United States Privacy Law and Policy

Robert R. Belair and Kevin Coy

INTRODUCTION

Privacy has "arrived" as a major policy issue in the United States. In recent months, privacy has received front-page and editorial coverage in major newspapers, been featured on the cover of magazines, and been discussed on television talk shows and newscasts. Thousands of legislative proposals with privacy components have been introduced at the federal and state levels, and scores have been enacted. The public is increasingly concerned about privacy and increasingly willing to act on that concern.[1]

For privacy, this is an extraordinary time. While it is true that there was significant privacy activity in the 1970s—the so-called early days of modern information-privacy protection in the United States—including the adoption of the Privacy Act, the addition of very important privacy language to the Freedom of Information Act, and the creation of the Privacy Protection Study Commission, the level of activity then was nothing like what we have today; nothing like the level of state activity today, nothing like the level of media penetration today, nothing like the level of activity in the Congress today. And just to go back to the 1970s again for a moment, in 1979, 67 percent of the American public said it was concerned about privacy; today it is 94 percent. Such an extraordinary level of attention and activity confirms that a sea change is underway.

Privacy's new traction as an issue is further illustrated by the following statistics:

- A *Wall Street Journal*/NBC News survey found that the potential loss of personal privacy is the issue of most concern to Americans entering the new millennium. Concerns about personal privacy finished ahead of concerns about issues such as terrorism, overpopulation, world war, and global warming.

- An October, 1999, public-opinion survey for IBM conducted by Harris Interactive and Dr. Alan F. Westin[2] found that 80 percent of respondents believe that consumers have "lost all control over how personal information about them is circulated and used by companies."
- There has also been a major increase in privacy-asserting behaviors by US consumers. According to the IBM survey, the percentage of people who say they have refused to give information to a business or company because they thought it wasn't needed or was too personal has risen from 52 percent in 1990 to 78 percent in 1999. Also in 1999, 53 percent of respondents said that they have asked a company not to sell or give their name and address to another company, and 54 percent said they had decided not to use or purchase something from a company because they weren't sure how their personal information would be used.
- During the 105th Congress, over 150 bills addressing privacy were introduced and more than 40 days of congressional hearings were devoted to privacy issues. The 106th Congress is on track to match or exceed those levels.
- Privacy issues also received considerable attention at the state level. During 1999, over 7,300 privacy bills were introduced, an increase of over 3,000 bills from the previous year.

Amid this frenetic privacy activity, it is sometimes said that privacy protections in the United States are an uneven and inadequate patchwork. True, the United States lacks the sort of comprehensive privacy legislation found in many European countries. It is also true there are areas of US privacy law that might be strengthened. However, let's be very clear. It is wrong to dismiss US privacy protections as inadequate. As this article will detail, the US privacy environment presents a diverse, interwoven array of *de jure* and *de facto* protections, which, despite the occasional loose end, provides considerable protection.

The article begins with a brief examination of the history of information privacy, the democratic interests served by information privacy, and the growing public concern over information

privacy. The article examines the legal and self-regulatory privacy protections that exist in the United States, including protections arising from US constitutional law, common law, federal statutory law, and state constitutional and statutory law, as well as informal, *de facto* privacy protections, such as media scrutiny, the actions of advocacy organizations, and corporate self-regulatory efforts. Finally, the article identifies key trends in privacy law playing out over the next few years.

UNITED STATES INFORMATION PRIVACY ENVIRONMENT

What Is Information Privacy?

"Information privacy" is certainly the focus of intense public, legislative, and media attention, but what does it mean? The term "information privacy" does not have a universally-accepted definition. Customarily, the term is used to refer to standards for the collection, maintenance, use, and disclosure of personally-identifiable information. The ability of an individual to control the use of information about that individual provides the individual with "information privacy."

Information privacy is frequently distinguished from other clusters of personal interests that are nourished by the privacy doctrine, including surveillance privacy—the interest in being free from governmental and other organized surveillance of individual activities under circumstances where one has a reasonable expectation of privacy; and behavioral privacy—the right to engage in certain intimate and sensitive behaviors (such as behaviors relating to reproductive rights) free from governmental or other control.[3]

The principal focus of surveillance privacy and behavioral privacy, in particular, is the protection of the privacy of citizens from governmental intrusion. The desire to protect citizens' privacy from governmental intrusion has deep roots in American law, most notably in the Fourth Amendment's constitutional limitations on the government's ability to conduct unreasonable searches and seizures. The public's perception of the government as the principal threat to personal privacy was refreshed by Watergate and events of the late 1960s and early 1970s, resulting

in new laws, some of which, such as the Privacy Act,[4] also protect information-privacy values by limiting the government's ability to collect and use information about individuals.

The concept of information privacy as a distinct branch of privacy is relatively new, emerging in the late 1960s amidst rising concerns about computers and growing disenchantment with government. Alan Westin's 1967 book, *Privacy and Freedom*,[5] made a seminal contribution to the nation's thinking about information privacy. Later iterations in the US Department of Health, Education and Welfare 1973 Fair Information Practice Report[6] and the 1972 National Academy of Science's Report, *Databanks in a Free Society*, developed a basic code of fair information practice.[7]

The Report of the Privacy Protection Study Commission published in July, 1977, provided further development for the concept of information privacy and its application to specific record-keeping relationships.[8] Five information-privacy strategies enunciated in the Privacy Commission report continue, to this day, to characterize the United States' approach to information privacy law:

- Record-keeping standards should be mostly industry specific, not omnibus.
- The protection of information privacy must depend primarily upon subject participation rights (such as the subject's right of access and correction and the right to bring a civil action for privacy violations).
- Record keepers should retain discretion to set standards for the type and amount of personal information which they collect.
- Record keepers should retain discretion to set standards for the management and use of personal information within their organizations.
- Record subjects should have an expectation that their personal information will be kept confidential—subject to specific expectations appropriate for the record-keeping relationship, the sensitivity of the personal information, and whether the information could be used to make decisions about the indi-

vidual (*i.e.* administrative uses) or is to be used only for non-decision-making purposes, such as marketing or research.

Interests Served by Information Privacy

Protection of information privacy is widely seen as serving at least four interests that are critical to the vitality of democracy:

- an interest in insuring that society (both public and private sectors) makes decisions about individuals in a way that comports with notions of due process and fairness;
- an interest in protecting individual dignity—when individuals endure stigma, embarrassment, and humiliation arising from the uncontrolled use and disclosure of information about them, they lose the sense of dignity and integrity that is essential for effective participation in a free and democratic society;
- an interest in promoting a sense of trust in institutions—when individuals lose the ability to selectively disclose their sensitive personal information, they lose trust in the institutions, both public and private, which collect, hold, use, and disclose this personal information (public-opinion surveys for *Privacy & American Business* indicate that the public's "distrust index," *i.e.* the extent to which the public distrusts the government, is at all-time-high levels of approximately 80 percent); and
- an interest in promoting the viability of relationships that are critical to the effective functioning of a democratic society—numerous relationships, such as the lawyer-client relationship or even the news-media-and-confidential-source relationship, depend upon promises of confidentiality in order to promote the candid sharing of personal information and trust within the relationship.

