ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **rgellman@netacc.net**
Washington, DC 20003

The American Way of Privacy

Prepared for

Colloque
Informatique: Servitude ou Libertés?

Sponsored by

National Commission for Information Technology and Liberties
French Senate
Université Pantheon-Assas Paris II

Palais du Luxembourg
Paris

November 7-8, 2005

The American Way of Privacy

By Robert Gellman
Privacy and Information Policy Consultant

I. Introduction

The American method of privacy regulation is sometimes described as a sectoral approach. This contrasts with the omnibus approach to privacy used by much of the rest of the world. An omnibus approach generally relies upon comprehensive privacy standards based on Fair Information Practices (FIPs) and enacted into law with applicability to nearly all types of personal data and record keepers. Another important feature of an omnibus approach is the establishment of an independent privacy supervisory authority.

A positive assessment of the U.S. sectoral approach emphasizes a careful selection of regulatory subjects and methods. America regulates activities and information for privacy only when a clear and focused need has been documented. Issues are typically left to the marketplace to resolve, and regulation follows only when there is a consensus that the market has failed, standards have developed in an inconsistent manner, or regulation would be more efficient. Privacy controls are then carefully tailored to the type of personal data and to the categories of record keepers who maintain and use the data. Methods for enforcing privacy laws also vary with the type of data and record keeper. Enforcement often relies on existing institutions with experience regulating the regulated institutions. Concern about constitutional protections for speech is also a regular feature of privacy debates in the United States.

A negative view of American privacy regulation observes that privacy laws and policies typically follow from crises, horror stories, or the uncoordinated efforts of individual legislators. Only some personal information is subject to any privacy regulation, without any overarching policy theme and with many major gaps in coverage, especially for private sector data. Laws are often based on a subset of Fair Information Practices, but not all laws implement the same elements of Fair Information Practices or do so in the same manner. Enforcement mechanisms for privacy laws vary significantly, and enforcement efforts are often non-existent or occasional. Enforcement by data subjects is often impossible or impractical. The numerous institutions charged with some privacy oversight or enforcement activities have narrow authority, and privacy enforcement for all enforcement agencies is at best a secondary function. No single institution has a broad responsibility for privacy policy, oversight, or enforcement.

This paper describes major elements of American privacy regulation. Rather than offering a comprehensive catalog of privacy law, court decision, and other materials, the paper selects examples that illustrate features, laws, policies, and institutions.

II. Scope of American Privacy Laws

A. Federal

1. Constitutional Law

Federal constitutional protections for information privacy are limited and uncertain in scope. In *Whalen v. Roe*, the Supreme Court described its own decisions involving privacy as protecting two kinds of interests.[1] One is the individual interest in avoiding disclosure of personal matters, and the other is the interest in independence in making certain kinds of important decisions (e.g., matters relating to marriage, procreation, contraception, family relationships, child rearing, and education). The Supreme Court never squarely defined the scope of constitutional protection for personal information, and lower courts decisions drew different conclusions from the Supreme Court's decision.

Constitutional standards give individuals rights against the government but not against other individuals or legal persons. Thus, the Fourth Amendment's protection against unreasonable searches and seizures only limits the power of the government to search houses and seize private papers. The protections of the Fourth Amendment do not apply when the government obtains personal information from third party record keepers.[2] In today's world where banks, telecommunications companies, and Internet providers are among the many institutions that maintain records on individuals, the constitutional protections lose some of their force.

Other provisions in the Constitution address other aspects of privacy, but not in any direct or comprehensive way. While the Constitution is not irrelevant to privacy protections for personal information, nearly all protections will be found either in statute or through the common law. Constitutional prohibitions against controls over speech create some tensions with privacy protections, but the courts have not extensively explored the conflict between speech and privacy.

2. Regulation of Federal Government Activities

The main data protection law for the federal government is the Privacy Act of 1974.[3] The Act applies to all federal agencies and to a limited class of government contractors. The law's origin offers a sharp contrast to most U.S. privacy laws because it was the product of a detailed policy process. An advisory committee established in 1973 studied the effects of growing public and private use of automated data systems containing information about

---

[1] 429 U.S. 589 (1976).

[2] *United States v. Miller*, 425 U.S. 435 (1976) (an individual has no expectation of privacy in account records in the possession of a bank). Congress partially overturned this Supreme Court decision in the Financial Privacy Act of 1978, 12 U.S.C. § 3401 et seq. However, that Act has many exceptions and limitations, and the degree of actual privacy protection is debatable.

[3] 5 U.S.C. § 552a.

individuals.[4] One product of this committee was the first published Code of Fair Information Practices, a code that Europeans later revised to serve as the basis for omnibus privacy laws.

A second set of recommendations led directly to the enactment of the Privacy Act of 1974. The law includes a complete set of fair information practices, including requirements for openness, access and correction rights, collection limitation, use and disclosure limitations, security, data quality, and accountability. Federal agencies have operated under the law for more than thirty years with few significant problems, although it appears that compliance with the Act is often indifferent.

There are four main problems with the Act. First, the law's technological model is the mainframe computer. The law is not well adapted to personal computers, databases, or the Internet. Second, the law applies to most but not all personal information that the government maintains. The distinction between regulated and unregulated information depends on how the information is retrieved, a distinction that makes little sense today. Third, the Act's controls on disclosure are only marginally effective. Agencies can easily avoid the purpose specification elements of the Act. Fourth, the Act is difficult for individuals to enforce, although enforcement is not impossible.

