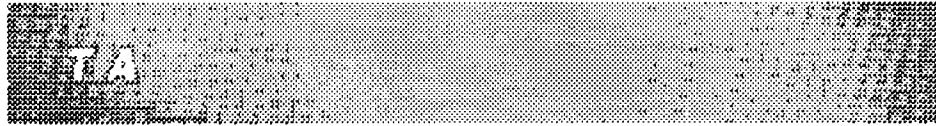




[[Yahoo](#) | [Write Us](#) | [Search](#) | [Headlines](#) | [Info](#)]

[[Business](#) - [Company](#) - [Industry](#) - [Finance](#) - [PR Newswire](#) - [Business Wire](#) - [Quotes](#)]



Thursday July 10 6:01 AM EDT

Company Press Release

New Interactive Trends Revealed at Industry Summit

WASHINGTON--(BUSINESS WIRE)--July 10, 1997--How will the Internet reshape consumer behavior and global commerce?

What breakthrough technology will drive interactive services? Can we protect consumers and businesses from online scams and smut? Can policymakers cope with the pace of cyber change?

Top national policymakers and business leaders will reveal the defining trends, vision and street-level solutions at one of America's premier interactive services forums -- the 12th annual conference of the Interactive Services Association (ISA), July 27-30 at the Sheraton Washington Hotel, in Washington (check out full program at www.isa.net).

Among the ISA's keynote speakers:

-- Steve Case, Chairman & CEO of America Online (9am, Monday, July 28);

- ☐ Ira Magaziner, lead White House interactive policy adviser
- ☐ (8:45 am, Monday, July 28);
- ☐ U.S. Rep. Edward Markey (D-MA), ranking Democrat on

Telecommunications, Trade & Consumer Protection Subcommittee

(noon-2 pm, Tuesday, July 29).

Among the 90-plus speakers and 14 panel sessions:

- ☐ Interactive Gaming: Who Wins? -- Online gaming is one of the most-lucrative and rapidly expanding areas of the Internet. What gaming programs are succeeding? Why? How are they

being marketed? How do we protect against abuse? Panelists: Sue Schneider (RIG Online); Kendell Lang (Casino World Holdings); Jenny Solursh (Cryptologic); Alex Igelman (Gaming Lottery Corporation).

- Investment Update: Where Is the Best Value? -- What Internet firms are the hottest investment targets? Why? What will the investment climate look like in 1998? Panelists: Paul Noglows (Hambrecht & Quist LLC); Ann Winblad (Hummer Winblad Venture Partners); Lise J. Buyer (T. Rowe Price Associates); Steve O'Leary (Broadview Associates LLC); Doug Stern (Scripps Ventures).
- Seedy Side of the Internet -- Consumer fraud, marketing sleaze to children, online harassment and business scams: How do we clamp down on seedy and even dangerous Internet practices? Can the private sector work it out? Are watchdogs watching closely enough? Should government play a heavier hand? Panelists: Glee Harrah Cady (NETCOM On-Line); Linda Golodner (National Consumers League); Martha Landesburg (Federal Trade Commission).
- Interactive TV: Dead or Alive? -- Does interactive TV have a future? Some think so, some don't. How high is consumer demand? What platforms are most popular? Where are the success stories? Panelists: Jack Galmiche and Fred Ciccone (Broadcast Interactive Group); Bob Regan (GTE Mainstreet); Maryann Schulze (Tribune Co.); Bob Mariano (COMSPAN); Eric Dentler (Thomson Sun Interactive).

Related News Event: A related forum on Internet domain names will be held July 30-31 at the Sheraton Washington Hotel. Internationally known experts will discuss issues such as... domain name reform and controversies... trademarks... role of government and private sector in domain name management.

The forum is sponsored by ISA, Center for Democracy and Technology, and International Technology Association of America. Contact Brian O'Shaughnessey (301/495-4955).

About the ISA -- Headquartered in Silver Spring, Md., the Interactive Services Association represents more than 300 companies that deliver online interactive services. The ISA is the nation's leading association focusing solely on providing consumer interactive services worldwide.

Contact:

Interactive Services Association
James Quiggle, director of Media Relations;
jimisa@aol.com
or
Patti McKnight, director of Conferences; pattimk@aol.com
301/495-4955

-
- *More news for related industries:* [computer](#), [internet](#), [telecommunications](#).

- *Additional news and quotes:*

GLCCF	Gaming Lottery Corp
TRB	Tribune Co

[Help](#)

Copyright © 1997 Business Wire. All rights reserved. All the news releases provided by [Business Wire](#) are copyrighted. Any

In 1972, the Secretary of the Department of Health, Education, and Welfare appointed a federal advisory committee to examine the growth of automated record keeping in the United States. The federal Advisory Committee on Automated Personal Data Systems (the Advisory Committee) concluded that an individual should have a right "to participate in a meaningful way in decisions about what goes in records about him and how that information shall be used."⁽¹⁾ The Advisory Committee first identified certain "fundamental principles" applicable to the recording, disclosure, and use of identifiable personal information. Agreed upon procedures for ensuring an individual's right to participate -- called "fair information practices," were derived from these fundamental principles.⁽²⁾ Subsequently, Congress created the Privacy Protection Study Commission to analyze and make recommendations for reform of information practices in the public and private sector.⁽³⁾

Other nations confronted similar issues during this period, and, in 1981, the Organization for Economic Cooperation and Development (OECD) issued Guidelines for the protection of Privacy and Transborder Flows of Personal Data (the OECD Guidelines),⁽⁴⁾ a voluntary, international standard of conduct applicable to personal data generally. The OECD Guidelines reflect the international consensus that existed about information privacy on the eve of the personal computer revolution, setting out eight basic privacy principles that remain applicable to data collection today: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.⁽⁵⁾ The U.S. government has endorsed these guidelines as have a number of U.S. businesses.

Rapid advances in computer technology, coupled with the integration of telecommunications and data processing, occurred in the years following the Advisory Committee report, the Privacy Commission report, and the promulgation of the OECD Guidelines. These advances dramatically altered the way information about individuals is obtained and used by the government and private industry. In the United States, commentators continued to express concern about the federal government's accumulation and use of data. By 1990, according to General Accounting Office reports, computers and advanced technologies, such as computer networking, were used widely throughout the federal government.⁽⁶⁾ Federal agencies both obtained information from and shared information with third parties, including state and local agencies and the private sector.⁽⁷⁾

2. The IITF Privacy Principles

In 1993, Vice President Gore established the Information Infrastructure Task Force (IITF) to articulate and implement the Administration's vision for the National Information Infrastructure (NII). The Task Force's Information Policy Committee (IPC) created a Privacy Working Group (PWG) to consider the ways in which the NII might affect individual privacy. The PWG issued the Principles for Providing and Using Personal Information (Privacy Principles) in 1995,⁽⁸⁾ to articulate the elements of fair information practices needed to ensure continued development of the NII. The Privacy Principles are the starting point for this Options Paper. The goal of this Options Paper is to frame the debate needed to identify the best approach to promoting privacy on the NII based on those Privacy Principles.

The Privacy Principles are designed to apply to the collection and use of information by both government and industry. They are based on existing international articulations of fair information practices in order to provide a common vocabulary for resolution of international conflicts involving data use.

The Privacy Principles reflect a recognition that the nature of the electronic medium itself must shape development of a workable privacy policy. Specifically:

- (1) consumers, government, and businesses have a shared responsibility for the fair and secure use of personal information;
- (2) the technology of the NII has the potential, as yet unexploited, to empower individuals to take steps to protect their personal information;
- (3) openness about, and accountability for, the process of collecting and using personal information is crucial on the NII; but,
- (4) openness and accountability will not be meaningful until consumers become educated about the ways in which their personal information is being used in cyberspace, and by whom.

The Privacy Principles identify three values to govern the way in which personal information is acquired, disclosed and used online - information privacy, information integrity, and information quality.