Concern about Information Privacy Is Persistent and Growing

Why all the attention to privacy? New advances in information technology and, particularly, advances associated with the Internet; new business models reflecting a seemingly ever-

growing "urge to merge"; international privacy developments; an apparently never-ending succession of media reports of "tin ear" business and governmental initiatives aimed at selling government-employee information; "deputizing" financial institutions to watch their customers; creating "Star Trek"-type surveillance systems and databases; and combining data about online and offline behaviors and preferences without adequate notice or permission have all combined to make the public more privacy-conscious than at any time in our history:

- The explosive growth of the Internet is having a profound impact on privacy. What began as a research tool for a small cadre of scientific and academic users has exploded into a mass-communication medium that has caught the imagination of the public, the media, and policymakers. Increasingly, anything impacting on the Internet, including privacy, is a ground for media, and potentially legislative, attention. Privacy concerns in the online environment are receiving particular attention because of the public's high level of concern over privacy, and because the Internet makes it far easier to obtain, collect, and redisseminate personal information. There is a widespread perception that if consumer privacy concerns are not addressed, electronic commerce will falter.
- Corporate restructuring is creating larger, more diverse conglomerates that increasingly use personal information for a wide array of purposes. Mergers, such as that of Citibank and Traveler's Insurance, have created new companies that collect information on consumers in a wide variety of contexts, creating consumer fears that their health, financial, and insurance information will be shared within these new companies in a way that will detrimentally impact their ability to obtain employment, insurance, health care, or other benefits or services.
- The European Data Protection Directive, with its restrictions on the transfer of data to countries outside the EU that lack "adequate" data-protection safeguards, is a driving force behind the growing globalization of information privacy as an issue. The directive has increased the pressure on the

United States to strengthen its privacy laws. The directive and the safe harbor discussions between the EU and the US have generated considerable press coverage, further raising the profile of privacy issues in the United States. In addition, some privacy advocates have argued that the draft safe harbor agreement would result in two sets of privacy protections in the United States, one for information pertaining to citizens of the EU and a second, lower, standard for Americans.

- The media has also fanned the flames of the public's privacy discontent by highlighting privacy practices that reporters find to be questionable. Once these practices become well-known, the ensuing firestorm of public pressure has frequently forced private- and public-sector entities to modify or terminate the offensive practices.
- Business is working to allay consumer privacy concerns through self-regulatory activity. Many individual companies and major industry associations have developed and adopted privacy guidelines. These typically draw on fair-information-practices principles and similar core expressions published over the past 30 years. The industry-association policies call upon the association's members to apply these principles to their particular organizations and operations; and—increasingly—promise to monitor member compliance and take enforcement actions against noncompliers.

Information-Privacy Legal Standards

The United States does not have an omnibus privacy law or a nationwide enforcement mechanism for the protection of privacy interests. The US, however, does embrace a particularly wide array of privacy protections, including:

- Federal constitutional law recognizes a right to privacy in a variety of contexts.
- The common law provides a number of privacy protections including actions for the public disclosure of private facts, actions under the misappropriation theory, and breach of implied contract actions.

- Federal statutory law provides the bulk of federal privacy protections. Specifically, over two dozen federal statutes address privacy concerns in both the public and private sectors. Of those measures regulating the private sector, the Fair Credit Reporting Act represents what is perhaps the most comprehensive approach.
- State law also provides privacy protections which are either independent of, or designed to supplement, federal privacy protections. These measures vary by state, although "uniform state laws" help to bring some degree of uniformity in some areas.
- In addition to legal protections, many other factors provide informal and *de facto* privacy protections. Chief among these factors is the "watchdog" effort of the media and consumer and privacy advocacy groups, as well as numerous self-regulatory efforts by business, including the Online Privacy Alliance, the Individual Reference Services Group, BBB*Online* and TRUSTe.

a. Constitutional Law

It is often emphasized that the federal Constitution does not include an express privacy provision. The Supreme Court, however, has read behavioral and surveillance privacy protections into several of the amendments to the Constitution, including, in particular, the First, Fourth, Fifth, and Ninth Amendments. For example, the Fourth Amendment protects citizens from "unreasonable searches and seizures" and has been interpreted, through an extensive body of case law, to mean that individuals may enjoy a reasonable expectation of privacy from improper governmental searches and seizures.[9] By contrast, the Supreme Court has had relatively little to say about the extent to which, and the way in which, the Constitution provides information privacy protections.

In *Paul v. Davis*,[10] the Court rejected a constitutional claim aimed at a local sheriff who had released the plaintiff's name on a police flier containing the names of individuals who had been arrested (but not convicted). The Court dismissed the constitutional privacy claim, suggesting that constitutional privacy

protections apply only to freedom of action in spheres thought to be private, and not to the government's disclosure of personal information. In *United States v. Miller*,[11] the Court ruled that the Fourth Amendment does not protect the confidentiality of personal information held by institutional record keepers (in that case, a bank).

In *Whalen v. Roe*,[12] however, the Court acknowledged that "the accumulation of vast amounts of personal information in computerized databanks or other massive government files" could constitute an unacceptable invasion of constitutional privacy rights, depending upon the government's purpose and its controls on redisclosure. While the Court upheld the New York statute at issue, which required physicians and pharmacists to report all prescriptions for specified controlled substances to the state, it suggested that there could be circumstances where the Constitution may limit "the unwarranted disclosure of accumulated private data, whether intentional or unintentional or by a system that did not contain comparable security provisions."[13]

Several Supreme Court decisions involving not the Constitution, but federal statutes, suggest that the present Court is sensitive to information-privacy claims and perhaps, when presented with the right case, would be willing to read information-privacy protections more directly and emphatically into the Constitution. In *Reporter's Committee for Freedom of the Press v. Department of Justice*,[14] the Court held that the compilation of public-record information and its automation in a comprehensive, name-accessible database of criminal-history information created a record which, if disclosed under the Freedom of Information Act, would create an unwarranted invasion of personal privacy. A few years later, in 1994, the Court again interpreted statutory privacy provisions to hold that individuals have a "far from insignificant" privacy interest in their home address information.[15]

In 1995, the Supreme Court once again took notice of the importance of privacy in the computer age. In *Arizona v. Evans*,[16] the Court found that the "exclusionary rule" does not require suppression of evidence seized incident to an arrest

resulting from an inaccurate computer record. In a concurring opinion, Justice O'Conner wrote that

> the advent of powerful, computer-based recordkeeping systems…facilitate [*sic*] arrests in ways that have never before been possible. The police…are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.[17]

Justice Ginsburg, in dissent, also expressed concern over the impact of modern technology on privacy:

> Widespread reliance on computers to store and convey information generates, along with manifold benefits, new possibilities of error, due to both computer malfunctions and operator mistakes.…[C]omputerization greatly amplifies an error's effect, and correspondingly intensifies the need for prompt correction; for inaccurate data can infect not only one agency, but the many agencies that share access to the database.[18]

During the 1999-2000 term, the Supreme Court handed down two decisions regarding controls on access to public-record information, which, while not decided on privacy grounds, are likely to encourage stronger privacy initiatives.

The first case, *United Reporting Publishing Corp. v. California Highway Patrol*,[19] arose from a 1996 change in California law governing the release of arrest information[20] to limit the release of arrestee and victim address information to those who certify that the request is made for scholarly, journalistic, political, or governmental purposes, or for investigative purposes by a licensed private investigator. The law specifically prohibits the use of such information "directly or indirectly to sell a product or service to any individual or group of individuals."