Despite the Act's shortcomings, it would probably qualify as providing an adequate level of protection under EU standards but for two major limitations. First, the law gives no rights to foreign nationals. Only U.S. citizens and resident aliens have rights. Second, the Act does not restrict forward transfers. If the government discloses personal information to anyone other than another federal agency, the information falls outside the protection of the Privacy Act of 1974.

3. Privacy Regulation for the Private and other Sectors

Federal regulation of the private sector is limited to those record keepers or records expressly covered by law.[5] In the absence of a specific law, it is likely that no formal regulation for privacy exists. Many records of routine commercial transaction remain unregulated for privacy. Merchants of all types, magazine publishers, restaurants, travel agents, charities, nonprofit organizations, and many others are often free to collect, use, or disclose personal information that they obtain from individuals without any statutory regulation. Many do just that. General regulatory laws – such as banking and telecommunications – sometimes provide limited consumer privacy protections through disclosure obligations or access rights. While these regulations are not unimportant, the focus here is on laws principally enacted to provide privacy protections and on the gaps in privacy protection provided by those laws.

· Fair Credit Reporting Act (1970) – The first modern federal privacy law was the Fair Credit Reporting Act (FCRA).[6] Although the law predated the development of the Code of Fair

---

[4] Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, (1973) (U.S. Department of Health, Education & Welfare), at http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[5] Professors Schwartz and Reidenberg describe private sector laws as revolving around "narrow rights addressing discrete issues." Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law: A Study of United States Data Protection 215 (1996).

[6] 15 U.S.C. § 1681 et seq.

Information Practices, the Act contains all of its elements. The Act passed originally largely due to the efforts of a Senator who organized congressional hearings that exposed the importance of credit reports to the ability to obtain credit, employment, and insurance as well as the lack of rights that individuals had with respect to credit records.

Under the FCRA, consumers have rights for records maintained by consumer reporting agencies and used by their clients. Access rights were recently enhanced, and consumers now have a right to a free copy of their credit report once a year. The law also includes better protections for identity theft victims. However, when businesses use comparable information from other sources (e.g., their own files or the Internet), the FCRA is not likely to apply. Regulation of affiliate sharing under the FCRA or other laws is either weak or non-existent. As more consumer information is accessible online through search engines or is available within a company (especially as a result of mergers among financial institutions), the importance of the FCRA may be slowly fading because of the rise of unregulated data sources.

A second limitation is that part of a credit file – known as *credit header information* – is not subject to regulation because of a decision made years ago by the Federal Trade Commission, the agency responsible for oversight of the FCRA. Credit header information includes name, address, former addresses, telephone number, date of birth, and Social Security number. Lists of most Americans and most households can be constructed from credit header data alone, and most vendors of these lists are unregulated for privacy. Entire spheres of commercial data activity exist solely because of the credit header "loophole".

· Family Educational Rights and Privacy Act[7] (1974) – This law provides access rights and disclosure limitations for student records maintained by federally funded schools and colleges. The law provides no privacy protections for students in institutions that do not receive federal funds. The Act offers no protections for records about faculty, staff, alumni, or contributors at any educational institution. The law originally passed as the result of a floor amendment by a Senator and without any hearings or meaningful debate.

· Cable Communications Policy Act[8] (1984) – A comprehensive regulatory scheme for the cable television industry provides some privacy protections, including disclosure restrictions for records that show the programs watched by a subscriber. However, consumers who obtained television services through direct broadcast satellite had no comparable legal protections until a new law passed more than 20 years later.[9] Should a new form of television transmission evolve, it will take another act of Congress to extend privacy protection to viewers.

· Video Privacy Protection Act[10] (1988) – During a controversial hearing on the confirmation of a Supreme Court justice, a reporter disclosed the titles of movies that the nominee rented. While the disclosure was not a factor in the defeat of the nominee, some Members of Congress were unhappy that the records were not private, perhaps because of concern that someone might disclose their own video rental records. The Video Privacy

[7] 20 U.S.C. § 1232g.
[8] 47 U.S.C. § 551.
[9] 47 U.S.C. 338.
[10] 18 U.S.C. §2710.

Protection Act was the result, and it provides narrow protection for records of video purchases and rentals. There is, however, no comparable statutory protection for information about purchases of books, magazines, or other similar materials.

· Driver's Privacy Protection Act[11] (1994) – This law restricts the disclosure and use of driver's license and motor vehicle records by state motor vehicle departments. The law's origins include the murder of a television actress by a deranged fan who obtained her home address through public motor vehicle files. States have their own laws and policies for motor vehicle records, but they must also comply with the federal restrictions. The federal law originally allowed marketing disclosures if drivers did not object, but a 1999 amendment made at the insistence of a single Senator changed the policy so that marketing disclosures now require affirmative consent. While this federal law regulates motor vehicle registers maintained by the states, none of the other numerous public registers maintained by the states is the subject of federal privacy legislation.

· Children's Online Privacy Protection Act[12] (1998) – This law establishes rules governing the collection, maintenance, use, and disclosure of individually identifiable personal information obtained online from children under the age of 13. However, there is no comparable regulation for information collected from older children or for information collected from children of any age by telephone, fax, or otherwise.