First, an individual's reasonable expectation of privacy regarding access to, and use of, his or her personal information should be assured. Second, personal information should not be improperly altered or destroyed. And, third, personal information should be accurate, timely, complete, and relevant for the purposes for which it is provided and used.

The Privacy Principles call on those who gather and use personal information to recognize and respect the privacy interest that individuals have in personal information by (1) assessing the impact on privacy in deciding whether to obtain or use personal information; and, (2) obtaining and keeping only information that could be reasonably expected to support current or planned activities. Data gatherers should use the information only for those current or planned activities or for compatible purposes.

Because individuals need to be able to make informed decisions about providing personal information, the organizations that collect information should disclose: (1) why they are collecting the information; (2) for what purposes they expect to use the information; (3) what steps will be taken to protect the confidentiality, quality and integrity of information collected; (4) the consequences of providing or withholding information; and (5) any rights of redress that are available to individuals for wrongful or inaccurate disclosure of their information.

Organizations that gather personal information should take reasonable steps to prevent improper disclosure or alteration of information collected, and should enable individuals to limit the use of their personal information if the intended use is incompatible with the reason for which the information was collected, or not disclosed in the notice provided by collectors.

Organizations that gather personal data should educate themselves, their employees, and the public about how personal information is obtained, sent, stored, processed, and protected, and how these activities affect individuals and society.

The Privacy Principles obligate individuals to obtain relevant information about why the information is being collected, what the information will be used for, what steps will be taken to protect that information, the

orgs that gather data = educate public

consequences of providing or withholding information, and any rights of redress that they may have. They should have notice and a means of redress -- and they should use the means provided -- if they are harmed by improper use or disclosure of personal information.

The Privacy Principles are designed to balance the rights of individuals with the information needs of both government and business. They establish a foundation upon which industry and associations may develop codes and standards for their profession, agencies may evaluate privacy policies, and legislators may enact legislative solutions. The Privacy Principles were developed collaboratively, with input from both the public and the private sectors. This Options Paper incorporates extensive research, analysis and writing undertaken in 1995 and 1996 by the Privacy Working Group in its subsequent study of options for protecting personal privacy on the NII.

3. *The EU Privacy Directive*

Nearly simultaneously with issuance of the IITF Privacy Principles, the Council of Ministers of the European Commission adopted a Council Directive "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (the EU Directive).⁽⁹⁾ The EU Directive requires members states to conform their national privacy laws by mid-1998.

Under the EU Directive, personal data must be collected for specified and legitimate purposes and "not processed in a way incompatible with those purposes."⁽¹⁰⁾ Data must be adequate, relevant, accurate, current, not excessive, and must not be kept in identifying form for any longer than necessary.⁽¹¹⁾ Personal data may be processed only if the data subject has consented "unambiguously" or if the processing falls within an exception, some of which include contract, legal obligation, or where a data subject's "fundamental rights and freedoms" in the personal information do not outweigh the legitimate interests of the data gatherer and where processing is necessary to pursue these interests.⁽¹²⁾ Under the EU Directive, member states must provide judicial remedies for any breach of the rights guaranteed, and adopt enforcement mechanisms, including sanctions for infringements of the privacy laws enacted in conformance with the Directive.⁽¹³⁾ The EU Directive requires member states to establish supervisory authorities to monitor the application of national law adopted pursuant to the EU Directive. The supervisory authorities are required to have investigatory authority, effective powers of intervention, and the power to engage in legal proceedings or to bring violations to the attention of judicial authorities.⁽¹⁴⁾

Article 25(2) of the EU Directive requires member states to ensure that personal data is transferred only to third countries with "adequate" privacy protection.⁽¹⁵⁾ Adequacy is to be determined on a case by case basis in light of all the circumstances surrounding a particular data transfer.⁽¹⁶⁾ The U.S. and EU are discussing how the EU Directive might affect transatlantic data flow, but these discussions are in early stages. Nevertheless, no discussion of online privacy protection can be complete without appropriate consideration of the EU Directive and its implications for international trade in the Information Age.

II.

PRIVACY DEFINED

The idea of a right to privacy was first applied to the private sector in 19th Century America. Samuel Warren and Louis Brandeis, for example, discussed the right to be "let alone" in a Harvard Law Review article published in 1891.⁽¹⁷⁾ Seventy years later another distinguished jurist, William Prosser, concluded that no right to privacy existed under U.S. Constitutional law, but identified various tortious invasions of privacy.⁽¹⁸⁾ Finally, in *Griswold v. Connecticut*, the Supreme Court recognized a limited Constitutional right applicable to certain intimate decisions related to family or marital matters.⁽¹⁹⁾

Other definitions of privacy include the right to be left alone and to control information about oneself with respect to less intimate matters.⁽²⁰⁾ Privacy expert Alan Westin defined information privacy as the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.⁽²¹⁾ On several occasions Congress has supplied statutory protection for records that does not fall within the sphere of protection recognized by the courts.⁽²²⁾

Information privacy is not an unlimited or absolute right. Individuals cannot suppress public records, nor control information about themselves that, by law, is used for a permissible purpose (e.g., criminal defendants cannot prevent courts from examining their prior criminal record before imposing sentence, and sellers of realty cannot prevent a title search of their property). Although individuals may refuse to disclose certain facts about themselves, such disclosure is often either required by law (e.g., tax information) or required if the data subject hopes to participate in society in a meaningful way (e.g., disclosing financial information to obtain a mortgage or releasing medical information to obtain insurance coverage). As a practical matter, individuals cannot participate fully in society without revealing vast amounts of personal data.

Networked electronic environments like the GII complicate the task of establishing the appropriate scope of privacy rights. For example, anonymous telephone communication poses a limited risk to society. The harm caused by any particular call is limited to the participants in that telephone call. The GII, on the other hand, facilitates low cost, simultaneous dissemination of harmful or illegal material to a far broader audience, making anonymity potentially a much bigger problem.⁽²³⁾ Nonetheless, there are many circumstances where individuals may legitimately seek to preserve their anonymity. And, of course, the same technologies for safeguarding anonymity in the digital environment empower individuals to control the dissemination of their personal information.

Although there is no universal agreement about what "privacy" is, it is of considerable and increasing concern to Americans.⁽²⁴⁾ Thus, the critical question becomes: how do we balance the need to use information (by government, commerce, and individuals) with the natural desire of individuals to decide what information about themselves will be exposed to others? Having articulated principles for striking that balance, how do we implement them?

III.

INFORMATION PRIVACY IN THE ELECTRONIC AGE

In a few short years, computers have become powerful and prevalent. This technology has facilitated a tremendous increase in the acquisition of personal information by the private sector. Consumers increasingly purchase goods with credit and debit cards, buy new information services (such as pay-per-view movies),

and engage in an ever greater number of electronic transactions (e.g., e-mail). The information generated in the course of these transactions is routinely gathered, aggregated, and shared.⁽²⁵⁾ Businesses often collect this information in ways that are not readily apparent to the individual.⁽²⁶⁾ New information technologies may not fall neatly within our current experiences.

