo users read its privacy policy. Even at the height of the publicity firestorm created in March 2002 when Yahoo changed its privacy policy to permit advertising messages by e-mail, telephone and mail, that figure rose only to 1%.*

On the other hand, consumers often have no opportunity to consent, even to information uses that they support, because of the practical difficulty of contacting consumers and motivating them to act. For example, when a business or other organization seeks consent to use personal information that it already possesses in a manner that is not already covered by an existing notice and consent, how does it reach customers who are not currently in direct contact? Most requests for consumer consent never reach their intended recipient. The U.S. Postal Service reports that 52% of unsolicited mail in this country is discarded without ever being read. It will not matter how great the potential benefit resulting from the information use, if the request is not read or heard, it cannot be acted on.

In either case, the opportunity to consent is illusory.

Consider the experience of U.S. West, one of the few U.S. companies to test an opt-in system. To obtain permission to use information about its customer's calling patterns, the company found that it required an average of 4.8 calls to each customer household before it reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, U.S. West customers received more calls and one-third were denied opportunities to receive information about new products and services.[52]

The difficulties of reaching consumers are greatly exacerbated when the party wishing to use the information has no (and may not have ever had) direct contact with the consumer. For example, most mailing lists are obtained from third parties. For a secondary user to have to contact every person individually to obtain consent to use the names and addresses on the list would cause delay, require additional contacts with consumers and almost certainly prove prohibitively expensive. And it could not be done without using the very information that the secondary user is seeking consent to use. Yet the information appears to have little potential to cause harm.

*Saul Hansell, "Compressed Data: The Big Yahoo Privacy Storm That Wasn't," *The New York Times*, May 13, 2002, at C4.

This is an especially acute concern in the area of medical research, where researchers performing chart review will likely have had no prior contact with the patient, and the patient will likely no longer be present in the health care system. To require that the researcher obtain the patient's consent means that the researcher will not only face all of the burdens normally associated with reaching individuals and getting them to respond to a consent request, but the additional burden of having to do so without the benefit of an existing relationship or a ready mechanism for communicating with them.

These difficulties, and the lack of publicized harms resulting from the use of personal information, may explain why opt-out rates are so low. Extensive experience with company-specific and industry-wide opt-out lists demonstrate that less than 10% of the U.S. population ever opts out of a mailing list; often the figure is less than 3%.

To comply with the Gramm-Leach-Bliley financial privacy provisions, by July 1, 2001, 40,000 financial institutions had mailed approximately 2 billion notices. If ever consumers would respond, this would appear to be the occasion: The notices came in an avalanche that seems likely to have attracted consumer attention; the press carried a wave of stories about the notices and about state efforts to supplement Gramm-Leach-Bliley's privacy provisions; privacy advocates lauded the opt-out opportunity and offered online services that would write opt-out requests for consumers; and the information at issue — financial information — is among the most sensitive and personal to most individuals.

Yet the response rate was negligible. By mid-August, only about 5% of consumers had opted out of having their financial information shared with third parties. A late September survey revealed that 35% of the 1,001 respondents could not recall even receiving a privacy notice, even though the average American had received 12 or more.[53]

Rates for opt-in, other than at time of service, are equally low. But the consequence of not responding are is greater. Under an opt-out system, consumers who fail to respond still receive service, their information is still available when they apply for loans, and the press can continue to draw on that information when identifying and

reporting news. Under opt-in, consumers who fail to respond — whatever the reason — cannot receive services or products that depend on personal information; their information is available neither for their own convenience nor for the use of the press.

This suggests that recent privacy mandates that forbid the collection and use of the information without express consumer consent impose an additional burden on consumers by denying them the benefits of information-sharing because they did not respond to consent requests that they may never have received. And it denies the use of that information to the press and the public. How would the press cover stories about the attempted assassination of President Reagan, the health of Vice President Cheney or victims of the terrorist attacks of Sept. 11, 2001, if they first had to get permission from the people involved?

As FTC Chairman Muris has noted,

> The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is a statute that only lawyers could love — until they found out it applied to them.