United Reporting Publishing Corp., a private publishing service that had been providing arrestee address information to clients under the old statute, filed suit, alleging that the statute was an unconstitutional violation of its First Amendment commercial-speech rights. The 9th Circuit, while finding that arrestees have a substantial privacy interest in the information at issue, nevertheless concluded (as did the district court) that the law was an unconstitutional infringement on United Reporting's First Amendment commercial-speech rights because the "myriad of exceptions…precludes the statute from directly and materially advancing the government's purported privacy interest."[21]

On December 7, 1999, in a decision that was somewhat of a surprise to many in the information industry, the Supreme Court voted seven to two to reverse, reinstating the California statute.[22] In its opinion, the majority characterized this as a case dealing with access to government records rather than restrictions on free speech.[23] The Supreme Court also characterized the case as a challenge to the "facial validity" of the California statute and not a challenge based upon its implementation or actual experience with the statute.[24]

In the second case, *Reno v. Condon*,[25] the Supreme Court unanimously reversed the 4th Circuit Court of Appeals, rejecting a 10th Amendment[26] challenge by the state of South Carolina to the constitutionality of the Driver's Privacy Protection Act of 1994 (DPPA).[27] The DPPA provides that state departments of motor vehicles (DMV) "shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record."[28] The DPPA does contain 14 exceptions pursuant to which states may elect to disclose DMV records in certain instances, such as with the consent of the licensee.[29] Violation of the DPPA may result in criminal fines and a civil cause of action against a person who knowingly violates the statute.[30] While the Court's brief opinion was based on 10th Amendment rather than privacy grounds, the decision potentially opens the door for further federal regulation of access to state records on privacy grounds.[31]

b. Common Law

Common-law information-privacy principles also have an impact on the private sector's handling of personal information. Outright false and malicious statements about an individual, of course, may constitute defamation or slander. Falsity, however, is not the key to common-law privacy protections for personal information. Common-law theories that may be used to protect the privacy of personal information include "public disclosure of private facts," "misappropriation of name or likeness," and a breach of implied contract or fiduciary duty.

Public disclosure of private facts. Where a party publishes or makes widespread disclosure of sensitive personal information without authorization, resulting in harm to the individual, the individual, in most states, will have a cause of action in tort for public disclosure of private facts.[32] According to the Restatement (Second) of Torts, the tort of public disclosure of private facts or "Publicity Given to Private Life" is described as follows:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is a kind that: (a) would be highly offensive to a reasonable person [if disclosed], and (b) is not of legitimate concern to the public.[33]

There are, of course, hurdles. In order to mount a claim of public disclosure of private facts, for instance, a plaintiff must demonstrate widespread disclosure of the private facts. In addition, public-record information (*e.g.* criminal-history records) is usually not considered to be private. On the other hand, private facts would typically include personal health information, financial records, and educational records.

In order for there to be publicity, most courts require "communication of the information to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[34] Some states have adopted

a more relaxed definition, permitting recovery based upon publicity to "a particular public" that has a special relationship to the plaintiff, such as coworkers, family, or neighbors.[35]

This tort may prove to be of particular and growing utility to protect privacy in the Internet environment, where everyone with e-mail capability has the potential to become a "publisher."

Misappropriation. The tort of misappropriation of name or likeness creates a cause of action when an individual's name, portrait, or photograph is used for commercial benefit, without the prior consent of the individual. Although the tort is not available to protect against the use of an individual name on a mailing list, the tort does protect very public uses of a name or likeness in a commercial setting.

Breach of implied contract. When record keepers in confidential and fiduciary relationships disclose personal information without authorization, some courts have provided victims of the disclosure with a cause of action for breach of an implied promise of confidentiality. Both physicians and bankers, for example, have been held liable for unauthorized disclosures of personal information about their patients and customers, based on breach of contract theories.[36]

Indeed, some courts have held that an implied contract of confidentiality between a doctor and a patient arises more or less automatically from the doctor-patient relationship. In a New York case, for example, a psychiatrist who included patient communications *verbatim* in a book without obtaining the patient's consent was found to have breached an implied contract with the patient.[37] Similarly, in *Hammonds v. Aetna Casualty and Surety*,[38] a physician's disclosure of medical information to a hospital insurer was held to constitute a breach of an implied contract between the physician and the patient.[39]

c. Existing Federal Statutory Law

Many existing laws address privacy. Most information-privacy protections are provided by statute and address particular

record-keeping relationships or types of records. Literally dozens of federal laws are in place. Examples include:

- Census Confidentiality (PL 87-813) limits the disclosure of identifiable data except to officers and employees of the Census Bureau, and prohibits the use of census data for purposes other than the purpose for which it has been gathered.
- The Equal Employment Opportunity Act of 1964 (PL 88-352) limits the collection and use of information to discriminate in employment on the basis of categories such as race, sex, religion, and national origin.
- The Freedom of Information Act (FOIA) (PL 90-23) requires that federal-agency records must be made available to the public unless one of the enumerated exemptions applies. The FOIA explicitly exempts from public disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" 5 U.S.C. § 552(b)(6) (1996).
- The Fair Housing Act of 1968 (PL 90-284) limits the collection and use of information to discriminate in housing on the basis of categories such as race, sex, religion, and national origin.
- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (PL 90-351) protects the privacy of wire and oral communications by prohibiting wiretapping and eavesdropping except for surveillance done pursuant to a court order.
- The Postal Reorganization Act of 1970 (PL 91-375) prohibits the opening of an individual's mail, with limited exceptions such as pursuant to a search warrant or the consent of the addressee.
- The Fair Credit Reporting Act of 1970 (PL 91-508) provides the subjects of consumer reports with rights of access and correction, as well as placing substantial restrictions on the disclosure and use of consumer reports.
- The Federal Youth Correction Act (PL 93-415) requires that juvenile records shall be safeguarded from disclosure to unauthorized persons. The act also sets forth the circumstances under which records may be released.

- The Privacy Act of 1974 (PL 93-579) gives individuals a right of access and correction to their personal information held by federal agencies; imposes data-quality standards on federal agencies; and places limits on the collection, use, and disclosure of personally-identifiable information. Under the Privacy Act, information contained in "systems of records" may not be disclosed by federal agencies without the prior written consent of the record subject, except under certain circumstances.[40] Federal agencies must also keep an accounting of records disclosed under the Privacy Act.[41]
- The Family Educational Rights and Privacy Act of 1974 (PL 93-380), sometimes called the Buckley Amendment, requires educational institutions to grant students or parents access to student records and establishes limits on disclosure to third parties.
- The Equal Credit Opportunity Act (PL 93-495) regulates the use of information by creditors in making decisions regarding extensions of credit and requires the retention of certain documents relating to credit transactions. It also requires notice if credit is denied or revoked and guarantees the opportunity for the individual to learn the reason for the denial or revocation.
- The Tax Reform Act of 1976 (PL 94-455) requires notice to taxpayers and an opportunity for taxpayers to challenge information requests before the Internal Revenue Service can obtain certain records. It also strictly limits the disclosure of tax returns and tax-return information by the agency.
- The Fair Debt Collection Practices Act of 1977 (PL 95-109) restricts the communications by debt-collection agencies concerning debtors from whom they are attempting to collect.
- The Right to Financial Privacy Act of 1978 (PL 95-630) provides customers of banks and certain other financial institutions with a right of notice and an opportunity to contest access when federal agencies seek to obtain their financial records.
- The Privacy Protection Act of 1980 (PL 96-440) prohibits government agencies from unannounced searches of press offices and files unless there is a reasonable basis for suspicion that a crime has been committed.