Modern technology makes it easier to integrate data from numerous sources to create a powerful information package about an individual. Data errors become more harmful as they are more readily propagated.⁽²⁷⁾ The result may be an "electronic clone,"⁽²⁸⁾ a personal profile in digital form that provides detailed and predictive insight into an individual's medical condition, buying habits, personal tastes, economic status, vacation choices, ethnic background, political and religious affiliations, and even the causes and programs which he or she supports.⁽²⁹⁾ Although estimates vary, privacy experts believe that lists track more than two billion names. The average American is on at least twenty-five (and as many as one hundred) of these lists at any one time.⁽³⁰⁾

This trend worries some commentators like David F. Linowes, former chairman of the Privacy Protection Study Commission, who has noted that:

Without our knowledge we are profiled and placed on many specialized lists, whether we like it or not. You could be classified as a foreign policy hawk, affluent ethnic professional, black activist, person who frequents the dice table. You don't know what lists you are on.⁽³¹⁾

Some industry groups have adopted codes and principles, but many have not.⁽³²⁾ Corporate privacy policies are sometimes inadequate in the digital context or simply non-existent. Where such policies do exist, a significant gap may remain between announced policies and actual practices.⁽³³⁾ The bottom line is, the vast majority of personal information currently can be sold, shared, exchanged and disseminated without notice to, or input from, the data subject.⁽³⁴⁾

Individuals disagree on the extent to which the collection and use of information should be limited to protect privacy, but most agree it is appropriate to engage in a careful weighing of benefits and harms. Professor Westin describes the majority of Americans as "privacy pragmatists" -- that is, individuals who are concerned about consumer privacy and consider promised benefits before they disclose personal information to business.⁽³⁵⁾

The Privacy Principles acknowledged this balancing process, stating that privacy interests are not absolute and must be balanced by the need for legal accountability, adherence to the First Amendment, law enforcement needs, and other collective benefits recognized in law.⁽³⁶⁾

How does one determine what constitutes an acceptable use of information in any particular situation? Some data uses create significant opportunities for both the data subject and society as a whole. For example, companies use sophisticated databases that identify individuals likely to buy a particular product. The data subject gets desired goods and services. Those goods and services may be less expensive because increased information about a consumer's credit history decreases the risk credit granters must bear. Lower marketing costs reduce entry barriers, and competition thrives. Another example is the use of databases to ensure that citizens receive government benefits that they need while minimizing payment of fraudulent claims. Compiling medical information for research purposes may help cure diseases.

Misuse of information, on the other hand, can create an equally lengthy list of harms. Employers might misuse medical information by denying an individual a job because of an old stigmatizing medical condition, such as depression. Improper use of demographic information by a bank could result in redlining, and the inappropriate disclosure of personal information may cause embarrassment, harassment, or victimization.

The Privacy Principles also recognize the need to consider "the individual's expectations regarding the use of the information."⁽³⁷⁾ Ultimately, the appropriateness of any given use of information must be considered on a case-by-case basis. The magnitude of information collection, storage, and dissemination today increases the probability that information will be used in a manner not reasonably contemplated by the data subject. Separating clearly acceptable uses (those that maximize opportunity with minimal impact upon privacy) from clearly unacceptable uses (those that severely reduce privacy with little or no benefit) may not be difficult. Most cases, however, fall in the middle of the spectrum where the benefits of using the information must be weighed against any diminution in privacy. Decisions about the use of personal data will be influenced by cultural norms, market forces, operating efficiencies, law and law enforcement efforts, civil liability and other factors. How will these factors be weighed in the borderless realm of cyberspace?

Thus, we turn to a consideration of current efforts to protect privacy in the United States. This work does not attempt to catalog and discuss every privacy law, or every substantive privacy issue. Instead, it focuses on four critical areas that illustrate a broad range of privacy concerns and various responses:

- (1) privacy of federal government records (the primary source of American concern traditionally);
- (2) privacy in communications (heavily regulated);
- (3) privacy of medical records (for the most part, unregulated); and
- (4) privacy in the marketplace (regulated in part, otherwise unregulated but subject, in some cases, to industry imposed codes of fair information practices).

IV.

PRIVACY PROTECTION IN FOUR ECONOMIC SECTORS

Privacy is a complex concept. An acceptable use of information in one setting may be an unacceptable invasion of privacy in another. Within a particular setting, individuals make very different judgments about what constitutes an acceptable use of their personal information. This diversity makes it difficult to apply a uniform privacy protection scheme across all sectors of human interaction.

In the United States, business and government have adopted sector-specific privacy rules, combining legislation, regulation, and voluntary codes to achieve the desired level of privacy protection in each sector. Each of these tools offers a different level of protection, and provides a different remedy. If a widely respected social custom is violated, the penalty may be embarrassment or ostracism. Market forces may cause a company that inappropriately sells personal customer information to lose business to a competitor. Failure to follow accepted computer security standards may result in civil liability. Failure to follow legal requirements may result in civil or even criminal penalties.

In the sector discussions that follow, we start with legal restrictions that bind information users and follow with an analysis of private policies and principles that supplement existing law and regulation. Finally, we consider how successful this combination of law and policy has been and how it is likely to hold up in the online environment.

PRIVACY OF FEDERAL GOVERNMENT RECORDS

The role of the federal government is to "establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity."⁽³⁸⁾ In support of its Constitutional mandate, the federal government coins money, collect taxes, regulates commerce, runs post offices, oversees immigration, funds social welfare programs, punishes crimes, and engages in a host of other activities designed to sustain the democracy itself and protect the welfare of its citizens.

Governments maintains volumes of records on their own activities and on the activities of their citizens (e.g. voter registration, motor vehicle, real property, commercial, criminal, marriage, birth, death and even library records). Increased computerization of these records permits them to be used and analyzed in new ways that could diminish individual privacy in the absence of data protection safeguards.

1. The Privacy Act of 1974

Congress passed the Privacy Act⁽³⁹⁾ after the Watergate break-in, and against its backdrop of governmental misuse of personal information.⁽⁴⁰⁾ The Act restricts the collection, use, and dissemination of personal information by federal agencies. The Privacy Act first limits federal collection of personal data to information that is "relevant and necessary" to accomplish a purpose of the agency.⁽⁴¹⁾ Federal agencies must also establish safeguards to ensure the security and confidentiality of records.⁽⁴²⁾ Unless a proposed disclosure falls within enumerated exceptions, the Privacy Act prohibits disclosure of that information without the prior written consent of the data subject.⁽⁴³⁾

The Privacy Act generally applies only to federal records that are retrieved by name or other personal identifier.⁽⁴⁴⁾ It protects U.S. citizens and permanent residents, but does not apply to foreign visitors, undocumented aliens, corporations, or other organizations.⁽⁴⁵⁾ Under the Privacy Act, individuals have the right to access agency records containing information about themselves,⁽⁴⁶⁾ and the right to request amendment of information that is inaccurate, irrelevant, untimely, or incomplete.⁽⁴⁷⁾ The Act provides civil remedies including injunctive relief for most violations,⁽⁴⁸⁾ and criminal penalties for knowing and willful violations of the Act.⁽⁴⁹⁾

The Act permits agencies to disclose records without consent when the disclosure is "compatible" with the purpose for which the information was collected.⁽⁵⁰⁾ Federal agencies have been repeatedly criticized for over-broad application of this "routine use" exception.⁽⁵¹⁾ Critics contend that agencies have ignored the requirements of a close nexus between the purpose of information collection and its proposed routine use.⁽⁵²⁾ Court attempts to close this loophole have had mixed results. One commentator notes that

[t]he Act has produced mechanisms for coping with paperwork, instead of the altered behaviors of bureaucrats and individuals that were anticipated" and that "it became clear from several years of experience, the compromises and exceptions of the 1974 Act erected the facade of a major bill of rights for individuals, against the reality of a 'paper tiger' privacy statute."⁽⁵³⁾

2. The Computer Matching and Privacy Protection Act of 1988

Congress passed the Computer Matching and Privacy Protection Act of 1988 (Matching Act)⁽⁵⁴⁾ to address concerns that agencies were using the routine use exception to justify widespread electronic comparison of federal databases.⁽⁵⁵⁾ The Matching Act, which amends the Privacy Act, regulates federal agency use and exchange of information contained in existing agency databases. Under the Matching Act, agencies must follow specific procedures when engaging in the automated comparison of Privacy Act databases on the basis of certain data elements.⁽⁵⁶⁾ Agencies must, for example, perform a cost/benefit analysis of proposed matching activity.⁽⁵⁷⁾ The Matching Act also protects individuals who suffer adverse consequences as a result of a computer match. Before denying or terminating a government benefit on the basis of computer matching, agencies must notify the data subjects and provide an opportunity to refute adverse information.⁽⁵⁸⁾ The Matching Act requires agencies engaged in matching activities to establish Data Protection Integrity Boards to oversee these activities.⁽⁵⁹⁾

The General Accounting Office has criticized both the substance of the Matching Act and its implementation.⁽⁶⁰⁾ The Act provides procedural safeguards, but does not provide substantive guidance as to the circumstances under which a match is or is not acceptable.⁽⁶¹⁾

