

Chapter 4

PRIVACY PROTECTION IN THE UNITED STATES

Fred H. Cate
Distinguished Professor of Law and Director
Center for Applied Cybersecurity Research
Indiana University
Senior Policy Advisor
The Center for Information Policy Leadership
at Hunton & Williams

Table of Contents

Introduction.....	1
Privacy Law, 1890-1990.....	2
Protection Against Government Invasions of Privacy.....	2
Protection Against Harmful Uses.....	5
Privacy Protection, 1990-2006.....	6
The Focus on Control.....	6
The Federal Trade Commission and the Regulation of “Unfair” and “Deceptive” Trade Practices.....	7
New Statutory Focus on Control.....	8
Privacy in Context: Costs and Competing Values.....	11
Benefits of Open Information Flows.....	11
Competition and Innovation.....	11
Advancing Public Welfare.....	11
Facilitating Consumer Credit.....	12
Enhancing Customer Convenience and Service.....	13
Targeting Interested Consumers.....	13
The Illusion of Consent.....	14
The Limits of Consent.....	16
The Cost of Regulation.....	16
Zealous Enforcement.....	17
Conclusion.....	18

Introduction

In the United States, the legal regulation of information privacy is characterized by its *variety*. There are many *sources* of privacy law. This reflects the fact that the federal Constitution establishes an hierarchical division of power among federal, state, and local regulators. In addition, the Constitution also creates a tripartite system of government—responsible for legislative, executive, and judicial functions—on the federal level, which is mirrored in most state governments. All three branches are involved to some degree in the creation of law: legislatures create statutory law, agencies create administrative law through rules or regulations and their interpretation, and courts create case law or common law through their decisions.

As the preceding paragraph suggests, there are also many *types* of law, such as constitutions, statutes, regulations, judicial decisions, and treaties. These are often supplemented by contracts, policies, self-regulatory codes, the threat of civil litigation and especially class action lawsuits, pressure from legislators and regulators often accompanied with the specter of new laws or more aggressive enforcement of existing laws, and the risk of exposure by the press and in the market. While not law *per se*, these all play a significant role in influencing the behavior of businesses and other institutions. Moreover, they are often backed up by more formal types of law (for example, the judicial enforcement of contracts or policies).

Privacy law in the United States tends to be *sectoral*. Usually, different laws apply to government than to private-sector activities. Moreover, different laws often apply depending upon the specific industry or government agency. For example, three entirely different laws regulate name and address information resulting from subscribing to cable television,¹ obtaining telephone service,² or renting video cassettes.³ This sectoral focus contributes significantly to the number and variety of privacy laws.

U.S. privacy law reflects an explicit *balance* between the benefits of protecting privacy and the burdens created by such protection. That burden includes the financial cost of complying with privacy law, the impact of privacy law on other important activities such as the prevention and detection of crime or the promotion of innovation and market competition, and the interference of privacy law with other societal values such as freedom of expression, protection against unnecessary government intrusion, and respect for private property. This too adds to the variety and the complexity of privacy law because it means that statutes and regulations are often quite detailed to achieve the optimum balance.

Finally, U.S. privacy law has been *changing* and *expanding*. For most of the last century, as discussed in greater detail below, it was concerned primarily with restraining the government's access to personal information and protecting against harmful uses of such information. During the past decade, however, U.S. privacy law has increasingly regulated private-sector uses of information, including those which do not threaten to harm individuals. In addition, the law has become increasingly bureaucratic and procedural. These changes have added to the variety of the law.

This paper surveys briefly the structure of privacy law in the United States, examines some of its most prominent features, and offers concluding observations about how that law is changing and the protection it affords personal privacy.

¹See The Cable Communications Policy Act of 1984, 47 U.S.C. § 551(a)(1).

²Telecommunications Act of 1996, 47 U.S.C. § 222.

³Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

Privacy Law, 1890-1990

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*.⁴ Brandeis and Warren were concerned that the press, armed with "instantaneous photographs" and "numerous mechanical devices," "is overstepping in every direction the obvious bounds of propriety and of decency." They proposed the creation of a tort for invasion of privacy by the press. That article and its authors contributed to the two dominant strands of early U.S. privacy law: protection against government invasions of citizen privacy and protection against harmful uses of personal information.

Protection Against Government Invasions of Privacy

In the United States, there is no explicit constitutional guarantee of a right to privacy. The Supreme Court, however, has interpreted many of the amendments constituting the Bill of Rights to provide some protection to a variety of elements of individual privacy against intrusive government activities. These include the First Amendment provisions for freedom of expression and association, the Third Amendment restriction on quartering soldiers in private homes, the Fourth Amendment prohibition on unreasonable searches and seizures, the due process clause and guarantee against self-incrimination in the Fifth Amendment, the Ninth and Tenth Amendment reservations of power in the people and the States, and the equal protection and due process clauses of the Fourteenth Amendment.⁵

None of these provisions refer to privacy explicitly, and the circumstances in which privacy rights are implicated vary as widely as the sources of those rights. Moreover, constitutional rights protect only against state action.⁶ As a result, any constitutional concept of "privacy" would apply only against the government. In addition, constitutional rights are generally "negative"; they do not obligate the government to do anything, but rather to refrain from taking certain actions. As a result, any constitutional right to privacy would at most require that the government refrain from taking actions which impermissibly invade privacy. A constitutional privacy right would not require the government to take steps to affirmatively protect individual privacy.

The first, and best developed, concept of privacy emerged from Justice Brandeis' 1928 dissent in *Olmstead v. United States*.⁷ 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."⁸

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

⁵See Fred H. Cate, *Privacy in the Information Age* 49-66 (1997).

⁶Only the Thirteenth Amendment, which prohibits slavery, applies directly to private parties. *Clyatt v. United States*, 197 U.S. 207, 216-220 (1905). Although state action is usually found when the government acts toward a private person, the Supreme Court has also found state action when the government affords a legal right to one private party which impinges on the constitutional rights of another, *New York Times Co. v. Sullivan*, 376 U.S. 264, 265 (1964), and in rare cases when a private party undertakes a traditionally public function, *Marsh v. Alabama*, 326 U.S. 501 (1946), or when the activities of the state and a private entity are sufficiently intertwined to render the private parties' activities public, *Evans v. Newtown*, 382 U.S. 296 (1966).

⁷277 U.S. 438 (1928).

⁸*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

Almost 40 years later, the Court adopted Justice Brandeis' reasoning in *Katz v. United States*.⁹ 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.'"¹⁰

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."¹¹ Nevertheless, despite having identified this new privacy interest, the Supreme Court has never decided a case in which it found that a government regulation or action violated it.¹²

In addition to these constitutional protections, U.S. privacy law also includes 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. For example, the federal Privacy Act of 1974 obligates government agencies to (1) store only relevant and necessary personal information; (2) collect information to the extent possible for the data subject; (3) maintain records with accuracy and completeness; and (4) establish administrative and technical safeguards to protect the security of records.¹³ The Privacy Act also limits disclosure of individuals' records. The Privacy Act provides twelve exemptions that permit disclosure of information to other government agencies.¹⁴ For example, the act does not apply to Congress. It does not restrict disclosures to law enforcement agencies. And, under the broadest exemption, the act does not apply to data requested by another government agency for "routine use." These exemptions reflect the inherent tension between protecting privacy and permitting valuable uses of personal information.

The Electronic Communications Privacy Act limits the government's ability to collect information through electronic surveillance.¹⁵ Federal law prohibits the Department of Health and Human Services from disclosing social security records.¹⁶ Similarly, federal law prohibits the Internal Revenue Service from disclosing information on income tax returns¹⁷ and the Census Bureau from disclosing certain categories of census data.¹⁸ Finally, many states have adopted laws and regulations that mirror their federal counterparts.

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, and that Congress has passed statutes, to restrict the government's collection and use of personal information.

affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Constitution amend. IV.