· Health Insurance Portability and Accountability Act[13] (1996) – This federal law authorized the issuance of health privacy rules by the Department of Health and Human Services. The rules took effect in 2003.[14] The regulation applies to health care providers, health plans, and clearinghouses. The regulation provides for openness, access and correction rights, limits on use and disclosure, and accountability, but many of the protections have significant exceptions or procedural limitations. Further, many institutions (e.g., law enforcement, public health, health oversight, courts, and researchers) permitted to obtain identifiable information without patient consent fall outside the regulatory scheme. The federal health privacy rule does not restrict their subsequent processing of the information. Other major institutions that routinely use health information, including life insurers, worker's compensation, and marketers, are not subject to the federal regulation for health privacy.

B. State laws and federal preemption

1. Constitutional Protections

Some state constitutions expressly recognize privacy as a basic right. The strongest state constitutional protection is in California, where a 1974 referendum made privacy one of several "inalienable rights".[15] The California Supreme Court held in 1994 that the constitutional

[11] 18 U.S.C. § 2721 et seq.
[12] 15 U.S.C. § 6501 et seq.
[13] 42 U.S.C. §1320d-2 note.
[14] 45 C.F.R. Parts 160 & 164.
[15] Cal. Const. at I, § 1.

protection applied to both the public and private sectors.[16] The full effect of the constitutional provision is still unclear. Other state constitutional protections for privacy do not appear to be as robust as California's.

2. State Laws

State laws on privacy vary enormously from state to state. About a quarter of the states have general privacy laws applicable to state records. State laws on health privacy are numerous, but the scope, quality, and currency cannot be easily characterized. Some states have more modern comprehensive health privacy laws, some do not, and others have old-fashioned laws that do not reflect the complexity of health care record keeping activities. All states have dozen of laws that affect health record keeping, but the laws may be different for different record keepers (physicians, pharmacists, psychiatrists), institutions (insurers, hospitals, nursing homes), and type of record (genetic, substance abuse, mental health). No state has the same regulatory scheme for health records. Privacy statutes regulating commercial record keepers are occasional, and most records and record keepers are unregulated for privacy at the state level.

3. Public Registers

State and local government maintain large numbers of records about individuals. These include motor vehicle registrations, land titles, property tax records, voting registration records, occupational licenses, firearms permits, court records, law enforcement records, financial disclosure (ethics) records, hunting and fishing licenses, and more.[17] While policies vary from state to state and from record system to record system, many of these records are public registers that are available in whole or in part for public uses. Private sector data brokers make extensive use of these records to develop personal and household profiles. The availability of these records over time allows lifetime tracking of addresses, financial and other activities, and living arrangements. Federal law only restricts disclosure of motor vehicle information. Because of concerns about identity theft, states have been reconsidering disclosure policies for some of these records.

4. Federal Preemption

The federal government and the states often share legislative jurisdiction over many aspects of commerce. Privacy regulation is sometime undertaken by the states, sometimes by the federal government, sometimes by both, and sometimes by neither. The federal government often has the authority to preempt state action, and federal preemption for privacy is an increasing trend.[18] Companies often oppose privacy legislation at the state and federal levels. After states begin to pass legislation, however, business sometimes supports a weaker federal law that preempts all state laws. The argument is that compliance with a uniform law would be

---

[16] *Hill v. NCAA*, 865 P.2d 633 (Cal. 1994).

[17] See Robert Gellman, *Public Records: Access, Privacy, and Public Policy*, 12 Government Information Quarterly 391-426 (1995).

[18] A California law that provided stronger privacy protections for financial records was recently held to be preempted by the federal Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 117 Stat. 1952. *American Bankers Association v. Gould*, 412 F.3d 1081 (9th Cir. 2005); on remand *American Bankers Association v. Lockyer* 2005 U.S. Dist. LEXIS 22437 (E.D. Cal., Oct. 4, 2005).

easier. States and privacy advocates generally oppose federal preemption because of federalism concerns and because federal laws often provide less privacy protection than the state laws that they preempt. The current trend in legislation is for federal privacy laws to preempt state laws in whole or in part.

C. Conclusions

The American sectoral approach produces privacy laws that offer limited protection for narrow categories of personal information, with differences in the nature of the protection from law to law. Similar categories of information may have widely disparate privacy rules, ranging from strong to non-existent. Many types of personal records maintained by private sector record keepers are not disclosed to the public and are not regulated for privacy at all. Some personal information is regulated in the hands of some record keepers while comparable information remains unregulated in other hands. It can be difficult even for lawyers to know what privacy law, if any, applies to personal information. It is rare for a privacy rule to follow records as they are transferred from the original record keeper to another user. Constitutional protections for government actions exist, but the protections are often narrow and their scope uncertain.

III. Enforcement Mechanisms

A. Privacy Torts

When there are no statutory protections for privacy, private tort litigation may provide a remedy for individuals. American jurisprudence about privacy began with a famous Harvard Law Review article from 1890 that proposed a privacy tort.[19] The four privacy torts most often recognized by state law are 1) intrusion upon an individual's seclusion or solitude; 2) public disclosure of private facts; 3) placing an individual in a false light highly offensive to a reasonable person; and 4) an unpermitted use for private commercial gain of a person's identity.[20]

The value of tort law for the protection of information privacy is far from clear.[21] Because of the often-hidden nature of the commercial exchange, compilation, and use of personal information, data subjects rarely know how frequently merchants and data brokers collect, use, and share personal information. The lack of transparency makes remedies difficult for consumers to consider.