- The Paperwork Reduction Act of 1980 (PL 96-511) prevents federal agencies from collecting information from the public if the Office of Management and Budget does not believe the agency either needs or can make use of the information, or if another agency has already collected the same information. The act also requires agencies to give notice why the information is collected, how it is used, and whether a response by the individual is required.
- The Cable Communications Privacy Act of 1984 (PL 98-549) requires cable companies to inform subscribers about the cable companies' information practices including collection, use, and disclosure, as well as providing subject-access rights.
- The Electronic Communications Privacy Act of 1986 (PL 99-508) extends Title III protections and requirements to digital voice data and video communications, including cellular phones, electronic mail, and computer transmissions.
- The Computer Matching and Privacy Protection Act of 1988 (PL 100-503) requires agencies to formulate procedures before exchanging computerized records for purposes of searching or comparing those records.
- The Employee Polygraph Protection Act of 1988 (PL 100-347) prohibits most private-sector uses of lie-detector tests for employment purposes.
- The Video Privacy Protection Act of 1988 (PL 100-618) prohibits video stores from disclosing their customers' names and addresses and the identification of the video tapes rented or bought by customers, except in certain circumstances.
- The Americans with Disabilities Act of 1990 (PL 101-336) prohibits the collection and use of information to discriminate in employment and accommodation on the basis of a disability.
- The Telemarketing Protection Act of 1991 (PL 102-243) and the Telephone Consumer Privacy Protection Act of 1992 (PL 102-556) restrict telemarketing calls, including those made by autodialers.
- The ADAMHA Reorganization Act of 1992 (PL 102-321) prohibits the unauthorized disclosure of information relating to the

treatment of individuals for alcohol and substance abuse in federally supported facilities.

- The Driver's Privacy Protection Act of 1994 (PL 103-322, as amended by PL 106-69) restricts the disclosure of identification and certain other personal information held by departments of motor vehicles for marketing and other purposes.
- The Telecommunications Reform Act of 1995 (PL 104-104) places restrictions on the disclosure by telecommunications carriers of customer proprietary network information (information about the pattern and use of consumer telephones and other telecommunications equipment, but not the content of calls).
- The Health Insurance Portability and Accountability Act of 1996 (PL 104-191) requires the Secretary of Health and Human Services to issue health-information privacy regulations for transactions electronically transmitted in connection with standard health-care transactions due to congressional failure to enact legislation by August 21, 1999.[42]
- The Taxpayer Browsing Act of 1997 (PL 105-35) prohibits unauthorized browsing through tax-return information by IRS employees.
- The Wireless Telephone Protection Act of 1998 (PL 105-172) prohibits the use of scanners to capture cellular-phone conversations.
- The Children's Online Privacy Protection Act of 1998 (PL 105-208) regulates the collection and use of personal information over the Internet from children under the age of 13.
- The Gramm-Leach-Bliley (Financial Modernization) Act (PL 106-102), enacted in November 1999, requires financial institutions to provide certain privacy protections for consumers' nonpublic personal information and permits consumers to opt out of disclosures of nonpublic personal information to nonaffiliated third parties under certain circumstances.

A closer look at the Fair Credit Reporting Act. Of all of the statutes cited above, the Fair Credit Reporting Act (FCRA), as amended, is one of the earliest and, perhaps, most comprehen-

sive measures regulating the privacy of personal information in the private sector in the United States.[43] The purpose of the FCRA is to promote the accuracy, fairness, and privacy of personal information held and distributed by consumer-reporting agencies.[44] Consumer-reporting agencies are organizations which, for a fee or on a cooperative, nonprofit basis, are in the practice of assembling or evaluating personally-identifiable information obtained from third parties and bearing upon a consumer's credit worthiness, credit standing, credit capacity, character, reputation, personal characteristics, or mode of living.

Under the FCRA, a consumer-reporting agency may only provide a consumer report to a party when the agency has reason to believe that the party will use the report to make a credit determination, an employment determination, an insurance-underwriting determination, or otherwise in connection with a legitimate business need in a transaction involving the consumer or pursuant to written instructions of the consumer. Reports can also be provided in connection with firm offers of credit or insurance.

The FCRA includes all of the safeguards expected in a comprehensive, fair-information-practice/privacy statute, including notice to consumers; choice, including opportunities for opt-in/opt-out; accuracy, relevance, and timeliness standards; confidentiality and use safeguards; security expectations; consumer-access and correction rights; content restrictions; and remedies, including administrative sanctions and private rights of action. More specifically, the FCRA provides consumers with the following privacy rights:

- A consumer must be notified when information in his or her credit file is used to take an action against him or her, such as the denial of a credit application. In such cases, the party denying the benefit must provide the consumer with information on how to contact the consumer-reporting agency that provided the information.
- Consumer-reporting agencies must, upon request, provide a consumer with a copy of that consumer's credit file, as well as

a listing of everyone who has requested it recently. The cost to the consumer of obtaining the report can not exceed $8.50, and may be free if requested in connection with a recent denial of benefits or other specified circumstances.

- Consumers are permitted to request a correction of information they believe to be inaccurate. The consumer-reporting agency must investigate unless the dispute is frivolous. The consumer-reporting agency must send a written investigation report to the individual and a copy of the revised credit report, if changes were made. The consumer may also request that corrected reports be sent to recent recipients. If the dispute is not resolved in the consumer's favor, the consumer has the option of including a brief statement in the consumer's file, typically for distribution with future reports.
- Consumer-reporting agencies must remove from their files, or correct, unverified or inaccurate information typically within 30 days after the consumer disputes the information.
- If a consumer disputes an item with a creditor, the creditor may not forward the disputed information to a consumer-reporting agency without noting that the item is in dispute.
- In most cases, a consumer-reporting agency may not report negative information that is more than seven years old; 10 years for bankruptcies. 1998 amendments to the FCRA would permit the inclusion of criminal-conviction information, without time limitations.
- Covered credit information may only be distributed by consumer-reporting agencies for a recognized need, typically consideration of an application for credit, insurance, employment, housing, or other business. Reports to employers or containing medical information require the consent of the individual.
- Consumers must be permitted to opt out of lists sold by consumer-reporting agencies to firms for unsolicited credit and insurance offers.
- Consumers can sue for violations or seek assistance from the Federal Trade Commission and other federal agencies responsible for the enforcement of the FCRA.

d. Congressional and Executive Branch Activity

Congressional efforts. In a certain sense, the roster of enacted legislation represents only the tip of the congressional privacy iceberg. Over 75 privacy-related bills have already been introduced in the 106th Congress, which would, if enacted, address a broad spectrum of privacy issues ranging from online privacy to health-information privacy to financial-information privacy to public-record privacy. In addition, congressional committees have held numerous hearings on privacy issues to both examine the implications of privacy proposals before Congress as well as to oversee the privacy-related activities of federal departments and agencies.