⁹389 U.S. 347 (1967).

¹⁰*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).

¹¹*Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).

¹²See Fred H. Cate, "The European Data Protection Directive and European-U.S. Trade," *Currents*, vol. vii, no. 1, at 61 (1998).

¹³5 U.S.C. § 552a(e)(1)-(5).

¹⁴*Id.* § 552(a)(b)(1)-(12).

¹⁵18 U.S.C. §§ 2510-2520, 2701-2709.

¹⁶42 U.S.C. § 1305.

¹⁷26 U.S.C. §§ 6103, 7431.

¹⁸13 U.S.C. §§ 8-9.

Protection Against Harmful Uses

The earliest protection against harmful uses of personal information in the private sector was through state tort laws, as advocated by Warren and Brandeis, which allowed individuals injured by such harmful uses to sue the persons responsible. By 1960 courts in many states had recognized common law privacy torts.

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.”¹⁹

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.”²⁰ 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.²¹ In 1967, the Supreme Court extended the First Amendment privileges previously recognized in the context of defamation to actions for false light privacy.²² 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 apply only when the information is “highly offensive to a reasonable person” and either false or of no “legitimate public concern to the public.” 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.²³

In the 1970s Congress also began adopting *statutes* to restrict certain uses of information that were considered likely to pose a risk of harm to individuals. Laws applicable to the context of financial transactions were among the earliest and provide a typical example of this model of privacy protection. The Fair Credit Reporting Act of 1970 restricts “consumer reporting agencies” from sharing information “bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living” with a third party unless the intended use fits within one of the broad “permissible purposes” set forth in the act.²⁴ The act requires that credit reporting agencies follow “reasonable procedures to assure maximum possible accuracy” of the information in their credit reports and implement a dispute resolution process to investigate and correct errors. Agencies also must inform consumers about whom adverse decisions on credit, employment, or insurance are made based on a consumer report, of the use and source of the report. The agencies must provide consumers with a copy of their reports upon request and, in many situations, without cost.

Following amendment of the act in 1996 and again in 2003, consumers have the right to be notified of, and to object to (opt out of) certain uses of personal information (for example, target marketing or prescreening for credit or insurance purposes). In two instances, affirmative

¹⁹Restatement (Second) of Torts § 652B.

²⁰Id. § 652D; see also id. at § 652D (cmt. a).

²¹Id. § 652E.

²²Time, Inc. v. Hill, 385 U.S. 374, 387-88 (1967).

²³Cantrell v. Forest City Publishing Co., 419 U.S. 245 (1974).

²⁴15 U.S.C. §§ 1681-1681t, 1681b(a), 1681a(d).

(opt-in) consumer consent is required: providing credit reports for employment purposes and including medical information in a credit report furnished in connection with employment, credit, insurance, or direct marketing.²⁵

Another example of a statute designed to protect privacy in an effort to prevent harm is the Children's Online Privacy Protection Act of 1998.²⁶ The act 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). 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.

The FCRA, the COPPA, and many other laws adopted in between, apply in only one industrial sector, to one technological setting, or to one population that is thought to be at risk. While they generally impose few substantive limits on the collection or use of personal data, they create significant bureaucratic hurdles to the collection and use of personal information.

Privacy Protection, 1990-2006

The Focus on Control

By the mid-1990s, a variety of developments prompted new concerns about privacy: the proliferation of new technologies, the spread of privacy law in Europe, a new awareness of how much personal information is collected and used, and the growth of identity theft. While these concerns have included 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.”²⁷

Columnist 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.”²⁸

²⁵Department of Defense Appropriations Act, 1997, H.R. 3610, 104th Cong., 2d Sess. §§ 2401-2422 (Sep. 30, 1996) (codified at 15 U.S.C. §§ 1681-1681t); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. §§ 1681-1681t).

²⁶Pub. L. No. 105-277, 112 Stat. 2681 (1998).

²⁷*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.)).