Tort actions have inherent limits otherwise. The scope of relief available through lawsuits will often be limited to monetary damages. Most elements of fair information practices are not directly attainable through tort litigation. The classic privacy torts are not likely to induce a record-keeper to publish descriptions of record systems, limit collection practices, meet

---

[19] Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).
[20] 3 Restatement (Second) of Torts §652A et seq. (1977).
[21] Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 Cornell Law Review 291, 334 (1983) ("After ninety years of evolution, the common law private-facts tort has failed to become a usable and effective means of redress for plaintiffs"); Fred H. Cate, Privacy in the Information Age, 90 (privacy torts "offer little protection for information privacy.").

data quality standards, allow individual access and correction, or restrict internal uses of data. Successful litigation could induce companies to reform practices, but successes by consumers in information privacy cases are rare. The threat of litigation can, however, influence privacy practices of some corporate actors.

B. Statutory Enforcement Methods

Enforcement of privacy statutes can be accomplished in different ways. Some laws provide more than one enforcement method. Many, but not all privacy laws, provide individuals with a cause of action that allows them to pursue lawsuits for violations. However, even when lawsuits are possible, they can be difficult to pursue. It if often hard to prove damages in privacy cases, and the lack of a sizeable recovery makes it difficult to find lawyers willing to take a case. Recent federal privacy laws tend not to permit private rights of action.

The Privacy Act of 1974 provides a private right of action with minimum statutory damages of $1000. The standard for proving damages is hard to meet, and a recent Supreme Court decision made success even harder to achieve.[22] The remedy has long been recognized as ineffective. The Act also provides for enforcement through a criminal misdemeanor punishable by a modest fine. The criminal penalties have been used a few times in thirty years.

The Cable Communications Policy Act includes a private right of action for cable television subscribers against cable operators. The private right of action is the only statutory enforcement mechanism in the Act. Because the Act establishes standards for openness, data quality, purpose specification, use limitation, and individual participation, a cable operator's failure to comply with any of these FIPs could form the basis for a lawsuit. Successful cases by individuals are rare.

The Driver's Privacy Protection Act has two civil enforcement methods in addition to the possibility of a criminal fine. The U.S. Attorney General can seek to impose a civil fine on a state that is in substantial noncompliance with the law. An individual can sue a person who obtains, discloses, or uses personal information from a motor vehicle record for an improper purpose. The State of Florida did not comply with the Act, and a private class action lawsuit was brought against companies that continued to buy drivers' records in violation of federal law. The litigation is not complete, but the plaintiffs recently won an important ruling that may allow them to recover significant damages.[23]

Administrative enforcement is sometimes the only option. The Family Educational Rights and Privacy Act can be enforced by the U.S. Department of Education by: 1) withholding payments to a school under any federal program; 2) a complaint to compel compliance through a cease-and-desist order; and 3) termination of eligibility to receive future funding. The statute makes it clear that ending funding is a last resort. Attempts to enforce the law through a private right of action failed.[24]

---

[22] *Doe v. Chao*, 540 U.S. 614 (2004).
[23] *Kehoe v. Fidelity Federal Bank & Trust*, 2005 U.S. App. LEXIS 18406 (11th Cir.).
[24] *Gonzaga University v. Doe*, 536 U.S. 273 (2002).

Recent privacy laws tend to provide only for administrative enforcement rather than private rights of action. Trials lawyers are not in favor with the political party that controls the White House and the Congress, and the creation of new opportunities for litigation attracts little support. Businesses that are the subject of privacy regulation also generally oppose private rights of action. Here are some of the recent laws that individuals cannot enforce through private litigation:

· The Children's Online Privacy Protection Act provides for enforcement by the Federal Trade Commission and by State Attorney Generals. Individuals cannot enforce their rights under the Act.

· The Gramm-Leach-Bliley law that regulates financial services companies is enforceable by federal banking regulators, state insurance authorities, and the Federal Trade Commission.[25] At least seven different federal agencies have enforcement authority under the law, reflecting the general diversity of banking industry regulation. The law does not provide a private right of action.

· The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) is considered by some to be a privacy law. It provides for enforcement by several federal agencies, by states, and by Internet service providers, but not by individuals. The federal act eliminated some state remedies formerly available to individuals.

· The health privacy rule issued under the Health Insurance Portability and Accountability Act has administrative enforcement and criminal penalties, but it provides no private right of action. In the first two years of experience with the rule, not a single administrative enforcement action was brought. The criminal penalty was used once to prosecute criminally an identity thief, but a new interpretation of the law by the Department of Justice significantly narrows the applicability of the penalty so that many recipients of health information will not be subject to prosecution no matter how they may misuse the information.[26]

Overall, administrative enforcement has been occasional, at best. The Wall Street Journal recently reported that the Federal Trade Commission receives every day between 1000 and 2000 complaints about violations of the Do Not Call law.[27] However, the FTC has filed only fourteen lawsuits and levied only four fines. The Federal Communications Commission, which also has responsibility, fined only two companies.[28] In another privacy case, the FTC took action against a company that sold its customer list in violation of the company's own privacy policy. The fine was precisely the amount of revenue that the company received for the list.[29]

---

[25] 15 U.S.C. § 6805.
[26] Department of Justice, Office of Legal Counsel, Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6 (June 1, 2005) at http://www.usdoj.gov/olc/hipaa_final.htm.
[27] 15 U.S.C. § 6101 note.
[28] Christopher Conkey, *Do-Not-Call Lists Under Fire: After Two Years and One Million Complaints, Only Six Federal Fines Have Been Issued*, Wall Street Journal, Sept. 28, 2005, D1.
[29] http://www.ftc.gov/opa/2004/07/gateway.htm.