3. The Paperwork Reduction Act

Congress enacted the Paperwork Reduction Act (PRA)⁽⁶²⁾ in 1980 to minimize the federal paperwork burden, to coordinate federal information policies and to ensure that the "collection, maintenance, use and dissemination of information by the federal government is consistent with applicable laws relating to confidentiality."⁽⁶³⁾ The PRA originally directed the Office of Information and Regulatory Affairs (OIRA) of the Office of Management and Budget (OMB) to ensure that information proposed to be collected by a federal agency⁽⁶⁴⁾ was necessary for the proper performance of the functions of the agency, including whether the information will have practical utility for the agency.⁽⁶⁵⁾ Congress specifically assigned various privacy functions to OIRA, including the development and implementation of policies, principles, standards, and guidelines on information disclosure, confidentiality, and on safeguarding the security of information collected or maintained by or on behalf of agencies.⁽⁶⁶⁾ Every year OIRA reviews, and has the opportunity to narrow, over two thousand federal agency requests to collect information.⁽⁶⁷⁾ Moreover, under the PRA, federal agencies are required to employ fair information practices by informing individuals why the information is being collected, how it is to be used, and whether responses to the inquiries are voluntary, required to obtain a benefit, or mandatory.⁽⁶⁸⁾

4. *The Freedom of Information Act*

Open government, and access to government records, facilitates public participation in governance. The Freedom of Information Act (FOIA)⁽⁶⁹⁾ empowers citizens to access government records. But FOIA also balances public access rights with individual privacy rights by allowing agencies to exempt from disclosure personal information subject to the Act.⁽⁷⁰⁾ In *Department of Justice v. Reporters Committee for Freedom of the Press*,⁽⁷¹⁾ the Supreme Court determined that purely personal information about private individuals is not subject to disclosure under FOIA because it does not advance the purpose of the Act, which is to shed light on the conduct of government agencies or officials.⁽⁷²⁾

5. *Statutory Limits Applicable to Federal Agencies*

A number of organic statutes limit the use of personal information collected by particular agencies in the course of fulfilling their statutory obligations. For example, federal law prohibits the use of census records for anything other than statistical purposes.⁽⁷³⁾ Subject to extremely narrow exceptions, only Census Bureau officers, sworn to uphold the confidentiality of census records, may access any census information that identifies individuals.⁽⁷⁴⁾

At the federal level, the Internal Revenue Service (IRS) possesses the most comprehensive personal financial information. Individuals must report income from all sources, and there are incentives to itemize certain types of deductible expenditures such as home mortgage interest, charitable contributions, and other expenses.

Section 6103 of the Internal Revenue Code, as amended by the Tax Reform Act of 1976,⁽⁷⁵⁾ prohibits unauthorized disclosure of tax returns and return information by employees of the federal government, state and local governments, or IRS contractors.⁽⁷⁶⁾ The statute covers virtually everything collected by or generated by the Internal Revenue Service related to a taxpayer's tax liability, including a taxpayer's identity, whether a return was, is being, or will be examined, any data submitted by the taxpayer or his or her representative, any data collected by the IRS from other sources, and any material generated by the IRS relating to any specific taxpayer's liability.

Unauthorized disclosure of tax information subjects the offender to criminal penalties and permits the wronged party to bring a civil action for damages. The statute provides for minimum damages of \$1,000 per disclosure.⁽⁷⁷⁾

The statute requires the IRS to keep records of requests for disclosure and to report a summary of requests for and disclosure of returns and return information each year to Congress. Furthermore, the statute requires

federal agencies that receive returns and return information from the IRS to establish procedures to safeguard such information and to report periodically to the IRS on those procedures.⁽⁷⁸⁾

6. The Privacy Principles

Although the Privacy Principles were issued in June of 1995, their impact on federal data collection is not yet clear. It should be noted, however, that a number of agencies, including the IRS and HHS, have appointed Privacy Advocates whose primary responsibility is to oversee their agency's compliance with privacy laws and to participate in the development of sector specific privacy policies.

7. Federal Law Regulating State Sale of Government Data

Most states lack comprehensive fair information principles applicable to data in the possession of the government.⁽⁷⁹⁾ That data is an increasingly important source of state revenue and in great demand in the marketing community.⁽⁸⁰⁾ In some cases, however, federal law conditions receipt of federal funding on the adoption of data protection at the state levels. Student records,⁽⁸¹⁾ child abuse information,⁽⁸²⁾ and motor vehicle related information⁽⁸³⁾ are all examples. Thus, under the Drivers Privacy Protection Act of 1994, states must afford motor vehicle registrants or licensed drivers an opportunity to choose not to make their data available before their personal information is released.⁽⁸⁴⁾

8. Summary

At the federal level, the United States has adopted a fairly comprehensive approach to protecting government held personal data from unauthorized or inappropriate disclosure. The approach combines limits on (1) the amount and type of data collected by an agency in the first instance, (2) the use of such information within an agency, and (3) the disclosure of that information outside an agency. In most cases, citizens are entitled to access and request amendment of personal information maintained in government files. Violators of the federal privacy statutes face both civil and criminal penalties.

The federal system of data protection, though comprehensive, is criticized, however, as a "paper tiger" with significant enforcement and remedial deficiencies.

COMMUNICATIONS PRIVACY

Americans consider few rights more sacred than the right to communicate privately with other individuals, whether by telephone or by mail. In recognition of this fact, the law protects all real-time communications and stored transmissions (e.g., electronic mail and voice mail).⁽⁸⁵⁾ Separate laws protect the privacy of paper mail.⁽⁸⁶⁾

1. Real-time Communications

Subject to enumerated exceptions, it is illegal in the United States to intercept the contents of wire, oral, or electronic communications or to disclose the contents of a communication that one knows to have been illegally intercepted.⁽⁸⁷⁾ Oral communications are protected whenever the speaker exhibits a reasonable

expectation of privacy.⁽⁸⁸⁾ Wire communications are defined as conversations that travel in whole or in part by wire and are understandable to the human ear.⁽⁸⁹⁾ Electronic communications are defined as any other transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects interstate or foreign commerce.⁽⁹⁰⁾ Thus, the protection for electronic communications covers faxes and other types of data transfers.

The most frequently used exceptions allow communications to be intercepted by: (1) a law enforcement officer if acting pursuant to a court order;⁽⁹¹⁾ (2) any person, if at least one party to the communication gives consent;⁽⁹²⁾ (3) an employer, when acting in the ordinary course of its business;⁽⁹³⁾ and (4) a service provider when the provider is monitoring wire or electronic communications in the normal course of business as a necessary incident to the rendition of service or to protect the rights or property of the provider.⁽⁹⁴⁾

Individuals now use e-mail as frequently as the telephone, but the distinction between wire and electronic communications retains legal significance. First, voice communications may only be intercepted pursuant to a court order in connection with the suspected commission of certain designated offenses.⁽⁹⁵⁾ By contrast, electronic communications may be intercepted in connection with the suspected commission of any federal felony.⁽⁹⁶⁾ Second, electronic communications are not covered by the statutory exclusionary rule, which otherwise prohibits the use of communications unlawfully intercepted in any judicial, legislative, or regulatory proceeding.⁽⁹⁷⁾

2. *Stored Communications*

The law also protects voice mail and electronic mail (e-mail) in electronic storage.⁽⁹⁸⁾ The statute defines electronic storage as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."⁽⁹⁹⁾ To be in electronic storage within the meaning of the statute, an electronic communication must be in storage as a by-product, or incidental feature, of the transmission of the message.⁽¹⁰⁰⁾ Storage for record keeping purposes is not covered.⁽¹⁰¹⁾

It is unlawful for anyone intentionally to access without authorization a facility through which an electronic communication service is provided, or intentionally to exceed authorization to access that facility, and thereby obtain, alter or prevent authorized access to a wire or electronic communication while it is in electronic storage.⁽¹⁰²⁾ Anyone who provides an electronic communication service or remote computing services⁽¹⁰³⁾ to the public is prohibited from voluntarily disclosing the contents of an electronic communication stored or maintained on the service.⁽¹⁰⁴⁾

There are several important exceptions to these non-disclosure provisions: stored content may be disclosed with the lawful consent of the originator, an addressee, or the intended recipient of such communication;⁽¹⁰⁵⁾ a service provider may disclose content incident to its rendition of service or to protect the rights of the provider;⁽¹⁰⁶⁾ and disclosure to a law enforcement agency is permitted if the contents were inadvertently obtained and appear to pertain to the commission of a crime.⁽¹⁰⁷⁾

Different rules govern access to a stored communication, depending upon how long the particular communication has been in electronic storage and who is seeking access. The government may access communications stored for one hundred and eighty days or less only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or an equivalent state warrant.⁽¹⁰⁸⁾ Prosecutors may use either a Rule 41 search warrant (without notice to the customer or subscriber) or an administrative subpoena, grand jury subpoena, trial subpoena, or a court order pursuant to 18 U.S.C. § 2703(d) (with notice to the customer or subscriber) to access information stored for more than one hundred eighty days.