²⁸William Safire, “Nosy Parker Lives,” *New York Times*, Sept. 23, 1999, at A29.

This movement toward investing individuals with the right to control certain uses of information about them, without regard to the potential of the information to cause harm or the public's interest in that information being available, is reflected in two forms of privacy protection. The first focuses on "voluntary" disclosures of privacy policies, backed up with strict-liability enforcement for violation of those policies. The second model relies on statutory mandates.

The Federal Trade Commission and the Regulation of "Unfair" and "Deceptive" Trade Practices

Beginning in the mid-1990s, the Federal Trade Commission (FTC) encouraged U.S. operators of commercial websites to adopt and publish online privacy policies. The primary inducement offered by the FTC was avoiding statutory regulation of online privacy.

The Commission pursued this approach both with industry groups that collect or use personal information and with individual website operators. For example, in 1997 the majority of companies providing look-up services on individuals agreed to abide by the Individual Reference Services Group Principles, which not only established 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. The Commission supported the development of these Principles and in 1997 reported them to Congress as a good example of effective self-regulation.²⁹

Similarly, under pressure from the FTC, the major providers of online advertising formed a coalition, the Network Advertising Initiative, that in 2000 promulgated a privacy code and provides a convenient way for consumers to opt out of having personal information used to target banner advertising to them.³⁰ The Commission was similarly supportive of this effort, although so much had the Commission's outlook changed between 1997 and 2000 that, when the FTC reported the NAI code to Congress, it recommended using it as a basis for statutory privacy protection.³¹

The Commission's efforts to encourage voluntary posting of privacy policies by individual website operators began in earnest in 1998, when the Commission conducted its first survey of commercial websites. The FTC reported that 92 percent collected personal information in some form, but only 14 percent of those had some form of privacy disclosure, while 73 percent of the "most popular" sites had a privacy disclosure.³² Nevertheless, the Commission recommended in 1998 and again in 1999 that Congress delay action to give self-regulation—under growing pressure from the FTC—a chance to work. The Commission did recommend, and Congress adopted, legislation protecting the privacy of children online.³³

The threat of congressional action had its desired effect. By 2000, the Commission found that 88 percent of a random sample of commercial websites and 100 percent of the most popular

²⁹Federal Trade Commission, *Individual Reference Services: A Report to Congress*, 1997, <http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm>.

³⁰See <http://www.networkadvertising.org/>.

³¹Federal Trade Commission, *Online Profiling: A Report to Congress*, 2000, <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>; Federal Trade Commission, *Online Profiling: A Report to Congress—Part 2: Recommendations*, 2000, <http://www.ftc.gov/os/2000/07/onlineprofiling.pdf>; Network Advertising Initiative, "Self-Regulatory Principles for Online Preference Marketing by Network Advertisers," http://www.ftc.gov/os/2000/07/NAI_percent207-10percent20Final.pdf.

³²Federal Trade Commission, *Privacy Online: A Report to Congress* 23, 27-28 (1998) <http://www.ftc.gov/reports/privacy3/priv-23a.pdf>.

³³The Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

commercial websites posted a privacy policy.³⁴ However, while in its earlier surveys the Commission had counted websites that had privacy disclosures irrespective of the content of those disclosures, by 2000 the Commission was “analyz[ing] the nature and substance of these privacy disclosures” to determine if the disclosures provided an adequate substantive level of privacy protection. No longer was it sufficient, in the FTC’s view, to provide Internet users with notice of how a website collected and used personal information; it was now necessary for websites to collect or use personal information only in ways specified by the Commission. Those requirements were:

- Notice—data collectors must disclose their information practices before collecting personal information from consumers;
- Choice—consumers must be given a choice as to whether and how personal information collected from them may be used;
- Access—consumers should be able to view and contest the accuracy and completeness of data collected about them;
- Security—data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use; and
- Enforcement—there must be a reliable mechanism in place to impose sanctions for noncompliance with these fair information practices.³⁵

The Commission’s 2000 survey found that only 10 percent of the random sample and 42 percent of the most popular sample met these substantive standards. The Commission therefore recommended that Congress give it explicit authority to require compliance by commercial website operators.