C. Self-Regulation and Industry Standards

It is difficult to evaluate self-regulation by business groups. Some groups touted as promoting business compliance with privacy standards no longer exist. The Individual Reference Services Group is no longer in operation. The Online Privacy Alliance still maintains a website, but nothing recent is posted there.[30] The organization does not appear to be active. The Privacy Leadership Initiative disbanded after a few years. One view of some of these organizations is that the main purpose was to lobby against the passage of privacy legislation. The Individual Reference Services Group, for example, disbanded after passage of the Gramm-Leach-Bliley law regulating financial institutions. The group said that it was no longer needed because there was statutory privacy regulation. However, the law offered limited privacy regulation, and that regulation did not generally apply to members of the group. It appears that the group disbanded for lack of interest by its members.

TRUSTe is an independent, nonprofit organization that maintains self-regulatory programs, including a privacy seal program, for Internet organizations. The organization is active, and its seal can be found on many websites. It reports on the number of privacy complaints that it receives, but it is difficult to determine the results of the complaint process or its effectiveness. The website reports that in the most recent completed year (2004), no investigations or terminations of members occurred.[31]

The Better Business Bureau also offers a privacy dispute resolution program through its BBBOnLine Privacy Program. Some statistics are available on its website,[32] but there are few published decisions. No enough information is available to evaluate the program. Other privacy seal programs are no longer operating.

D. Enforcement Conclusions

Overall, enforcement of privacy laws in the United States is of questionable effectiveness. While many enforcement methods are available in theory, privacy laws sometimes do as much to limit enforcement as to encourage it. Private remedies – whether statutory or common law – are welcomed by the privacy advocacy community, but lawsuits are difficult to bring and expensive, and recoveries are infrequent. Proving damages can be difficult. Lawsuits tend to be most successful when the facts are sufficient egregious to sway a jury. The threat of a lawsuit may be a mildly effective enforcement tool, but the hazard of adverse publicity from a privacy horror story may be even more effective. On the other hand, aggressive business lobbying against private remedies suggests that lawsuits are unwelcome. Whether that means that lawsuits are effective, costly, or merely bothersome is debatable.

The effects of administrative enforcement on privacy compliance are not clear. The enforcement agency with the most jurisdiction is the Federal Trade Commission, but the scope of that jurisdiction is significantly restricted. The Commission argues that it has limited resources, but that its occasional enforcement actions provide a real incentive to business to comply with

[30] http://www.privacyalliance.org.
[31] http://www.truste.org/consumers/watchdog_advisories/2004.php.
[32] http://www.bbbonline.org/privacy/dr.asp.

privacy standards. The Commission brings few cases, and it rarely imposes significant penalties on violators or provides any remedies for consumers.

Evidence about private sector enforcement mechanisms, including seals and audits, is limited. The regular demise of business-supported organizations dedicated to privacy enforcement or privacy activities in general may be a telling indicator of fundamental lack of interest on the part of the business community. Seal programs and trade association activities are financed by the businesses that use them, and their privacy dispute resolution programs may have no independent participation, reporting, or auditing.

In some ways, the most effective enforcement mechanism may be the possibility of adverse publicity. A privacy incident that results in a widely reported horror story may produce the greatest change in law and practice. For example, recent press accounts of security breaches and other privacy shortcomings at ChoicePoint and other companies attracted widespread public and legislative interest. The stories not only made companies more aware of their own security and legal vulnerabilities, but they spurred the passage of more security breach notification laws by many states. Federal legislation is pending. In the end, however, the result of these incidents is more activity and legislation addressing elements of privacy in the typically uncoordinated and piecemeal American manner.

IV. U.S. Privacy Institutions

The institutions that oversee or enforce privacy in the U.S. show the same diversity that is characteristic of American approaches to privacy generally. Institutions are created or assigned new roles without much forethought or coordination. No government institution plays a primary role for privacy or has comprehensive jurisdiction.[33]

A. Office of Management and Budget

Because of its role in formulating the President's budget, the Office of Management and Budget (OMB) is a powerful agency. Congress assigned OMB an oversight role for the Privacy Act of 1974. However, OMB's management activities have always been secondary to its budget functions, and privacy receives little attention. With one significant exception, OMB traditionally assigns one staff member or less to work on privacy matters. OMB is not an enforcement agency and cannot be expected to play any operational role in privacy enforcement or to help data subjects. OMB only has a defined – and rarely exercised – role in oversight of federal agencies.

The one period of expanded administrative attention to privacy came during the Clinton Administration. Clinton established a privacy counselor at OMB in March 1999. The privacy counselor played a role in Privacy Act of 1974 oversight and participated actively in other privacy policy and legislative matters. However, the Bush Administration abolished the position

[33] For a more detailed review of U.S. privacy institutions, see Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 Hastings Law Journal 1183 (2003); Robert Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, VI Software Law Journal 199 (1993).

when it took office in January 2001, and the broader policy work that the privacy counselor undertook has disappeared from the executive branch of government.

Some other federal agencies – principally at the State Department and Commerce Department – have occasionally become involved in international privacy or privacy policy matters, but these activities are fitful. The Department of Homeland Security has taken on a role in some international aspects of privacy related to anti-terrorism activities.