The most prominent piece of privacy legislation to be enacted so far during the 106th Congress is Title V of the Gramm-Leach-Bliley Act (G-L-B Act). The principal focus of the G-L-B Act is modernization of the nation's banking laws and the elimination of many of the legal barriers that have separated banks, insurers, and securities firms since the Great Depression. The debate over the privacy provisions of the bill was heated and received significant media attention. At one point, representatives of the financial-services industry publicly suggested that the industry would oppose the bill, years in the making, if it contained unacceptable privacy provisions. As enacted, Title V of the G-L-B Act requires that financial institutions take steps to protect the privacy of nonpublic financial information about consumers, including providing notice and an opportunity to opt out of most disclosures of nonpublic personal information to nonaffiliated third parties. The enactment of the G-L-B Act, however, has not ended the debate. The Clinton administration, Senator Richard Shelby (R-AL), and others have already introduced measures to strengthen the privacy protections offered by Title V of the G-L-B Act.

A second privacy-related enactment came from an unlikely source, the Fiscal Year 2000 Transportation Appropriations Act.[45] Section 350 of the Act, sponsored by Senator Shelby, amended the Driver's Privacy Protection Act of 1994 to require that states obtain an opt-in from licensees before disclosing cer-

tain personal information from motor vehicle records, including opt-in requirements for purposes of look up, survey, and marketing. Senator Shelby has included a similar provision in the transportation appropriations bill for fiscal year 2001.

As if all of this congressional activity were not enough to underscore the increased importance and attention that privacy issues are receiving from Congress, on February 9, 2000, Senate Minority Leader Daschle (D-SD) announced the formation of the Senate Democratic Privacy Task Force, which will be headed by Senator Patrick Leahy (D-VT), to educate consumers and to work with industry, consumer groups, and the administration to address ways in which the privacy of Americans' medical records, financial records, records of Internet activity, as well as other personal information, can be protected. The very next day, Senator Shelby, Senator Richard Bryan (D-NV), Rep. Ed Markey (D-MA), and Rep. Joe Barton (R-TX) held a news conference to announce the formation of the bipartisan, bicameral Congressional Privacy Caucus (CPC).[46] The purpose of the CPC is threefold: 1) educate members of Congress and staff about individual-privacy issues; 2) provide a forum for the discussion of individual-privacy issues; and 3) advocate for personal-privacy protections.

Clinton administration privacy efforts. The Clinton administration has been active in addressing privacy issues, supporting a variety a self-regulatory and legislative initiatives to provide increased privacy protections. In 1999, President Clinton named Ohio State University Professor Peter Swire to be the first Privacy Counselor to the President to coordinate the administration's position on privacy issues.

The president and the vice president have both spoken out on privacy issues. The president, for example, included remarks about consumers' financial privacy in his final State of the Union address. Specifically, the president stated that citizens' privacy must be safeguarded and, with respect to financial privacy, referred to the G-L-B Act: "[W]e've taken the first steps to protect the privacy of bank and credit-card records and other

financial statements." The president also stated that he plans to send legislation to Congress adding to those protections. The president also mentioned medical-record privacy during the address, as he had the year before, stating that the administration would finalize health-information privacy regulations this year.

The vice president has also spoken on privacy issues, calling for Congress to enact comprehensive legislation to protect medical records. In addition, the vice president has called for an "electronic bill of rights" to protect personal information in the electronic age. One component of the administration's effort is a presidential memorandum ordering federal departments and agencies to review their information practices, ensuring "that new technologies do not erode Privacy Act protections while also examining how new technologies can be used to enhance personal privacy."[47] Other aspects of the plan include a web site, administered by the Federal Trade Commission (FTC), where individuals can opt out from various types of mailing lists.

The federal departments and agencies have also devoted considerable resources to the information-privacy issue, with the FTC taking an increasingly active role in a wide range of privacy issues.

The FTC has entered into privacy-related consent decrees with numerous companies in the credit-reporting industry. In addition, the FTC is currently engaged in litigation with TransUnion, one of the major credit-reporting systems. In the TransUnion case, the United States Court of Appeals for the District of Columbia reversed a Federal Trade Commission ruling that TransUnion's practice of using identification and tradeline information from a credit report to create mailing lists for direct marketing violated the FCRA. The Court of Appeals remanded the case to the FTC for certain factual findings. On March 1, 2000, the FTC issued an opinion holding that TransUnion violated the FCRA by selling tradeline information for target-marketing purposes.[48]

The FCRA is only one of many weapons at the FTC's disposal for addressing privacy issues. The agency is charged with enforcing the Children's Online Privacy Protection Act and has

taken a broad interest in privacy on the Internet, including online profiling issues. In addition, the FTC is one of over a half-dozen federal agencies with enforcement authority over the financial-privacy protections in Title V of the G-L-B Act.

The FTC also asserts authority under Section Five of the FTC Act, which prohibits unfair and deceptive trade practices, to prohibit companies from using personal information in ways that the agency believes to be unfair or deceptive. During the summer of 1998, the FTC successfully settled an action against web host GeoCities for allegedly violating Section Five by misleading customers as to GeoCities' handling of the personal information of its customers. The FTC has also launched an investigation of DoubleClick to determine if the online company's data practices constitute deceptive trade practices. Looking toward the future, the FTC's Section Five authority will be an essential enforcement mechanism for any safe harbor agreement between the EU and the United States (discussed below).

The Department of Commerce, which has been coordinating many of the Clinton administration's self-regulatory privacy initiatives, issued a draft "Elements" paper in January, 1998, setting forth the department's views on the necessary elements of a self-regulatory privacy-protection program.[49] Drawing upon long-standing fair-information-practice principles, the department believes that, in order to be effective, self-regulatory programs must address the following areas: awareness, including privacy policies, notification provisions, and consumer education; consumer choice with respect to "whether and how their personal information is used"; data security; and consumer access to information that companies hold about that individual.[50]

In addition, the department emphasizes that in order for any self-regulatory regime to be effective, it must also include adequate enforcement provisions, including components such as readily-available and cost-effective means for consumer recourse for the resolution of complaints; verification procedures to ensure that company practices comply with the company's stated privacy policies; and meaningful consequences for companies that fail to comply with the self-regulatory principles.[51]

The Department of Commerce has also spearheaded negotiations with the EU over the creation of a safe harbor mechanism to permit the continued flow of personal data from the European Union to the US in compliance with the data protection directive. The Safe Harbor Principles, which were formally approved by the European Commission in July, 2000, include seven principles: notice, choice, onward transfer, security, data integrity, access, and enforcement. In addition, the Principles are accompanied by fifteen sets of "Frequently Asked Questions" (FAQs) which provide additional detail with respect to: sensitive data; journalistic exceptions; secondary liability; investment banking and audits; the role of data-protection authorities; self-certification; verification; access; human-resources data; Article 17 contracts; dispute resolution and enforcement; choice (timing of opt-out); travel information; pharmaceutical and medical products; and public-record and publicly-available information. Financial services are not covered by the safe harbor agreement, however the issue is to be revisited once the G-L-B Act has been implemented.

The Department of Health and Human Services (HHS) has also been active on privacy issues, supporting federal legislation to protect health-information privacy (no such legislation has yet been enacted, despite a self-imposed congressional deadline of August 21, 1999). In the absence of legislation, HHS has relied on statutory authority under the Health Insurance Portability and Accountability Act of 1996 to issue proposed health-information privacy regulations. The public-comment period ended on February 17, 2000. Public response to the proposed regulations was overwhelming—over 50,000 comments, many of them critical of the proposed regulation. The Health Subcommittee of the House Ways and Means Committee held a hearing on February 17 about medical-record confidentiality and, in particular, the impact of the proposed HHS medical-record privacy regulations on Medicare as well as on private-sector health care. At that hearing, Margaret Hamburg, HHS Assistant Secretary for Planning and Evaluation, said that finalizing the rule will take a while due to the high volume of comments. It is anticipated, however, that the rule will be finalized before the end of the year.

e. State Statutory Law

In addition to privacy protections found in federal law, law in each of the 50 states also provides a myriad of statutory privacy protections to individuals. The scope of these protections vary from state to state, as is often the case in our federal system. The wide variety of state legislation makes a detailed review impossible in a paper of this size, however some broad observations are possible.