The Commission and state attorneys general also stepped up their enforcement efforts against website operators that violated their privacy policies. The Commission brought its first Internet privacy case in 1998 against GeoCities for allegedly misrepresenting the purposes for which it was collecting personal identifying information from children and adults through its website. The primary legal theory on which the Commission proceeded was that by posting a privacy policy with which it did not comply, GeoCities had engaged in a “deceptive” trade practice. Section 5 of the Federal Trade Commission Act prohibits “unfair and deceptive practices in or affecting commerce” and empowers the FTC to investigate and prosecute them.³⁶ GeoCities ultimately settled with the FTC, the first in a long series of such settlements the Commission has managed to obtain against offending website operators.³⁷ Most of these cases have in common that the only or primary offense alleged was the failure to comply with a voluntarily adopted privacy policy. None involved a finding of harm. In addition, the Commission has enforced compliance with privacy policies on a strict liability basis.

New Statutory Focus on Control

The movement to invest individuals with legal rights to control the use of information about them, and couch those rights in increasingly bureaucratic procedural requirements, is also reflected in statutory mandates. These new laws invest consumers with greater rights to control the use of information about them. They do so with less if any regard for the potential of the information to cause harm. They are highly bureaucratic, conditioning any use of information on compliance with notice, consent, and other requirements that burden and may effectively prohibit uses of information.

³⁴Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress*, 2000, p. 11, <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

³⁵*Id.* at 4.

³⁶15 U.S.C. § 45(a)(1).

³⁷*GeoCities*, Docket No. C-3849, Feb. 12, 1999.

There are many examples. One that involves fewer substantive limits, but many bureaucratic ones, is Title V of the Gramm-Leach-Bliley Financial Services Modernization Act,³⁸ passed in 1999. Enacted as part of a law breaking down decades-old barriers between financial services, Title V contains three substantive restrictions on the use of personal information: prohibitions on account numbers to third parties for marketing purposes, on pretext calling, and on transfers of personal information to third parties for marketing purposes if the data subject has opted out.

The real burden of the new law is in its procedural requirements. The 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 must be sent at least annually even if there is no change in its terms. 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, protect against fraud or other liability, or comply with applicable laws.

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. 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.

A second and more onerous example of the statutory control/disclosure model is found in the rules for protecting the privacy of personal health information adopted in April 2001 by the Department of Health and Human Services, under the Health Insurance Portability and Accountability Act (HIPAA).³⁹ As amended in August 2002,⁴⁰ the HIPAA 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, and, indirectly, to anyone who receives protected health information from a covered entity. 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.” 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.” 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

³⁸Gramm-Leach-Bliley Financial Services Modernization Act, 106 Pub. L. No. 102, 113 Stat. 1338 (1999).

³⁹Standards 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), <http://www.hhs.gov/ocr/hipaa/finalreg.html>.

⁴⁰Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 43,181 (2002) (HHS, final rule) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506), <http://www.hhs.gov/ocr/hipaa/privrulepd.pdf>. The unofficial text of the final rule as amended may be found at <http://www.hhs.gov/ocr/combinedregtext.pdf>.

exceptions, under which personal health information may be disclosed, usually to government agencies, with neither consent nor authorization.

A covered entity may use or disclose personal health information for directories and to notify and involve other individuals in the care of a patient if the covered entity obtains the “agreement” of the individual. An agreement need not be written, provided that the individual is informed in advance of the use and has the opportunity to opt out of any disclosure. This is the only consent requirement under the amended rules for which opt-out (rather than opt-in) consent is sufficient.