3. Toll Records and Other Subscriber Information

The prohibitions on real-time interceptions and access to voice and electronic mail protect the contents of communications. But communications systems not only carry messages, they create records that reveal information about system users. Telephone toll billing records, for example, indicate what phone line was used to call what numbers, when, and for how long.

Prior to 1986, telephone toll billing records were not protected from disclosure under federal law and the federal government routinely gained access to telephone toll records without any judicial process. Indeed, in *Smith v. Maryland*, the Supreme Court held that toll records could be obtained without a search warrant because a caller had no "legitimate expectation of privacy" in the telephone numbers he or she dialed.⁽¹⁰⁹⁾

In 1986 Congress enacted the Electronic Communications Protection Act (ECPA),⁽¹¹⁰⁾ which, among other things, extended protection to toll records.⁽¹¹¹⁾ ECPA permits a government entity to obtain "a record or other information pertaining to a subscriber to or customer of such service" without the subscriber or customer's consent only with an administrative subpoena, grand jury subpoena, trial subpoena, search warrant, or a court order.⁽¹¹²⁾ In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA).⁽¹¹³⁾ Under CALEA, basic subscriber information can be obtained with a subpoena.⁽¹¹⁴⁾ Subscriber information includes the name, address, toll records, telephone number or other subscriber number or identity, a subscriber's length of service and the types of services the subscriber or customer utilized.⁽¹¹⁵⁾ To obtain other information (e.g., records of the addresses to which the subscriber has sent e-mail messages), the government must now obtain a search warrant or court order.⁽¹¹⁶⁾ In either case, law enforcement need not notify the data subject.⁽¹¹⁷⁾

Additionally, CALEA raised the level of proof required to obtain court orders. Pre-CALEA, the government had only to show that there was "reason to believe" that the information sought was "relevant to a legitimate law enforcement inquiry." Now, the government must present "specific and articulable facts showing that there are reasonable grounds to believe" that what they seek is "relevant and material to an ongoing criminal investigation."⁽¹¹⁸⁾

Although the ECPA specifically prevents electronic communications service providers from disclosing information to the government unless certain conditions are met, it does not preclude them from selling that

same transactional data to non-governmental entities.⁽¹¹⁹⁾ Communications providers have access to a wide variety of telecommunications-related personal information (or TRPI).⁽¹²⁰⁾ This transactional data may include routing data that indicates who communicated with whom at what time, day, and month, and for how long, as well as billing records and associated data. Other personal information may be available, including records of electronic purchases made over interactive networks, point-of-sale payments transacted electronically over networks, and even cable movies ordered and billed separately. Telecommunications service providers can automatically capture, monitor, and sell such information.

4. The Telecommunications Act of 1996

The Telecommunications Act of 1996⁽¹²¹⁾ imposed new limits on the use of customer proprietary network information (CPNI) by common carriers.⁽¹²²⁾ CPNI is information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service by customers obtained by virtue of the carrier-customer relationship, including billing information.⁽¹²³⁾

Section 222 of the 1996 Act provides that telecommunications carriers may use, disclose, or permit access to individually identifiable CPNI only to provide the telecommunication service from which the CPNI is derived, or services necessary to provide such services, including publishing directories.⁽¹²⁴⁾ The law establishes three exceptions to this blanket prohibition. A telecommunications carrier may use individually identifiable CPNI to (1) initiate, render, bill and collect for telecommunications services; (2) protect its rights or property, or to protect its users and other carriers from fraudulent, abusive, or unlawful telecommunications services; or (3) provide inbound telemarketing, referral, or administrative services to a customer, for the duration of the call, if the customer initiated the call and approves of the use of CPNI to provide such service. Carriers are required to disclose individually identifiable CPNI to any person affirmatively designated by the customer in writing.

The FCC reviewed public comments on proposed regulations to specify and clarify the obligations of telecommunications carriers under these 1996 Act CPNI provisions.⁽¹²⁵⁾ It has issued a further request for public comment on the interplay between the non-discrimination provisions and Section 222.⁽¹²⁶⁾

5. Other Telecommunications Services

New telephone service options like Caller ID and Automatic Number Identification (ANI) raise new privacy issues. Recently, the FCC approved final rules for nationwide Caller ID, which will let subscribers see the phone number of even long-distance calls they receive. To protect consumer privacy, the FCC will allow callers to block their numbers from being displayed on a per-call basis and a per-line basis.⁽¹²⁷⁾ With ANI, a marketing firm can immediately obtain the phone number of a caller and then obtain other specific personal data on that individual by using commercial databases. ANI data can easily be used to build marketing lists without a caller's knowledge or consent. No policy limits this type of activity, and most consumers are not aware of its existence.⁽¹²⁸⁾

In October 1995, the Commerce Department's National Telecommunications and Information Administration (NTIA), drawing upon the Privacy Principles, developed a White Paper, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information.⁽¹²⁹⁾ The NTIA White Paper constructed a framework for safeguarding personal information associated with subscribing to and using telecommunications or

information services. NTIA proposed a voluntary framework for the telecommunications industry with two fundamental elements: provider notice and customer consent.⁽¹³⁰⁾ NTIA calls upon telecommunications and information service providers to notify individuals about their information practices, abide by those practices, and keep customers informed of subsequent changes to such practices. Under this framework, individuals are considered to have consented to use of their information in accordance with the business' notice if they do not object. This tacit consent (opt-out) is considered sufficient in most cases. When sensitive information is at issue, however, explicit consent (opt-in) is required.⁽¹³¹⁾

Following release of the proposed framework, NTIA contacted more than 40 telecommunications and information providers requesting feedback on their policies and practices. NTIA is now meeting with the providers to determine if they adhere to the principles outlined in the report. Based on the outcome of these discussions, NTIA will determine whether further government action is needed.

NTIA has also issued a call for papers on how to make voluntary codes more effective and, more specifically, to obtain consensus on principles, including provisions for auditing and dispute resolution. NTIA plans to issue a report on papers received from members of industry, as well as from the academic and legal communities.