THE LIMITS OF CONSENT

Consent may be not only illusory, but, as these examples suggest, detrimental as well. It could hinder not only press coverage of public figures and events, but also many uses of personal information that derive their benefit from the fact that the consumer has not had control over the information. This is certainly true of credit information: Its value stems from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make the credit report useless. In the words of Chairman Muris: The credit reporting system "works because, without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies. If consent were required, and

consumers could decide — on a creditor-by-creditor basis — whether they wanted their information reported, the system would collapse."[55]

Moreover, many of the beneficial uses of information that consumers now enjoy and to which they have the opportunity to consent, depend on spreading the cost of collecting and maintaining the information over a variety of uses. For example, commercial intermediaries collect and organize government records and make them accessible to the public. These records are used for many socially valuable purposes: monitoring government operations, locating missing children, preventing and detecting crime, apprehending wanted criminals, securing payments from "deadbeat" parents and spouses, and many others.

If the law restricted the other valuable uses of public records or made those uses prohibitively expensive, then the data and systems to access them would not be in place for any use. Inasmuch as the beneficial uses of information outlined above are interconnected and often depend on common systems and spreading the cost of acquiring and managing data over many uses, consent-based laws may lead to consumers having fewer opportunities made available to them to which they can consent. As a result, recent privacy laws may unintentionally restrict, rather than enhance, consumer choice.

THE COST OF REGULATION

Finally, there is a financial cost to privacy regulation. We have already seen that a major component of that cost is caused by the interference of privacy laws with open information flows. Those costs will ultimately be reflected in higher prices for products and services.

Another source of that cost is the burden of complying with privacy laws. Crafting, printing and mailing the 2 billion disclosure notices required by Gramm-Leach-Bliley, for example, is estimated to have cost $2 billion to $5 billion.
Privacy protections requiring opt-in are even more costly. The Department of Health and Human Services calculates the cost of complying with the recently adopted health-privacy rules to be $3.2 billion for the first year and $17.6 billion for

the first 10 years. Health care consulting companies predict that the cost will be much higher — between $25 billion and $43 billion for the first five years for compliance alone, not including impact on medical research and care or liability payments.

During its opt-in test, U.S. West found that to obtain permission to use information about its customers' calling patterns for marketing services cost between $21 and $34 per customer.[56]

A 2000 Ernst & Young study of financial institutions — representing 30% of financial services industry revenues — found that financial services companies would send out three to six times more direct marketing material if they could not use shared personal information to target their mailings, at an additional cost of about $1 billion per year.[57]

The study concluded that the total annual cost to consumers of opt-in restriction on existing information flows — precisely because of the difficulty of reaching customers — was $17 billion for the companies studied, or $56 billion if extrapolated to include the customers of all financial institutions. And those figures do not include the costs resulting from the reduced availability of personal information to reduce fraud, to increase the availability and lower the cost of credit, to provide co-branded credit cards and nationwide automated teller machine networks, and to develop future innovative services and products.

Other types of privacy protections may cost even more. According to a 2001 study by Robert Hahn, director of the Brookings Joint Center on Regulation, the initial cost of complying with even a modest access requirement in online privacy legislation would be $9 billion to $36 billion.[58]

And these costs are not limited to business users of information. A new study by Michael Turner calculates that the annual cost to charities of complying with opt-in privacy laws when fund raising would be $16.5 billion — 21% of the total amount raised by U.S. charities in 2000.[59]

Ultimately, it is consumers and individuals, in the words of Alabama Attorney General Bill Pryor, who "pay the price in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace."[60]

THE NEW DEBATE

The fact that there are costs to privacy laws, and that those laws interfere with other important values and interests, is not surprising. Nor does it lead to the conclusion that the law should not protect privacy. It does suggest, however, that the privacy debate should more clearly take into account the impact of new privacy enactments.

This may be one effect of the terrorist attacks of Sept. 11. The vital role played by accessible personal information in the subsequent hunt for the perpetrators and in protecting against future attacks demonstrated both the value of open information flows and the risk of allowing privacy mandates to restrict those flows.

This was unmistakable evidence of the inherent tension between privacy and other values. In the aftermath of Sept. 11, public opinion polls, which only days earlier had demonstrated overwhelming support for new privacy protections, reflected an equally great willingness to trade privacy for security. Moreover, in the face of long lines and intrusive searches at airports, the public seemed increasingly willing to reveal more personal information (for example, for background checks or passenger identification) simply for greater convenience (such as not standing in security checkpoint lines at airports).

By Nov. 5, 2001, Mike France and Heather Green could write in *Business Week:* "The war on terrorism is still in its early days, but one thing is already clear: In the future, information about what you do, where you go, who you talk to, and how you spend your money is going to be far more available to government, and perhaps business as well. … Across a wide range of battlefields, privacy is on the retreat."[61]

That retreat is neither uniform nor long-lived, to judge by the renewed consideration of a wide range of privacy bills in Congress and state legislatures. But

the lessons about the inevitable trade-offs between privacy and other values may endure longer. We can hope so, because it is only when the privacy debate more accurately reflects the cost, as well as the benefits, of privacy protections that it can lead to rational judgments about whether those protections are warranted or whether there are alternative approaches that could protect privacy as, or even more, effectively, but at less cost and with less intrusion into other important values.