Ironically, HIPAA’s federal health privacy rules originally developed as a reaction to HIPAA’s push for more uniform electronic data standards to make health care and health insurance cheaper and more efficient (just as the financial privacy provisions in Gramm-Leach-Bliley were enacted in response to that law’s effort to make obtaining financial services easier). The legislation’s “administrative simplification” provisions were aimed at reducing costs and making health benefits more portable by smoothing and accelerating the flow of health and health insurance information. But political demands for greater individual control of personal health information pushed HIPAA privacy rules in the opposite direction. Indeed, federal rule makers declined to preempt more restrictive state privacy rules, inviting states to go beyond the federal privacy standards. Texas has taken Congress up on its invitation, by enacting the HIPAA regulations into state law, but dramatically expanding the definition of “covered entity” to include anyone who “comes into possession of protected health information,” “obtains or stores protected health information,” or “maintains an Internet site.”⁴¹

A final example of statutory mandates that impose restrictions on information flows in an effort to give individuals control over even innocuous uses of data about them is found in the many laws adopted over the past decade limiting access to public records. For example, in 1994 Congress enacted the Driver’s Privacy Protection Act.⁴² 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. States are permitted 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. Two years later, however, Congress amended it to require that states, as a condition of receiving federal highway funds, obtain explicit opt-in consent from individuals before information about them contained in motor vehicle records is used for “surveys, marketing, or solicitation” purposes.⁴³

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 opt-in consent of the individuals involved. South Carolina has gone even further to ban outright the use of public records for marketing.⁴⁴ This may point to the next generation of U.S. privacy protection: not merely burdening the responsible use of personal information with disclosure and consent requirements, but prohibiting those uses altogether—substituting government control for even the illusion of individual control.

Collectively, these enactments reflect a much broader concept of privacy protection than previously recognized by U.S. law. These statutes are focused on information collection and use by the private sector, not the government; in fact, some would make it easier for the government

⁴¹Texas Health & Safety Code § 181.001.

⁴²Pub. L. No. 103-322, 108 Stat. 2099-2102 (1994) (codified at 18 U.S.C. § 2721).

⁴³Department of Transportation and Related Agencies Appropriations Act, 2000, § 350, 106 Pub. L. No. 69; 113 Stat. 986 (1999).

⁴⁴Bill 204, Family Privacy Protection Act of 2002 (codified at S.C. Code §§ 30-2-10 to 30-2-30).

to access personal information. They apply very broadly. And they do not purport to restrict or punish only harmful uses of information; in fact, liability under these statutes in no way depends on causing harm or injury. Except for a few specific exemptions, these laws all condition the collection and use of broad categories of information on consumer consent, but they then put in place burdensome requirements that make obtaining that consent expensive and difficult. The very breadth and bureaucratic nature of these laws—restricting both many private sector uses of personal information and access to that information in the first place—increase the extent to which they conflict with other important values and impose unanticipated costs on consumers and on society at large.

Privacy in Context: Costs and Competing Values

The increasing focus on consumer control as the goal of privacy protection poses considerable costs—financial and otherwise—on consumers and industry, and increasingly brings privacy law into other values.

Benefits of Open Information Flows

Advancing Public Welfare

Laws that allow consumers to control the collection and use of information about them interfere with responsible efforts to protect public health and safety. For example, law enforcement officials rely on collected personal information to prevent, detect, and solve crimes. In the days after the terrorist attacks of September 11, 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 percent of all crime-related stories, 57 percent of all city or state stories, 56 percent of all investigative stories, and 47 percent of all political campaign stories rely on public records. Access to public record databases, according to Professor 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 percent 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 uses of public records, provides no exemptions for access by political parties or journalists.

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

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

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.”⁴⁶

Facilitating Consumer Credit

Privacy laws also run the risk of restricting the greater convenience, lower prices, and other benefits that depend on accessible personal information. 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.”⁴⁷ 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.”⁴⁸

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 trebled. 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 more than \$80 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.

⁴⁶Helena 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).

⁴⁷Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud 2* (1997).

⁴⁸Timothy J. Muris, *Protecting Consumers’ Privacy: 2002 and Beyond*, Privacy 2001 Conference, Cleveland, OH, Oct. 4, 2001.