6. Self Regulatory Efforts

Non common-carrier providers of telecommunication services -- including, for example, online service providers -- are not subject to FCC regulations or federal law regarding commercial use of CPNI. Nonetheless, the industry is sensitive to consumer privacy concerns and has embarked on a program of self-regulation. In June of 1995, the Interactive Services Association issued voluntary minimum guidelines for online services wishing to disseminate online subscriber information.⁽¹³²⁾ The guidelines are based on a regime of notice and opt-out. At a minimum, online service providers are called upon to clearly and actively notify subscribers of their information practices and to offer every subscriber an easy, obvious, and recognizable opportunity to have his or her name and address excluded from information made available to third parties. Several online service providers participated in the development of and have subscribed to these guidelines. In most cases, online service provider use of personal data is governed by terms of service that are, in turn, enforceable in a court of law.⁽¹³³⁾

7. Laws Protecting the Privacy of Mail

First class domestic mail may be opened, and the contents inspected, only (1) with the authorization of the addressee, (2) pursuant to a valid search warrant authorized by law, or (3) by an officer or employee of the Postal Service for the sole purpose of determining an address at which the mail can be delivered.⁽¹³⁴⁾

A different federal statute applies to mail originating outside the United States. Under this statute a customs officer or other person authorized to board or search vessels may "search any . . . envelope, wherever found, in which he may have a reasonable cause to suspect there is merchandise which was imported contrary to law" ⁽¹³⁵⁾

The Postal Service regulates permissible use of the "mail cover," an investigative procedure whereby government officials record information appearing on the exterior of first class mail, and information regarding both the exterior and contents of lower classes of mail. Under Postal Service regulations, the government may

use mail covers only to protect national security; locate a fugitive; obtain evidence of commission or attempted commission of a crime; obtain evidence of a violation or attempted violation of a postal statute; or assist in the identification of property, proceeds or assets forfeitable under law.⁽¹³⁶⁾ Furthermore, law enforcement agencies must submit mailcover requests to the Post Office in writing, setting forth reasonable grounds to believe the mail cover is necessary for one of the enumerated purposes.⁽¹³⁷⁾

8. Summary

Existing law regulates and limits government access to and use of communications information, including both communications content and transactional data generated by communications. Existing law also prohibits the interception of the contents of a communication by a private party. Traditionally, telecommunications service providers were free to disclose transactional data regarding customer use of enhanced telecommunications services to others in the private sector. The Telecommunications Act of 1996 closes this loophole with respect to common carriers. With respect to other service providers, however, such as online services, the United States rely on self regulatory approaches, including contract law, to promote an appropriate level of communications privacy.

MEDICAL RECORD PRIVACY

Cost concerns are driving the nation's health care delivery system to a more cost-conscious, competitive, managed care environment. The health care industry is increasingly committed to computer networks that can collect, aggregate, and disseminate personal medical information on a nationwide basis. Use of the NII may help provide better care for less, and better use of information technology generally can make an important contribution to this effort. Existing and potential applications include telemedicine (remote medical diagnosis/care), unified electronic claims, personal health information systems, and computer-based patient records.⁽¹³⁸⁾ The Physician Computer Network, Inc. (PCN), for example, has developed software that links physicians to insurance companies, clinical laboratories and hospitals. The system benefits doctors and patients by cutting the cost and delays associated with processing medical claims, receiving test results and changing medications and orders for hospitalized patients. In exchange for providing discount computers, PCN acquires aggregated patient records, including diagnoses and treatments, which it compiles and then sells to pharmaceutical companies and insurers.⁽¹³⁹⁾

Public concern about medical privacy is quite high.⁽¹⁴⁰⁾ Medical records often contain highly sensitive and personal information and can reveal more about an individual than virtually any other type of record.⁽¹⁴¹⁾ In response to public concerns, companies like PCN have implemented internal security measures and engaged a public accounting firm to certify that their data is maintained securely.⁽¹⁴²⁾ In 1994, the Institute of Medicine called upon Congress to enact preemptive legislation to assure the confidentiality and protection of privacy rights in personally-identifiable health data.⁽¹⁴³⁾ The National Research Council recently reported that computerized medical records are "vulnerable to misuse and abuse" and likewise called for the creation of additional incentives to ensure that healthcare industry employees protect patient information.⁽¹⁴⁴⁾

Medical privacy concerns are not new. As early as 1977 the Privacy Protection Study Commission recognized that the trend toward computerization of medical record information posed "new problems" from a "privacy protection viewpoint."⁽¹⁴⁵⁾ Among other things, the Commission concluded that medical records

contained more information and were available to more users than ever before. Additionally the Commission found that changes in the medical profession, increased population mobility, and increased demands by third parties for medical record information had greatly diluted the control that medical care providers had once exercised over such information. The Commission predicted that the demand for access to such information by third party users would increase over time, observing:

[T]he importance of medical-record information to those outside of the medical-care relationship, and their demands for access to it, will continue to grow. Moreover, owing to the rising demand for access by third parties, coupled with the expense of limiting disclosure to that which is specifically requested by the non-medical user, there appears to be no natural limit to the potential uses of medical-record information for purposes quite different from those for which it was originally collected.⁽¹⁴⁶⁾

The Commission's 1977 prediction is a 1997 reality. Today, industry amasses and shares staggering amounts of medical information.⁽¹⁴⁷⁾ Health care providers are now able to develop centralized profiles on the medical condition of patients, as well as the treatment of that condition in order to facilitate care, research, and insurance billing and coverage.⁽¹⁴⁸⁾ Another example is the Medical Information Bureau (MIB), a non-profit trade organization that serves life and disability insurance companies by maintaining extensive databanks of medical and other information on millions of Americans and Canadians.⁽¹⁴⁹⁾ This information has been referred to as "the medical equivalent of a credit report."⁽¹⁵⁰⁾

As the Privacy Protection Study Commission predicted in 1977, medical information is routinely shared with and viewed by third parties who are not involved in patient care. Secondary users of medical information include educational institutions, the civil and criminal justice systems, life and health insurers, rehabilitation and social welfare programs, credit agencies, public health agencies, and medical and social researchers.⁽¹⁵¹⁾ The American Medical Records Association has identified twelve categories of information seekers outside of the health care industry who have access to health care files, including employers, government agencies, credit bureaus, insurers, educational institutions, and the media.⁽¹⁵²⁾

Traditionally, health care and health insurance providers have guarded patient privacy in accordance with professional codes of ethical behavior, such as doctor-patient confidentiality. But no federal statute generally protects the confidentiality of medical records in the private sector.⁽¹⁵³⁾ As an OTA report observed, existing law allows development of private-sector databases and data exchanges of patient information without regulation, statutory guidance, or recourse for individuals harmed by misuse of the data.⁽¹⁵⁴⁾

Not surprisingly, technology and market pressures are beginning to erode the traditional protections for medical records. Consensus is emerging that doctor-patient confidentiality practices and the widely varying protection afforded under individual state laws no longer adequately protect the privacy of medical information. The Computer-based Patient Record Institute (CPRI), for example, drafted principles that call for federal standardization of patient confidentiality safeguards including stiff penalties and fines for those who knowingly breach the confidentiality of patient records.⁽¹⁵⁵⁾

Some health organizations and companies have adopted voluntary privacy standards based on fair information principles.⁽¹⁵⁶⁾ Major model codes and statutes in this industry include, for example, the American Health Information Management Association's Health Information Model Legislation language.⁽¹⁵⁷⁾ As a practical matter, however, model codes and statutes have woven only a loose web of protection: they

may apply to limited types of information, may not address secondary users of health information, lack enforcement powers, or simply have not been adopted (only a handful of States have comprehensive health-care information confidentiality statutes).⁽¹⁵⁸⁾

The FTC recently entered into an agreement with the Medical Information Bureau (MIB) under which insurance companies must notify consumers when information provided by MIB plays a part in a decision to deny coverage or to charge a higher rate. Under these circumstances, MIB will give consumers a free copy of their medical information report, in order to verify that all information is correct.⁽¹⁵⁹⁾

In its 1993 report, OTA concluded that the current system fails to address privacy issues in a borderless, computerized environment.⁽¹⁶⁰⁾ Rep. Gary Condit, (D-Calif.) has echoed this conclusion: "[B]ecause health information increasingly moves from a computer in one state to a computer in another state, uniform federal rules are needed."⁽¹⁶¹⁾ State privacy advocates have voiced similar concerns.⁽¹⁶²⁾

The nation is some years away from full computerization of the traditional patient record used for clinical care, but is moving swiftly in that direction. Organizations such as the Computer-based Patient Record Institute are coordinating policy development in this area.⁽¹⁶³⁾ Meanwhile, a large volume of medical data is already computerized in the context of insurance payment, managed care, and internal management in health care facilities.