B. Privacy Officers

Some federal agencies established privacy offices following passage of the Privacy Act of 1974. These offices typically focus narrowly on implementation of the Act, and most never play any role in broader privacy policy. In the 1990s, the Internal Revenue Service and the Department of Health and Human Services established small privacy offices with a broader function. Congress established the first statutorily created privacy officer when it created the Department of Homeland Security in 2002.[34] The position has no independence. The Secretary of the Department appoints the privacy officer, and the first privacy officer was a political appointee who served at the pleasure of the President. Legislation has been proposed to give the privacy officer more authority and a fixed term, but prospects are highly uncertain. It remains to be seen if it is possible practically or politically to have a privacy office within a department function with any real degree of independence.

In a 2004 law, Congress directed each agency to establish a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy.[35] The legislation passed without any hearings or debate because a single Senator placed the requirement in an appropriations bill. A member of the House of Representatives introduced a bill to repeal the provision before it even became law. While the requirement for more attention to privacy may be welcome at some level, the Chief Privacy Officers were given no resources to carry out their statutory functions. Another part of the law requires agencies to hire independent third party auditors to review privacy activities. That part of the law was rumored to have been written by a privacy consulting company seeking to obtain more government business. Nearly a year later, almost nothing has been done to implement any of the requirements of this law.

C. Privacy Impact Assessments

In 2002, Congress passed a law requiring agencies to conduct a privacy impact assessment (PIA) when employing new information technology or undertaking new collections of information.[36] The required elements of a PIA contain little more than privacy notices already required under the Privacy Act of 1974, with no requirement for a substantive assessment of privacy and no requirement that agencies pay attention to the PIAs that they prepare. While the PIA process has not been evaluated to date, anecdotal evidence suggests that some agencies have used PIAs effectively. At other agencies, the PIA process lacks substance, commitment, and a clear role in the decision making process.

---

[34] 6 U.S.C. § 142.
[35] 5 U.S.C. § 552a note.
[36] 44 U.S.C. § 3501 note.

D. Federal Trade Commission

The privacy institutions discussed above focus almost exclusively on federal government activities. The principal agency with the most jurisdiction over private sector privacy activities is the Federal Trade Commission (FTC). The Commission has specific enforcement responsibilities over several privacy laws. In some cases, numerous other agencies share enforcement responsibilities because the industry being regulated is subject to multiple regulators. When multiple agencies enforce the same law, it is a common practice to issue identical regulations.

The FTC's other jurisdiction derives from its ability to pursue unfair or deceptive acts or practices.[37] The authority is potentially broad, but the FTC's jurisdiction over the private sector is not comprehensive. Major segments of the economy – banking, insurance, telecommunications – may not be subject to the Commission's jurisdiction. The large nonprofit sector is also generally beyond the FTC's authority. While the FTC has issued regulations implementing some privacy statutes, it has not issued any general rules defining what constitutes an unfair or deceptive privacy practice. Its legislative authority makes it difficult for the Commission to promulgate rules of that type. The FTC has pursued a few companies that failed to comply with their own privacy policies because making a case for an unfair or deceptive practice is easier when a company has a formal policy. Companies learned that they may be in a better position if they do not have a privacy policy or if they have a policy that is broad, vague, or lacking in enforceable standards.

The Commission's authority over unfair and deceptive practices provides an enforcement backstop for some privacy self-regulatory programs, including the Safe Harbor program for U.S. companies seeking to comply with European Union standards. The Commission makes the programs appear to have actual enforcement, although the agency is so highly selective in the cases that it brings so it is not clear how much of an actual deterrent exists. Further, the Commission does not resolve individual consumer problems and may not offer any meaningful help to individual consumers harmed by a company's failure to comply with a stated privacy policy.

E. Corporate Responses

One recent corporate response to privacy has been the establishment of Chief Privacy Officers (CPOs) in many American corporations. The International Association of Privacy Professionals[38] reports that it has more than 1000 individual and corporate members, and many of its members are CPOs at major corporations. The number and actual function of corporate CPOs is uncertain, and there is evidence that some CPOs have little power and few resources while other CPOs are more powerful. Some function primarily as compliance officers. Regardless, the functioning of a professional society/trade association for privacy professionals is a sign that the corporate movement for CPOs has developed roots.

---

[37] 15 U.S.C. §57a(a)(1)(B).
[38] http://www.privacyassociation.org/.

While it is difficult to assess the corporate CPO movement, it is clear that the activity is substantial. For whatever reason, many corporations see privacy as an area that requires significant attention and coordination. While U.S. privacy legislation is still occasional, large companies with multiple lines of business – and especially those with international operations – find that merely keeping track of applicable privacy rules is a complex task. The establishment of CPOs in many companies represents a sincere effort to deal with privacy. The CPO movement was spurred in part by the requirement in the federal health privacy rule that each covered entity have a privacy officer. At major medical institutions, a privacy officer is likely to be a full-time job.

Another development of the last decade has been the adoption of privacy policies on most commercial websites. These policies responded to consumer concerns, government pressure, and business attempts to avoid regulation through legislation. Also, some legislation requires websites, health care institutions, banks, and others to have privacy policies. While the content of the policies has been questioned, the spread of policies is a notable development and, in at least some instances, a market response to privacy concerns of consumers.