Enhancing 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.”⁴⁹

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 likely to be 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.

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—meaning more unsolicited mail, e-mail, and telephone calls—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 value, 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.

⁴⁹Financial 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).

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.”⁵⁰

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

Proponents of consumer choice privacy laws often argue 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 percent 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 percent.⁵¹

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. Post Office reports that 52 percent 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

⁵⁰Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates*, Working Paper 99-3, AEI-Brookings Joint Center for Regulatory Studies (1999).

⁵¹Saul Hansell, “Compressed Data: The Big Yahoo Privacy Storm That Wasn’t,” *New York Times*, May 13, 2002, at C4.

⁵²Brief 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).

The difficulties of reaching consumers are greatly exacerbated where 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.

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 percent of the U.S. population ever opts out of a mailing list—often the figure is less than 3 percent.

To comply with the Gramm-Leach-Bliley financial privacy provisions, by July 1, 2001, 40,000 financial institutions had mailed approximately 4 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 2001, only about 5 percent of consumers had opted out of having their financial information shared with third parties. A late September survey revealed that 35 percent of the 1001 respondents could not recall even receiving a privacy notice, even though the average American had received 20.⁵³

Rates for opt-in, other than at time of service, are equally low. But the consequence of not responding are far 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 September 11 if they first had to get permission from the people involved?

As former FTC Chairman Muris has noted,

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

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.⁵⁴

The Limits of Consent

Consent may not only be illusory, but, as these examples suggest, undesirable as well. This is true not only of press coverage of public figures and events, but of the many beneficial uses of personal information where the benefit is derived from the fact that the consumer has not had control over the information. This is certainly true of credit information: Its value derives 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 former 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 these 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. Those 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

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 4 billion disclosure notices required by Gramm-Leach-Bliley, for example, is estimated to have cost \$2-5 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 ten years. Health care consulting companies predict that the cost will be much higher—between \$25 and \$43 billion for the first five

⁵⁴Muris, *supra*.

⁵⁵*Id.*

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 customer's calling patterns to market services to them cost almost \$30 per customer contacted.⁵⁶

A 2000 Ernst & Young study of financial institutions representing 30 percent 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's 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, increase the availability and lower the cost of credit, provide co-branded credit cards and nationwide automated teller machine networks, 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 AEI-Brookings Joint Center on Regulation, the initial cost of complying with even a modest access requirement in online privacy legislation would be \$9-36 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 percent of the total amount raised by U.S. charities in 2000.⁵⁹

Ultimately, it is consumers and individuals, in the words of federal judge and former 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

Zealous Enforcement

The costs of privacy regulation are exacerbated by unusual features of the ways in which privacy laws are enforced in the United States. State attorneys general are generally authorized to enforce laws that are also enforced by the FTC. This means that an alleged breach of a privacy law can be the subject of not only a federal inquiry but also as many as 50 state inquiries. In addition, U.S. law often allows for class action lawsuits—where one individual sues on behalf of a large group of other individuals. Since harm is not required to violate many private laws, this can lead to multiple overlapping lawsuits where no injury has been caused. Moreover, as already noted, the FTC and state Attorneys General have indicated that they consider privacy policies, even if adopted voluntarily, to be legally binding contracts, without regard for whether a data subject read or relied on the notice. Again, this allows for more litigation without evidence of consumer injury or willful or negligent conduct by the processor.

⁵⁶Brief 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).

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

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

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

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

Enforcement in the United States has also become increasingly punctilious, begun with often hair-trigger speed. Actions that in no way compromise privacy, or that were mere errors, corrected as soon as they were detected, have become the basis for investigations and litigation in the United States. The effect is not to enhance privacy, but to distract attention and resources from real privacy issues to focus instead of technical legal issues that may be used to generate headlines for government officials and fees for attorneys.