First, over one dozen state constitutions contain language protecting personal privacy rights.[52] These privacy protections take a variety of forms, but tend to mirror federal Fourth Amendment language protecting surveillance-privacy interests. Some states offer additional privacy protections. California's constitutional privacy-protection language, for example, found in Article I, Section 1, explicitly protects individual privacy as an "inalienable right." This language has been interpreted to apply not only to governmental agencies but also to private actors.[53]

Second, states frequently seek to provide additional protections in areas where there is already some level of federal protection, which is permissible provided that the federal law does not preempt state action and the state law is consistent with the federal statute. Over one-third of the states, for example, have enacted their own laws supplementing and further regulating the use of consumer-report information. In addition, many states are currently considering proposals to supplement the privacy provisions of the G-L-B Act.

Third, states often seek to regulate the use of personal information by state and local governments. Over one-third of the states have enacted their own "mini" privacy acts regulating the collection, maintenance, use, and disclosure of personal information by state and local government agencies. States also have adopted numerous more-narrowly-drawn statutes which extend confidentiality protections to particular information, such as information collected by the state for public-health reporting.

Fourth, while state privacy protections are frequently uneven, greater interstate uniformity exists in some areas where "model statutes" have been adopted. Almost 20 states, for example, have

enacted the National Association of Insurance Commissioners (NAIC) uniform state law regulating the use of personal information by insurance companies and insurance-support organizations. In September, 1998, the NAIC unveiled a model statute for regulating the use health information by insurance companies and their support organizations. In addition, the National Conference of Commissioners on Uniform State Law is drafting a new health-information-privacy model law to replace the model it proposed in the 1980s, which was adopted in only three states. While states typically make some changes to these model statutes, the resulting statutes contain a high degree of uniformity.

Fifth, states stand ready to legislate in a wide array of areas to provide privacy protections. Several states have adopted statutes that regulate employers' use of personal information for employment purposes. Many states regulate the use of Social Security numbers; tax records; computer records; credit reporting and investigation; employment records; medical records; cable and video records; bank records; school records; electronic communications; polygraph testing; and arrest and conviction records. In recent years, the states have been very active in considering legislation to regulate genetic-record information and information obtained through, or generated over, the Internet or other online networks.[54]

State activity on privacy is not confined to the state legislatures. Governors and other state officials, particularly state attorneys general, have been increasingly active on privacy issues. The National Association of Attorneys General, for example, has devoted a considerable amount of time and attention to privacy issues in recent months. In addition, individual attorneys general, including those in Washington, Michigan, Minnesota, and New York, have filed a number of privacy-related legal actions and launched privacy initiatives in their states.

Nonlegal Sources of Privacy Protections

In addition to federal and state legal protections, the privacy of individual information is also protected by nonlegal means

including media scrutiny and public opinion, as well as self-regulatory efforts undertaken by the private sector. Privacy issues are frequently the subject of intense media and legislative scrutiny in the United States. The issue is marked by frequent crises and confrontations involving close broadcast and print media coverage, hostile and frequent Internet postings, legislative hearings, and, occasionally, court battles.

In February, 1998, for example, *The Washington Post* reported that two pharmacy chains, CVS and Giant, used, or planned to use, an outside contractor to send prescription-refill notices and drug promotions, using prescription information supplied by the pharmacies.[55] Both companies took out full-page advertisements announcing the cancellation of the programs amid a flurry of editorial criticism and customer complaints.[56] CVS has since been sued,[57] with the plaintiff alleging that CVS breached its fiduciary duty as well as its duty of confidentiality to its pharmacy customers.[58]

Washington Post stories signaled the start of another privacy firestorm in January, 1999, when the *Post* reported that Image Data, a small New Hampshire company, had developed a product designed to combat check and credit-card fraud and identity theft using state DMV photographs. Under the Image Data plan, the company entered into contracts with several states, whereby Image Data was permitted to digitize DMV photographs of individuals and store the photographs in a database. Merchants could then access this database, using a small screen installed near the cash register, when a customer presented a check or credit card for payment, in order to assist the merchant in verifying the identity of the purchaser.

Image Data had entered into agreements with South Carolina, Colorado, and Florida to obtain driver's license photos and other information, and was testing its program in South Carolina when the project was featured in a *Washington Post* article on January 22. A public outcry ensued, with state officials receiving a torrent of angry calls protesting the plan (and a class-action lawsuit in Florida). Public ire appears to have been a product of several factors. As one South Carolina woman described it:

> We were livid [upon hearing about the Image Data program]. In my opinion, a South Carolina driver's license is a need, not a want. We have no choice but to give our information in order to have one. Then they turn around and sell it to a company, as personal as it is: my weight, my height, my address—my God, my image. There are endless possibilities as to what could be done with it.

As a result of the public outcry that has ensued, all three states have ended the transfer of photos to Image Data and sought to retrieve any photos already transferred.

A third example is the case of Internet advertising-giant DoubleClick. During its four-year life, DoubleClick collected click-stream information from its participating web sites and then used that data to help those web sites customize the banner ads and pop-up ads that visitors see. DoubleClick could not identify the visitor, only the visitor's computer. The privacy firestorm began in November, 1999, when DoubleClick spent $1.7 billion to purchase Abacus Direct, the largest database of consumer catalogue activity. DoubleClick's plan, brilliant from a marketing perspective, was to marry its click-stream data with Abacus' offline data to identify specific consumers (not just their computers) and then create a profile of the consumers' interests and buying activity.

This plan produced a firestorm of criticism in the media, from privacy advocates and from consumers. Finally, on March 2, 2000, DoubleClick announced that it would not go forward with its plan to build personal profiles. Pressure to abandon the plan was intense; not only did DoubleClick receive a torrent of adverse media coverage, it also received over 100,000 consumer complaints in response to an online protest organized by the Center for Democracy and Technology. The FTC, as well as the Michigan, Connecticut, New York, and Vermont attorneys general, announced an investigation of DoubleClick's activities and several class-action lawsuits were filed. In addition, shortly before DoubleClick made its announcement, Internet-industry players such as search engine AltaVista Co. and Internet home-

delivery service Kozmo.com Inc. took steps to distance themselves from DoubleClick. If that had not been enough, the company's stock price fell by more than 25 percent during the firestorm (it rebounded somewhat following the March 2 announcement).[59]

Public concerns about privacy are having an undeniable impact on corporate policy and practice as more and more industries and companies seek to self-regulate through industry standards and company privacy codes. Prominent examples of collective self-regulatory initiatives include efforts by the Individual Reference Services Group, the Direct Marketing Association, and the Online Privacy Alliance. In addition to cooperative efforts, many individual companies have also adopted their own privacy policies and codes. These policies reflect the growing importance the business community places on the privacy of personal information.[60]

Technology-based, nongovernmental solutions are another nonlegal source of protection for personal information. BBB*Online*, TRUSTe, and others have developed online privacy-seal programs, whereby companies who meet established privacy standards can affix the online seal to their Internet site to promote public confidence in the site's privacy practices. Other technology-based programs for the protection of privacy include: the Platform for Privacy Preferences (P3) advocated by the Center for Democracy and Technology and the Internet Privacy Working Group, which would permit users of Internet browsers to program the browsers to block sites that do not meet an individual's privacy needs; the Platform for Internet Content Selection (PICS), which is sponsored by the World Wide Web Consortium at MIT, and serves as a content-rating system and may be expanded to function as a privacy-rating system as well; and the Open Profiling Standard (OPS) sponsored by companies including Netscape, IBM, American Express, and Hewlett Packard, among others, which would protect Internet-user privacy by permitting the user to block personal information that is typically sent to a web site by a user's computer.