F. Privacy Advocates

The privacy advocacy community has grown in numbers and in importance in the past decade. Leading groups with major privacy functions include the Electronic Privacy Information Center, Center for Democracy and Technology, Privacy Rights Clearinghouse, Electronic Frontier Foundation, American Civil Liberties Union, Public Interest Research Group, World Privacy Forum, Privacy Activism, and others. Many other groups whose principal concerns involve issues not directly related to privacy also participate occasionally in privacy activism.

While privacy advocacy groups do not play an official role in any privacy enforcement activity, they are nevertheless important. The groups find and publicize privacy problems, and they help to cultivate the privacy horror story culture that tends to drive events in the U.S. These efforts will sometimes affect the immediate legislative agenda, but they do not necessarily help to address or achieve broader, long-term strategic goals.

Some privacy groups are active lobbyists in legislative efforts on privacy, especially in California and at the federal level. Some also seek to use the Federal Trade Commission to further a privacy agenda. In several recent cases, the FTC took enforcement action after a privacy group filed a complaint about an industry practice. For reasons suggested elsewhere in this paper, FTC actions may leave much to be desired, but privacy groups are typically pleased to see a response to their complaints.

The business community tends to overestimate the importance of privacy advocates in the overall scheme of privacy policy making and enforcement. Privacy groups tend to be more effective in calling congressional attention to a privacy matter. However, business lobbyists have generally been more effective in achieving their goals with the substance of federal privacy legislation. This pattern is likely to continue unless there is a shift in control in the Congress or the White House. Nevertheless, privacy groups have a voice and have sometimes achieved compromises that improve privacy protections.

G. Structure Conclusions

Like so much else about American privacy law and policy, structures to oversee and enforce privacy standards are highly variable in form, location, and function. Government institutions with privacy responsibilities always have other functions, and privacy is typically a secondary activity, at best. Corporate structures are hard to assess, but much has happened in the last decade that appears to be positive. One reason for the acceptance of structural responses to privacy is that it may be easier to offer procedural changes rather than substantive restrictions on information processing functions. Privacy activists continue to play a significant role in calling attention to privacy problems and in helping to place issues on the legislative agenda.

V. Conclusions

At the beginning of this paper, two sharply divergent views of the American approach to privacy were offered. Many intermediate judgments, particularly on specific laws and activities, are also possible. Without question, however, the American regulatory framework for privacy has major gaps, inconsistencies, and weaknesses. Only a few American privacy laws fully address all elements of Fair Information Practices or would arguably qualify as adequate under the EU Data Protection Directive. American laws rarely control onward transfers of personal information, and few laws expressly recognize the possibility that regulated information could be transferred to another jurisdiction with weaker privacy regulation. Another major gap is a lack of transparency. In particular, the collection, maintenance, use, and disclosure of personal information by corporations often occur without any notice to consumers. Entire segments of the personal information industry are unknown to the American public because of a lack of transparency. Many companies do not want to tell customers how much personal information is collected routinely or how that information is used or disclosed.

Two different current issues illustrate some of the political and policy dynamics of privacy. The growth of identity theft has been a major driver for legislation. Because of identity theft, the public is now fully aware that misuse of personal information can lead directly to significant harm. Privacy advocates have a clear answer to business objections that consumers are not harmed by the widespread sharing of personal information.

The continuing surge of publicity about the costs and consequences of identity theft prompted the federal government and many states to pass legislation adding criminal penalties, expanding the jurisdiction of courts, providing assistance to victims, creating new remedies, and requiring security. Other laws impose collection and use limitations for specific categories of personal data or on particular government or private record keepers.

While American legislatures have passed many laws responding to identity theft, the efforts are not sharply focused, have done little to deter criminals, and have done only a little to improve general privacy protections. Some laws have made it easier for victims to address the consequences of identity theft and for government to prosecute victims. The diffuseness and difficulty of the identity theft problem directed attention toward smaller responses and away from larger privacy issues.

However, the 2005 disclosure that ChoicePoint, a major data broker, had a security breach that exposed data to organized identity thieves produced a major change in legislative efforts. More states passed security breach notification laws, and preemptive federal legislation on security breach notification is now pending before the Congress and has a good change of passing. Federal privacy legislation seeking to regulate data brokers is also pending, although many observers doubt that the effort will succeed.

Regardless of the legislative outcome, the fresh horror story provided the spark that transformed the identity theft debate. The publicity led to new, broader proposals for privacy regulation of data brokers, something that was not under consideration earlier. The incident underscores the importance of adverse publicity as a driver of the American political process. If a legislative response emerges, it will surely be another privacy law regulating a particular sector in a way that will be different than the way that other sectors are regulated and that will continue to leave other privacy intensive activities unregulated.

The second example of a current privacy issue is technologically based. An American response to radio frequency identification (RFID) technology is still embryonic. The privacy consequences of RFID are attracting increasing attention from industry, policy makers, privacy advocates, and legislatures. The Federal Trade Commission held a workshop in 2004. California considered but did not pass legislation setting standards for using RFID on consumer products. A recently passed federal law called for a study of RFID use by motor carriers. Privacy groups have called for boycotts of companies using RFID chips. Several books on RFID technology and policy were recently published. Industry standards (both in the U.S. and elsewhere around the world) for the technology have paid some attention to privacy.

This early privacy interest in the RFID debate is relatively unusual in the United States. By contrast, the data broker industry developed in the last two decades with no public, policy, or legislative attention. International attention to the technology may have helped put privacy on the American RFID agenda.