This inquiry is especially important for the press, which acts both as a monitor of government and as a key source of information for the public. The news media depend on an open flow of personal information to fulfill those roles. It is precisely for this reason that the U.S. Supreme Court has long interpreted the First Amendment to protect both expression and access to the information necessary to make that expression meaningful. We should proceed cautiously and thoughtfully before discarding that commitment in the name of protecting privacy.

ENDNOTES

[1]Kent Walker, "Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange," Stanford Technology Law Review 15 (2001).

[2]Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4 Harvard Law Review 193 (1890).

[3]277 U.S. 438 (1928).

[4]Id. at 478-79 (Brandeis, J., concurring). The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Constitution amend. IV.

[5]389 U.S. 347 (1967).

[6]Id. at 361 (Harlan, J., concurring); see *Terry v. Ohio,* 392 U.S. 1, 9 (1968); *Smith v. Maryland,* 442 U.S. 735, 740 (1979).

[7]*Whalen v. Roe,* 429 U.S. 589, 599-600 (1977).

[8]Restatement (Second) of Torts § 652B.

[9]Id. § 652D; see also id. at § 652D (cmt. a).

[10]Id. § 652E.

[11]*Time, Inc. v. Hill,* 385 U.S. 374, 387-88 (1967).

[12]*Cantrell v. Forest City Publishing Co.,* 419 U.S. 245 (1974).

[13]15 U.S.C. § 1681b(a).

[14]Enactment of the Children's Online Privacy Protection Act, 146 Cong. Rec. E616, May 2, 2000, statement of Jay Inslee (D-Wash.) (emphasis added); Democrats Hold News Conference on Financial Privacy, May 4, 2000 (statement of John LaFalce (D-N.Y.)).

[15]S. 30, 107th Cong. § 2 (2001); H.R. 89, 107th Cong.§ 2(b)(1) (2001); H.R. 347, 107th Cong. § 2(b)(1)(A) (2001).

[16]William Safire, "Nosy Parker Lives," *The New York Times,* Sept. 23, 1999, at A29.

[17]Gramm-Leach-Bliley Financial Services Modernization Act, 106 Pub. L. No. 102, 113 Stat. 1338 (1999).

[18]Id. § 503(b).

[19]Id. §§ 502(b)(2), (e)

[20]Id. § 509(3).

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

[22]Standards for Privacy of Individually Identifiable Health Information, amended by 67 Fed. Reg. 14,776 (2002) (HHS, proposed rule, modification) (to be codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

[23]45 C.F.R. § 164.506(a).

[24]Id. § 164.508(a)(1).

[25]Pub. L. No. 105-277, 112 Stat. 2681 (1998).

[26]Pub. L. No. 103-322, 108 Stat. 2099-2102 (1994) (codified at 18 U.S.C. § 2721 (1997)).

[27]*Reno v. Condon,* 528 U.S. 141 (2000).

[28]Department of Transportation and Related Agencies Appropriations Act, 2000, § 350, 106 Pub. L. No. 69; 113 Stat.

986 (1999).

[29]Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You," 52 Stanford Law Review 1049, 1050-51 (2000).

[30]*Public Utilities Comm'n v. Pollack,* 343 U.S. 451 (1952); *Erznoznik v. City of Jacksonville,* 422 U.S. 205 (1975); *Cohen v. California,* 403 U.S. 15 (1971).

[31]*Edenfield v. Fane,* 507 U.S. 761, 776 (1993); *Bolger v. Youngs Drug Products Corp,* 463 U.S. 60, 72 (1983) (quoting Consolidated Edison, 447 U.S. at 542 (quoting Cohen, 403 U.S. 15)) (internal quotation marks omitted).

[32]*Martin v. Struthers,* 319 U.S. 141 (1943); *Lamont v. Postmaster General,* 381 U.S. 301 (1965); *Denver Area Educational Telecom. Consortium, Inc. v. FCC,* 518 U.S. 727 (1996).

[33]*Philadelphia Newspaper, Inc. v. Hepps,* 475 U.S. 767, 777 (1986).