The U.S. tendency for pile-on litigation poses special risks in data protection, because if a data processor makes an error it is likely to affect millions of records. If every data subject has a lawsuit and every state Attorney General can bring an action, the sheer cost of responding (even when the processor acknowledges the error) may threaten the processor's livelihood and result in expenditures far beyond what is necessary to compensate data subjects for any harm done. "[R]egulation via lawsuit is a terrible outcome—uncertain, costly, resulting in bad allocation of resources, and often not improving the underlying problem, if one exists."⁶¹ Data protection laws would work better if they permitted appropriate enforcement, but only by an appropriate federal agency or state Attorney General in the state where the activity took place. Private lawsuits and class actions should be reserved for unusual circumstances, involving demonstrable harms, not adequately addressed by government enforcement.

The same need to limit the number of duplicative oversight authorities is present in data transfers between countries. Under the safe harbor negotiated between the U.S. Department of Commerce and the European Union Commission, European data protection officials continue to exercise investigatory and enforcement authority over activities (especially those involving human resources data) that occur in the United States. Given that U.S. oversight is already committed under the safe harbor to the FTC (or in some cases to the Department of Transportation) the presence of multiple government regulators is wasteful and expensive. The principle of oversight belonging to the government with jurisdiction over where the act occurred—which, under the directive, is followed within Europe—should be applied to data protection in other countries as well.

Conclusion

Even this brief survey of U.S. privacy demonstrates that it is highly contextual, depending on industry sector, type of information, intended use, and geographic location. These features are the result of many factors. Some, like the division of governmental responsibility between three branches of government and between the federal, state, and local levels reflect distinctive characteristics of the U.S. legal and political system. Other features that contribute to the variety and complexity of U.S. privacy law reflect experience that may offer useful lessons—both positive and negative—for other nations as they consider their privacy laws. These include:

- Recognition of the economic and societal value of accessible personal information. As nations and industries become more information-dependent, access reliable, accurate, personal data is key to economic growth, innovation, and service. Privacy protections must not overly burden the availability of this information.
- Inevitability of conflicting interests and need for careful balancing. Privacy protection is always in tension with other interests and values. The goal, therefore, of privacy law should be to maximize individual and public benefits. Laws that treat privacy as an absolute fail to do this; they are unworkable and undesirable. Laws that recognize competing interests and compliance costs and seek to balance those with the goal of protecting privacy, taking into account the sensitivity of information involved and the risk of harm, achieve a better outcome at lower cost.

⁶¹Kent 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).

- Advantage of focusing on harm rather than choice. As the U.S. system has evolved to become more like the European system, it has relied more and more on regulations that do not afford effective protection to privacy but that prove burdensome and expensive to implement. As Professor Paul Schwartz has written, choice-based systems about privacy “promise too much, namely data control, and deliver too little.”⁶² Focusing privacy laws on preventing harm, rather than implementing bureaucratic procedures for facilitating consumer choice, helps to reduce the conflict with other interests, reduce compliance costs, and ensure that those costs are justified.
- Different rules for government collection and use of personal data than for private-sector processing. This reflects important differences between the public- and private-sector settings and the difficulty of relying on market-based protections and self-help when dealing with the government.
- Heavy dependence on market forces and individual action, backed up by law, in the private sector. This allows for more sensitive and individualized balances between the benefits and burdens of privacy protection, and facilitates faster innovation in the development of new tools for protecting privacy in response to new technologies and other challenges.
- Challenge of diverse, multinational information flows and their growing importance to domestic and international commerce. Privacy law in the United States, as in most other countries, has responded poorly to the transborder data flows, even as those flows have become more critical to people and societies around the world. The complexity and inconsistency of U.S. privacy law, the prevalence of overlapping state and federal laws and enforcement, and the absence of a federal privacy office or officer have all contributed to this problem. There are positive steps, especially in the context of privacy discussions within the Asia Pacific Economic Cooperation forum, to help remedy this situation, but it remains the most pressing challenge for privacy law world wide.

⁶²Paul M. Schwartz, “Privacy and Democracy in Cyberspace,” 52 *Vanderbilt Law Review* 1607, 1677 (1999).