TRENDS

While there is an incredible amount happening on privacy right now, a few trends that are likely to play out over the next few years can be identified:

- Public concern over privacy is likely to remain high. Technology is the moon that is pulling up the privacy tide. Until the public becomes accustomed to, and comfortable with, the new information technologies, and a consensus on privacy acceptable-practices develops, the public is likely to remain intensely concerned about risks to personal privacy.
- Privacy is a bipartisan issue. Nobody in the business community should have any illusion that the Republicans will be necessarily more sensitive to the importance of using personal information to drive down costs, deliver services, improve products, and improve public safety. The bipartisan nature of the issue was again highlighted in February, 2000, with the formation of a bipartisan Congressional Privacy Caucus. With public concern over privacy at such high levels, the bipartisan approach to this issue is likely to continue.
- Legislative activity is likely to continue almost unabated. With public-opinion surveys showing overwhelming public concern and the media fanning the flames by highlighting business practices, a continuing high level of legislative activity is almost a certainty.
- The traditional US approach of selective privacy regulation is eroding. There is increasingly-widespread adoption of privacy programs like the Online Privacy Alliance principles, that are comprehensive "one-size-fits-all" measures. There is also an increasing trend toward omnibus government solutions. While the draft safe harbor proposal is something of a hybrid between the traditional selective approach and the omnibus approach,[61] omnibus proposals or privacy packages are increasingly being introduced in state legislatures, including those of New York, California, Massachusetts, Hawaii, and Minnesota.
- Opt-out versus opt-in and affiliate sharing will be key issues. The debate over the G-L-B Act and Senator Shelby's amend-

ments to the DPPA illustrate the contentious role that the opt-out/opt-in debate is likely to play in future congressional and state debates over privacy legislation. If business is to prevail on the issue, it will be necessary to demonstrate two things: opt-out really does work to protect privacy, and opt-in is an economic deflator. Title V also demonstrated the sensitivity surrounding affiliate sharing, an issue of growing concern to the public because of mergers of companies, such as the financial-services firms, that hold a wide range of personal data about them.

CONCLUSION

Information-privacy protections in the United States are strong and rapidly growing stronger. United States' protections for information privacy, however, cannot be measured simply by reference to a single omnibus law or by reference to the work of a single agency. To the contrary, the scope and substance of US information-privacy law are measured by reference to a wide array of sources of law and types of law, as well as self-regulatory measures.

Such law can be found in numerous state statutes which provide privacy and fair-information-practice-type protections for specific types of records or specific types of record-keeping relationships. Such law can also be found in dozens of federal statutes which provide notice, choice, access, data quality, and confidentiality protections for specific types of records or specific types of record keepers. In addition, the measure of US law can be taken from an important body of constitutional and common-law jurisprudence. Finally, US information-privacy law is embodied in hundreds of state- and federal-agency regulations and administrative rulings.

Moreover, as a practical matter, much of the information-privacy protection in the United States does not even lie in law but, rather, is found in an array of self-regulatory mechanisms. These mechanisms include umbrella, cross-sectional privacy codes aimed mostly at e-commerce including, in particular, the Online Privacy Alliance standards. These mechanisms are found

in emerging privacy-seal and verification programs such as TRUSTe and BBB*Online*. These mechanisms are also found in countless industry and company codes. Finally, but not to be overlooked, the robustness of the self-regulatory approach is sustained by an ever vigilant privacy-advocacy community and by the threat and reality of close media scrutiny.

Notes

[1] During the winter of 1999, the public deluged federal financial agencies with over 250,000 comments, mostly negative, regarding a proposed regulation that would have required banks to monitor customer transactions for suspicious activity; this year the Department of Health and Human Services reports receiving over 50,000 comments on its proposed health-information privacy rule.

[2] IBM Multi-National Consumer Privacy Survey (October 1999) available at http://www.ibm.com/services/e-business/priwkshop.html.

[3] In *Whalen v. Roe*, 429 U.S. 589, 599, 600 (1977), the Supreme Court discussed the various clusters of interests protected by the broad term "privacy."

[4] 5 U.S.C. § 552a.

[5] Atheneum (1967).

[6] *Records, Computers and the Rights of Citizens*, MIT Press (1973).

[7] Westin and Baker, Quadrangle (1972). See also Belair, "Information Privacy: A Legal and Policy Analysis" in *Science, Technology and Uses of Information*, National Science Foundation (1986).

[8] *Personal Privacy in an Information Society*, GPO (1977).

[9] See *e.g., Katz v. United States*, 389 U.S. 347 (1967), holding that electronic eavesdropping by the government constituted a search and seizure and therefore must meet Fourth Amendment requirements.

[10] 426 U.S. 693 (1976).

[11] 425 U.S. 435 (1976).

[12] 429 U.S. 589, 605 (1977).

[13] In a subsequent information-privacy decision, *United States v. Westinghouse Electric Corp.*, 638 F.2d 570 (3rd Cir. 1980), the 3rd Circuit set out seven factors to consider when determining whether governmental information-collection practices infringe upon individual privacy. "The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the

degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access."

[14] 489 U.S. 749, 762 (1989).

[15] *U.S. Department of Defense v. Federal Labor Relations Authority*, No. 92-1223, February 23, 1994.

[16] 514 U.S. 1 (1995).

[17] Ibid. at 17-18 (O'Connor, J., concurring).

[18] Ibid. at 26 (Ginsburg, J., dissenting).

[19] *Los Angeles Police Department v. United Reporting Publishing Corp.*, 528 U.S. 32, 120 S.Ct. 483 (1999).

[20] Cal. Gov. Code § 6254(f).

[21] *United Reporting*, 146 F.3d 1140 (9th Cir. 1998).

[22] *Los Angeles Police Department v. United Reporting Publishing Corp*.

[23] The Court's decision did not address the commercial-speech interests at issue in the regulation of the use of personal information in private records, an issue which also has drawn the attention of the Appellate Courts. The 10th Circuit Court of Appeals, for example, acted on First Amendment commercial-speech grounds to vacate a rule issued by the Federal Communications Commission which required consumers to opt in to most disclosures of their consumer proprietary network information (CPNI). *U.S. West, Inc. v. Federal Communications Commission*, 182 F.3d 1224 (10th Cir. 1999). cert. denied sub. nom. *Competition Policy Institute v. U.S. West*, ___U.S.___, 120 S. Ct. 2215 (2000). CPNI is information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, including most information contained in telephone bills, which is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. See 47 U.S.C. § 222(f)(1)(A)-(B).