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

[35]*Landmark Communications, Inc. v. Virginia,* 435 U.S. 829 (1978); *Smith v. Daily Mail Pub. Co.,* 443 U.S. 97 (1979); *Florida Star v. B.J.F.,* 491 U.S. 524 (1989); *Cox Broadcasting Corp. v. Cohn,* 420 U.S. 469 (1975).

[36]Peter B. Edelman, "Free Press v. Privacy: Haunted by the Ghost of Justice Black," 68 Texas Law Review 1195, 1198 (1990).

[37]*Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.,* 425 U.S. 748, 762-64 (1976) (footnote and citations omitted).

[38]*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).

[39]Edenfield, 507 U.S. at 770-71.

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

[41]Id. at 1235 (quoting *Rubin v. Coors Brewing Co.,* 514 U.S. 476, 486 (1995)).

[42]Id.

[43]532 U.S. 514 (2001).

[44]Id at 534, 121 S. Ct. at 1765 (quoting *Time, Inc. v. Hill,* 385 U.S. 374, 388 (1967) (quoting *Thornhill v. Alabama,* 310 U.S. 88, 102 (1940))).

[45]Brooke Barnett, "Use of Public Record Databases in Newspaper and Television Newsrooms," 53 Federal Communications Law Journal 557 (2001).

[46]Society for Professional Journalists, Medical Privacy Rules Ignore Public's Interest, Media's Role (press release) (Dec. 22, 2000); Comments of the Reporters Committee for Freedom of the Press Concerning RIN 099-AB08, Standards for Privacy of Individually Identifiable Health Information (Feb. 17, 2000).

[47]Helena Gail Rubinstein, "If I am Only for Myself, What Am I? A Communitarian Look at the Privacy Stalemate," 25 American Journal of Law and Medicine 203 (1999).

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

[49]Timothy J. Muris, Protecting Consumers' Privacy: 2002 and Beyond, Privacy 2001 Conference, Cleveland, OH, Oct. 4, 2001.

[50]Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the House Comm. on Banking and Financial Services, July 21, 1999 (statement of Edward M. Gramlich).

[51]Robert E. Litan, Balancing Costs and Benefits of New Privacy Mandates, Working Paper 99-3, AEI-Brookings Joint

Center for Regulatory Studies (1999).

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

[53]Star Systems, Financial Privacy: Beyond Title V of Gramm-Leach-Bliley 9 (2002).

[54]Muris, supra.

[55]Id.

[56]Brief for Petitioner and Interveners at 15-16, *U.S. West, Inc. v. FCC,* 182 F.3d 1224, 1239 (10th Cir. 1999) (No. 98-9518), cert. denied 528 U.S. 1188 (2000).

[57]Ernst & Young LLP, Customer Benefits from Current Information Sharing by Financial Services Companies 16 (Dec. 2000).

[58]Robert W. Hahn, An Assessment of the Costs of Proposed Online Privacy Legislation (2001).

[59]Michael A. Turner & Lawrence G. Buc, The Impact of Data Restrictions on Fund-raising for Charitable & Nonprofit Institutions 2-3 (2002).

[60]Bill Pryor, Protecting Privacy: Some First Principles, Remarks at the American Council of Life Insurers Privacy Symposium, July 11, 2000, Washington, D.C., at 4.

[61]Mike France & Heather Green, "Privacy in an Age of Terror," *Business Week,* Nov. 5, 2001, at 82.

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

—First Amendment to the U.S. Constitution

First Reports is an ongoing series of publications produced by the First Amendment Center to provide analysis and background on contemporary First Amendment issues.

The First Amendment Center works to preserve and protect First Amendment freedoms through information and education. The center serves as a forum for the study and exploration of free-expression issues, including the freedoms of speech, press and religion and the rights to assemble and to petition the government.

The center is housed in the John Seigenthaler Center at Vanderbilt University in Nashville, Tenn. It also has offices in Arlington, Va. It is an operating program of the Freedom Forum, a nonpartisan foundation dedicated to free press, free speech and free spirit for all people.

FIRST AMENDMENT CENTER
FUNDED BY THE FREEDOM FORUM

First Amendment Center

Kenneth A. Paulson
EXECUTIVE DIRECTOR

John Seigenthaler
FOUNDER

1207 18th Avenue South
Nashville, TN 37212
615/727-1600

1101 Wilson Boulevard
Arlington, VA 22209
703/528-0800

www.firstamendmentcenter.org

To order additional copies of this report,
Call 1-800-830-3733 or e-mail
puborder@freedomforum.org and
request publication #03-F01.

Publication #03-F01 | 2.5K | BL