The 104th Congress considered these issues in some detail, particularly with respect to Senate consideration of S. 1360, The Medical Records Confidentiality Act. No general health record confidentiality legislation was enacted, but the House companion bill to S. 1360 has been reintroduced in the 105th Congress as HR 52.⁽¹⁶⁴⁾

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996,⁽¹⁶⁵⁾ includes an administrative simplification subtitle to encourage the development of a health information system based on uniform technological standards for the electronic transmission of financial and administrative health care data. The Secretary of Health and Human Services is required to establish standards to facilitate such transactions. The standards are to include security standards as well as standards for a unique identifier.

HIPAA established a National Committee on Vital and Health Statistics to advise the Secretary of HHS on these standards issues and on medical records privacy. The Committee has held a series of hearings addressing different uses of medical records (e.g. providers, insurers, law enforcement, etc.).⁽¹⁶⁶⁾

Another provision of the Act requires the Secretary to submit detailed recommendations to the Congress with respect to the privacy of individually identifiable health information (i.e. general health record confidentiality legislation applicable to health care providers, insurers, and others) by August 1997. If Congress does not itself act by August 1999, the Secretary must issue privacy standards applicable to electronic transmission before the transmission standards are implemented.⁽¹⁶⁷⁾

PRIVACY IN THE MARKETPLACE

Advances in information technology have produced an economy that thrives on information. Marketplace privacy issues are, in turn, as complex as the market itself. A comprehensive analysis of these issues exceeds the scope of this paper. In order to frame the issues generally, this paper examines how the government and business community balance their information needs with personal privacy values in three specific areas: (1) personal financial information (considered private by most but frequently and necessarily disclosed); (2) video rental records (interesting because this example highlights the problem of dissimilar privacy protection schemes for similar types of information); and (3) direct marketing (a topic of interest to consumers and the source of many complaints to government agencies).

1. Personal Financial Records

Most people consider their financial condition a private matter and are reluctant to disclose their net worth or annual income. At the same time, however, many entities -- including the government, banks, and credit reporting agencies -- possess detailed information on the financial status of many individuals. Frequently, the use and disclosure of this information is regulated, but information that cannot be obtained from one source may be readily available from another.

Tax Records. Tax records held by the government are strictly governed by section 6103 of the Internal Revenue Code. This statute applies to use of tax records by the government for government purposes, as well as disclosure by the government to the private sector.⁽¹⁶⁸⁾

Bank Records. Financial institutions generate and retain vast quantities of financial data on individuals.

(a) **Government access.** Government access to financial information held by financial institutions is regulated by the Right to Financial Privacy Act of 1978 (RFPA).⁽¹⁶⁹⁾ The impetus for enactment of the RFPA can be traced to both prior legislation and judicial decisions.⁽¹⁷⁰⁾

The RFPA limits federal government access to and use of personal financial information maintained by private sector financial institutions in two ways: (1) it regulates the disclosure from the financial institution to the federal agency in the first instance, and (2) it regulates the disclosure among government agencies where an agency has lawfully obtained records from a financial institution pursuant to the Act⁽¹⁷¹⁾.

The RFPA affords significant protection regarding government access to personal financial information. The RFPA attempts to balance this protection with the federal government's legitimate interest in such information. For example, the RFPA requires the government to notify customers of any request for their financial records⁽¹⁷²⁾ and permits customers to challenge the government's request.⁽¹⁷³⁾ Under certain conditions, however, the government may delay the notification.⁽¹⁷⁴⁾ Additionally, the RFPA provides for civil penalties and injunctive relief where financial records have been disclosed in violation of the Act but does not provide for the suppression of records so obtained.⁽¹⁷⁵⁾ Finally, the Act exempts many types of disclosures (*e.g.* disclosure pursuant to a grand jury subpoena or in conjunction with litigation to which the government authority and the customer are parties).⁽¹⁷⁶⁾

(b) **Private sector use.** Banking customers value financial privacy. The banking industry, from the consumer's perspective, is very competitive, particularly at the branch level. A consumer's ability to take his or her

banking business elsewhere may account, in part, for the banking industry's traditional reluctance to disclose banking records.

In the Information Age, can consumers continue to rely on competition to protect their banking records from unwanted disclosure? As new information technologies rapidly expand the abilities of banks to collect, combine, and transmit data about customers, incentives to use banking records for marketing purposes may erode industry's historic restraint. In many cases individuals have little knowledge of or control over the use of their bank records. BankAmerica describes the dilemma aptly:

Privacy is not a new concept in banking. By law and custom, it is recognized throughout the world that the relationship between a bank and its customer is confidential. The proliferation of computers has made the adherence to this concept of privacy more complex. Specifically, the public's concern has centered on the difficulty an individual can have in discovering and controlling what data will be collected about him or her, challenging the accuracy of the data, and determining who will have access to that data and for what purpose.⁽¹⁷⁷⁾

The financial services industry is being challenged by new technology. For example, on-line banking allows customers to pay bills, transfer money between accounts, check balances, and perform other banking transactions by computer or touch-tone phone.⁽¹⁷⁸⁾ Today, consumers can download mortgage application forms, fill out the forms on a computer, and then submit the loan application electronically.⁽¹⁷⁹⁾ Several innovative U.S. banks are exploring the uses of smart cards. These services in turn generate digitized transactional data. Smart cards, for example, might contain a customer's entire credit, purchase, and medical history, along with any other data that can be stored on a microchip.⁽¹⁸⁰⁾ Banks are beginning to use existing customer information more creatively, and adding demographic information to existing customer lists for targeted marketing purposes.⁽¹⁸¹⁾

Changes in the banking industry hold the promise of significant consumer benefits, including:

... the great potential to permit cost-effective, risk-managed marketing to small niches that were often by-passed in big-scale mass marketing efforts because they were too small to pitch a product or promotion to. Lots of data and sophisticated scoring models make it possible to evaluate risk and set prices soundly at low cost, while lots of data and sophisticated marketing make it possible to design products and promotions that go just to target groups, at low cost. This combination opens an opportunity for expanded marketing pitched to the special interests of ethnic minorities, to people who lack traditional credit profiles, and to more people at the margins of the economic mainstream.⁽¹⁸²⁾

The move from traditional banking services into other areas such as database marketing, however, presents new privacy concerns for the industry.⁽¹⁸³⁾ For example, card-issuing banks have access to direct-marketer customer information as part of their billing procedures. Database marketing has likewise brought banks into business relationships with buyers and sellers of personal information who do not share the banking industry's traditional approach to customer privacy. These information brokers are essentially unregulated in their use of personal data.⁽¹⁸⁴⁾ The dramatic fall in the price of computer storage has made it possible for businesses to accumulate and maintain large quantities of data about their customers. For ten cents a name, middlemen offer extensive data on most U.S. families.⁽¹⁸⁵⁾

In the absence of privacy statutes applicable to the financial services sector, some individual financial institutions have adopted privacy codes. But the banking industry is only beginning to adopt industry wide privacy principles.⁽¹⁸⁶⁾

Individual banks and financial service providers have developed internal policies on handling and disseminating customer information. For example, a bank might not release account numbers along with personal financial information furnished to credit bureaus, or may enter into a confidentiality agreement that precludes a third party service provider, such as a supplier of credit life insurance, from using customers' names for any other purpose.⁽¹⁸⁷⁾ Some financial services providers have demonstrated leadership by adopting formal privacy policies.⁽¹⁸⁸⁾ These policies generally restrict disclosure of data to those with a "business need" to see it, and often offer consumers the ability to "opt out" of receiving promotional mail. The opt-out programs do not limit the information that financial companies collect about their customers or purchase from outside sources.⁽¹⁸⁹⁾

In the Information Age, inadequate protection of privileged financial information among banks, credit bureaus, and software manufacturers, especially when combined with other types of information such as demographic profiles, could result in the misuse or abuse of personal information. As banks merge and become more electronically oriented, the potential for privacy problems increases dramatically. Yet, as noted above, there are few laws and privacy principles in place. Whether privacy standards in the banking industry will keep pace with the industry's adoption of new information technologies remains to be seen. But, to the extent that confidentiality of customer information has been "the missing link" for providing on-line transactions,⁽¹⁹⁰⁾ privacy concerns must be addressed if "cyberbanking" is to take root.