It is not possible, however, to predict how or if the United States will ultimately respond. Industry appears firmly opposed to legislation, but that position could change if a state manages to pass a regulatory law. Industry might then seek a federal law to preempt state action on the grounds that the technology needs a single national standard. Public concerns might grow and force better market responses or a political solution. However, public concerns over new technology in the past have sometimes faded over time. When caller identification technology for telephones was first introduced, it provoked considerable opposition. Over time, however, the technology has been accepted with modest accommodation to those concerned about privacy. RFID use for highway tolls has drawn almost no privacy controversy.

So far, RFID technology lacks the horror story often needed to drive the American legislative process. Some uses on consumer products have drawn opposition and publicity, but not to the extent necessary to overcome industry's resistance to legislation and the inertia of the legislative process. Industry response to the concerns expressed by advocates may be enough to

assuage public fears. RFID remains a technology with many different possible privacy outcomes.

In many ways, the American approach to privacy is identical to the approach taken on many other important public policy matters in the United States. The American political system shapes laws and institutions through cycles of neglect, evolutionary changes, and occasional bursts of activity and innovation. This approach often produces inconsistencies and gaps. Broad assessments and reviews of policy approaches happen only occasionally, and they are often ignored when they do occur. A 1977 study commission on privacy issued a comprehensive report, but Congress enacted few of its legislative recommendations.

Rhetorical and political pressures for "market-driven" responses to policy matters and consumer demands are not limited to privacy. The importance of media attention to horror stories is also a phenomenon not limited to privacy. U.S. legislation is often enacted with little consideration to its international consequences.

It is difficult to suggest that these patterns are likely to change in the future in the privacy arena. There is scattered recognition (outside the privacy advocacy community) that a plethora of separate and inconsistent privacy laws is creating problems and increasing costs for business. In addition, international pressures on privacy have slowly increased awareness of the breath of interest in privacy, the benefits of more uniform standards, and the costs of disparate privacy regulatory regimes. One response to these concerns from the business community has been some support for the development of international privacy standards not as rigorous as those found in the EU Data Protection Directive.

Nevertheless, it is difficult to suggest that there is likely to be broad-based support for a more coherent or omnibus approach to privacy in the near future. The federal legislative structure makes it difficult to enact broadly applicable laws that cut across traditional sectoral lines and political power centers. Further, it will take much more time and effort before the need to address privacy spreads throughout the American business community. Should public concern about privacy fade, the business community is likely to dismantle quietly many of its privacy efforts.

Elements that are likely to continue to focus public and legislative attention on privacy – and that may ultimately produce a change in the American approach to privacy – include the spread of identity theft, phishing and other criminal activities on the Internet, private litigation, and responses to terrorism. While some anti-terrorism activities have negative implications for personal privacy, Congress and agencies have also been responsive in part to privacy concerns. It remains possible that pressures for more privacy invasive activities may be accompanied in the future by counterbalancing developments that augment or support privacy in other ways. That is how the first statutory federal privacy office – at the Department of Homeland Security – was established. Congressional oversight of airline security activities at the Transportation Security Administration at the Department of Homeland Security has been sharply focused on the need to address privacy in the passenger screening process.

The constitutional limits on government activities continue to be important to ongoing debates about national security and terrorism. Legislation and administration actions often arise at the edge of the constitutionally permissible, and the courts frequently serve as the final arbiters. One development receiving more attention as a result of the war on terrorism is the weakening of traditional distinctions between government and private sector activities. Increasingly, information processing functions that would be subject to regulation if conducted by federal agencies are contracted to private companies that are not regulated. This is an area where the piecemeal applicability of privacy legislation makes a significant difference. The law that applies to the federal government can be evaded by hiring private sector companies to provide data services.

Perhaps the biggest shortcoming in the American approach to privacy is the lack of a federal privacy agency. As each privacy matter arises – often prompted by media coverage of identity theft, security breaches, or unfair uses of personal information by companies or government – government typically responds as if approaching privacy for the first time. Without a permanent source of policy advice, policy makers and legislators tend to reinvent the wheel each time. While there is slowly growing recognition of Fair Information Practices as establishing fundamental privacy policy, each venture into privacy policy making tends to begin from a blank slate. That is one reason privacy statutes vary so much. Further, the Federal Trade Commission and business groups often redefine Fair Information Practices and use the label to promote policies that are different from international standards. When legislation finally succeeds, it tends to be characterized by sharp limits on the scope of coverage, restricted enforcement options, and substantive standards that are both weak and divergent.

An independent federal privacy agency could help to cure these shortcomings. It could provide expertise, oversight, support, and a consistent voice in privacy debates. While there have been proposals for a privacy agency from time to time in the past, there appears to be no meaningful political support for an agency at present.

Others have commented upon what might now be called the traditional inadequacies of the American approach to privacy. In 1992, Spiros Simitis described the American approach to data protection as "an obviously erratic regulation full of contradictions, characterized by a fortuitous and totally unbalanced choice of its subjects".[39] In 1989, Professor David Flaherty observed: "The United States carries out data protection differently than other countries, and on the whole does it less well, because of the lack of an oversight agency."[40] These two comments, while not recent, still fairly describe the American approach to privacy. There is little reason to expect a significantly different approach in the near future.

[39] Spiros Simitis, *New Trends in National and International Data Protection Law*, in Recent Developments in Data Privacy Law 22 (J. Dumortier ed. 1992).

[40] David Flaherty, *Protecting Privacy in Surveillance Societies* 305 (1989).