[24] In a related development, on December 13, 1999, the Supreme Court issued an order in *McClure v. Amelkin*, 120 S. Ct. 630 (1999) (Order no. 99-200), setting aside a decision by the 6th Circuit Court of Appeals which struck down a Kentucky law limiting access to motor vehicle accident reports. The 6th Circuit struck down the law—which allows access to accident victims, victims' lawyers, victims' insurers, and the news media (but not for commercial purposes)—after finding that the law violates commercial free-speech rights. The Supreme Court sent the case back to the 6th Circuit and ordered the lower court to restudy the case, taking into consideration the Supreme Court's decision in *United Reporting*.

[25] ___ U.S. ____, 120 S. Ct. 483 (2000). The 4th Circuit case was the first of four decisions issued by the Courts of Appeals on the constitutionality of the DPPA; two decisions upheld the constitutionality of the DPPA, two held it to be unconstitutional. See *Condon v. Reno*, 155 F.3d 453 (4th Cir. 1998) (holding DPPA is unconstitutional); *Pryor v. Reno*, 171 F.3d 1281 (11th Cir. 1999)

(holding DPPA is unconstitutional); *Travis v. Reno*, 160 F.3d. 1000 (7th Cir. 1998) (upholding DPPA); *Oklahoma v. United States*, 161 F.3d 1266 (10th Cir. 1998) (upholding DPPA). The DPPA also has been challenged on First Amendment grounds; however, discussions of First Amendment challenges are omitted here. See *e.g., Travis v. Reno*; *Oklahoma v. United States.*

[26] "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." US Constitution, Amendment X.

[27] 18 U.S.C. § 2721 et. seq.

[28] 18 U.S.C. § 2721(a).

[29] 18 U.S.C. § 2721(b).

[30] 18 U.S.C. §§ 2723(a) & 2724(a).

[31] The Court concluded that "the DPPA does not require States in their sovereign capacity to regulate their own citizens. The DPPA regulates the States as the owners of databases. It does not require the South Carolina Legislature to enact any laws or regulations, and it does not require state officials to assist in the enforcement of federal statutes regulating private individuals. We accordingly conclude that the DPPA is consistent with the constitutional principles enunciated in [*New York v. United States* and *United States v. Printz*.]" *Reno v. Condon*, 120 S. Ct 666, 672. In addition, the Court disagreed with the 4th Circuit's holding that the DPPA exclusively regulated the states, finding instead that the "DPPA regulates the universe of entities that participate as suppliers to the market for motor vehicle information—the States as initial suppliers of the information in interstate commerce and private resellers or redisclosers of that information in commerce." Ibid. As a result, the Court did not address the "question whether general applicability is a constitutional requirement for federal regulation of the States."

[32] For the most part, this "common law" privacy tort has a statutory grounding. See Trubow, *Privacy Law & Practice* (Matthew Bender, 1991) at Section 1.05 and the cases cited therein.

[33] *Restatement (Second) of Torts* § 652D (1977).

[34] *Privacy Law & Practice* at 692 (quoting *Restatement (Second) of Torts* §652D cmt. A; internal quotation omitted).

[35] *Doe v. Methodist Hospital*, 690 N.E.2d 681,692 (Ind. 1997).

[36] See *Hammonds v. Aetna Casualty and Surety Co.*, 243 F.Supp. 793 (N.D. Ohio 1965); *Milohnick v. First National Bank of Miami Springs*, 224 So.2d 759 (Fla. Ct. of Apps. 1969).

[37] *Doe v. Roe*, 400 N.Y.S.2d 668, 674 (N.Y. Sup. Ct. 1977) ("implied covenant of secrecy").

[38] 237 F.Supp. 96 (N.D. Ohio 1965).

[39] See *Office of Technology Assessment, Protecting Privacy in Computerized Medical Information*, 43 (1993).

[40] 5 U.S.C. § 552a(b) (1996).

[41] 5 U.S.C. § 552a (1996).

[42] See 64 Fed. Reg. 59917 et. seq., November 3, 1999, as amended by 65 Fed. Reg. 427, January 5, 2000.
[43] 15 U.S.C.A. § 1681 et. seq.
[44] See a summary of a consumer's rights under the FCRA in the FTC's model notice for distribution to consumers. 16 C.F.R. Part 601, Appendix A (1998).
[45] Pub. L. No. 106-69.
[46] The CPC supports the following four privacy principles:

1. Notice. Whenever private companies or government agencies plan to collect, use, and/or disclose personally-identifiable information, they must notify individuals in a clear and conspicuous manner. Individuals must also be notified about the intended recipient of personally-identifiable information and the purpose for which the information will be used.
2. Access and Correction. Individuals must have access to personally-identifiable information about themselves maintained by private companies and governmental agencies in order to review the information for accuracy, timeliness, and completeness. Individuals must also have the opportunity to correct inaccurate information.
3. Consent. Private companies and government agencies must obtain individuals' affirmative consent before using and/or disclosing the individual's information for a purpose other than that for which the information was originally provided.
4. Preemption. In order to provide individuals with the strongest possible privacy protections, federal law must not preempt stronger state privacy protections.

[47] Press Release, "Vice President Gore Announces New Comprehensive Privacy Action Plan for the 21st Century," Office of the Vice President, May 14, 1998.
[48] *In re Trans Union*, available at www.ftc.gov/os/2000/03/index.htm The FTC also held, for the first time, that age data is a consumer report when used or expected to be used for an FCRA-permissible purpose.
[49] Department of Commerce, "Elements of Effective Self-Regulation for Protection of Privacy," discussion draft (January 1998).
[50] Ibid. at 1-2.
[51] Ibid. at 2.
[52] Fred H. Cate, *Privacy in the Information Age* (1997) at 66-68.
[53] Ibid. at 67. See *Urbaniak v. Newton*, 156 Cal. Rptr. 55 (Cal. Ct. App. 1979); *Division of Medical Quality v. Gherardini*, 277 Cal. Rptr. 354 (Cal. Ct. App. 1991). See also Paul M. Schwartz, "The Protection of Privacy in Health Care Reform," 48 *Vanderbilt Law Review* 295, 320-321.
[54] See "Privacy Legislation in the States 1999 Trends," *Privacy and American Business*, Alan Westin & Robert Belair, eds. (September/October 1999).
[55] Robert O'Harrow, Jr., "Prescription Sales, Privacy Fears: CVS, Giant Share Customer Records With Drug Marketing Firm," *Washington Post*, February 15, 1998.

[56] Robert O'Harrow, Jr., "Giant Stops Sharing Customer Data: Prescription-Marketing Plan Drew Complaints," *Washington Post*, February 18, 1998; Robert O'Harrow, Jr., "CVS Also Cuts Ties to Marketing Service," *Washington Post*, February 19, 1998.
[57] *Weld v. CVS*, (Mass. Superior Ct. Suffolk) No. 98-0897 (1998).
[58] "Class-Action Suit Targets CVS Over Use of Prescription Data," *Privacy Times*, Evan Hendricks, ed., April 3, 1998, at 1-2.
[59] "DoubleClick Cries 'Uncle' …Sam (Sort of)," *Privacy Times*, March 3, 2000, at 5-6. See also *Bloomberg News*, "DoubleClick in Settlement Discussions," CNET News, March 23, 2000, at http://aolcom.cnet.com/news/0-1005-200-1582990.html.
[60] See generally *Privacy & American Business, Handbook of Business Privacy Policies and Codes Volume 4* (1997).
[61] The draft Safe Harbor Principles are omnibus, while the accompanying Frequently Asked Questions are often selective in their approach.