Credit Information. The credit reporting industry maintains the largest repositories of information about Americans outside of the federal government.⁽¹⁹¹⁾ The industry is dominated by three giant credit bureaus -- Experian Inc. (formerly TRW Information Services), Equifax, and TransUnion. These bureaus keep files on anyone who buys anything on credit, which includes nearly 90 percent of American adults.⁽¹⁹²⁾

Credit bureaus sell credit reports to credit grantors so that they can assess a consumer's willingness and ability to repay a credit grant. Businesses that grant credit, such as banks, retail stores, and credit card issuers, report the credit history of their customers to these credit bureaus.

For the consumer, the credit reporting industry does not provide competitive options. Credit reports about an individual are often maintained by more than one of the big three bureaus, and the consumer will only know which bureau possesses what information if he or she makes the effort to acquire his or her credit records. Within the industry, however, there is a great deal of competition among the large credit bureaus for the business of credit grantors.

The Fair Credit Reporting Act (FCRA) governs disclosure of credit information by credit bureaus.⁽¹⁹³⁾ Congress enacted the FCRA in 1970 to ensure that consumer reporting agencies provide consumer credit information only to businesses with a legitimate need for this information, and in a manner that is fair to the consumer with respect to the confidentiality, accuracy, relevancy, and proper use of such information.⁽¹⁹⁴⁾

The FCRA regulates the information that credit reporting agencies may maintain on consumers. For example, agencies must delete most adverse information from consumer credit reports after seven years.⁽¹⁹⁵⁾ The

FCRA also prohibits the production of reports on a consumer's character and reputation based solely on interviews, without disclosure to the consumer and other safeguards.⁽¹⁹⁶⁾ Furthermore, whenever a consumer is denied credit for personal, family, or household purposes, or is denied employment, and (in either case) the denial is based on information in a consumer report, the entity that received and used the report is required to notify the consumer and identify the consumer reporting agency in question.⁽¹⁹⁷⁾

The FCRA also requires consumer reporting agencies to provide consumers with information from their files; establish procedures for dealing with disputes about the completeness or accuracy of information maintained in their files, and take special precautions, when reporting public record information, to ensure the completeness and accuracy of that information or, in the alternative, to notify the consumer that such information is being reported.⁽¹⁹⁸⁾ Finally, the FCRA places some restrictions on the dissemination of credit information to third parties. For example, it provides that a consumer reporting agency may disseminate a report on a consumer only pursuant to a subpoena or court order; with the consumer's consent; or for use in connection with one of several enumerated purposes.⁽¹⁹⁹⁾

Early proponents of the FCRA had sought to limit the disclosure of confidential credit information to third parties, such as banks and other credit grantors, who needed access to this information to make credit granting decisions.⁽²⁰⁰⁾ As enacted, however, the FCRA requires only that credit bureau customers must have a permissible business purpose to purchase credit reports.⁽²⁰¹⁾ The FCRA defines permissible purposes broadly, encompassing employers, landlords, private investigators, and others.⁽²⁰²⁾ The scope of the permissible purpose language concerns many privacy advocates. According to one commentator, just one of the "big three" credit reporting agencies sells 500,000 records each day.⁽²⁰³⁾

Other commentators have criticized the FCRA for vague drafting, poor enforcement, obsolescence in the face of technological change, and lack of consumer education.⁽²⁰⁴⁾ Additionally, commentators have pointed out that only limited transactions are protected. For example, the FCRA does not cover exchanges of information involving business transactions, only those involving "consumer" oriented matters.⁽²⁰⁵⁾ In addition, the FCRA only applies to the items specifically enumerated in the statute, excluding from coverage items such as credit reports sought in connection with insurance claims.⁽²⁰⁶⁾

During recent years the credit reporting industry has come under increasing attack on consumer issues. In 1993, the Associated Credit Bureaus (ACB) adopted mandatory member policies to improve privacy, accuracy, and consumer relations issues.⁽²⁰⁷⁾ Additionally, the industry has recently acted to establish standards and procedures for the automation of consumer dispute verification⁽²⁰⁸⁾ and has created a specialized electronic mail network to speed resolution of consumer complaints about inaccurate personal information.⁽²⁰⁹⁾ In 1991 Experian (then TRW) agreed to a consumer credit information gathering and dissemination code in cooperation with a number of states. Equifax reached a similar agreement in 1992.⁽²¹⁰⁾

The industry has also adopted some voluntary privacy standards and mechanisms to correct erroneous personal information. For example, Experian adopted what it calls a "values approach" to guide decisions on how to use information.⁽²¹¹⁾ Equifax first created and published a code of fair information practices in the 1980s, and has recently updated that code.⁽²¹²⁾ Equifax has also conducted and published annual national surveys of consumer attitudes about privacy.⁽²¹³⁾ Furthermore, in 1990, Equifax responded to mounting

consumer and privacy concerns by establishing a toll-free number that consumers could call to order credit reports, obtain advice, and correct inaccuracies.⁽²¹⁴⁾

Notwithstanding these laudable efforts, complaints of damaging mistakes in credit reports and the release of names to marketers and others who do not meet the "permissible use" requirement under the FCRA continue to plague credit agencies.⁽²¹⁵⁾ "Prescreening" techniques now used extensively also generate many new privacy concerns.⁽²¹⁶⁾

In 1996, Congress adopted sweeping changes to the Fair Credit Reporting Act, to be effective on October 1, 1997.⁽²¹⁷⁾ The amendments establish opt-out requirements for prescreening, permit corporate affiliates to share information without becoming subject to the FCRA requirements, impose new obligations on creditors with respect to the accuracy of information furnished to consumer reporting agencies, establish new reinvestigation and notice obligations, and impose significant new consent requirements to obtain reports containing medical information and reports for employment purposes.

The 1996 FCRA Amendments also required the Federal Reserve Board to conduct a study, in consultation with the Federal Trade Commission and other banking agencies, of whether organizations that are not credit reporting agencies are making sensitive consumer identifying information available to the public. The Federal Reserve released the report on April 7, 1997.⁽²¹⁸⁾ The Report explains how information becomes available and discusses some aspects of financial fraud. Although it reaches no conclusions about whether legislation is needed at this time, the Report does indicate that fraud related to identity theft is a growing concern that is expanded by relatively easy access to personal information.⁽²¹⁹⁾

2. Movies

(a) Video rental record privacy. The Video Privacy Protection Act of 1988⁽²²⁰⁾ is a good example of the U.S. practice of enacting privacy legislation in response to dramatic instances of information misuse. Prior to its enactment in 1988, anybody could obtain a list of movies rented by a particular customer without that customer's permission. Congress passed legislation to protect video records only after a Washington newspaper published Judge Robert Bork's video rental history following his nomination to the U.S. Supreme Court.⁽²²¹⁾

Today Americans are free to watch rented films in the privacy of their own homes without fear that their video rental records might be disclosed to the public. A video store that knowingly releases a customer's rental information or video purchases is liable for damages to that customer.⁽²²²⁾ There are logical exceptions to this rule, however. Video stores may, of course, release rental records with a customer's consent.⁽²²³⁾ Law enforcement agencies may obtain this information pursuant to a search warrant, court order, or grand jury subpoena.⁽²²⁴⁾

(b) Cable movie records. Pay-per-view cable might be viewed as the online counterpart of video rental shops. But a different privacy standard applies to cable movie rental. Under the Cable Communications Policy Act (CCPA),⁽²²⁵⁾ enacted to establish a cohesive national cable communications policy and to set guidelines for the cable television industry, cable subscriber information may be disclosed to a government entity only pursuant to a court order,⁽²²⁶⁾ a higher hurdle than obtaining the grand jury subpoena necessary to obtain video rental records.

Cross-sector inconsistencies exist as well. For example, the CCPA protects personally identifiable information, including lists of names and addresses on which the subscriber is included.⁽²²⁷⁾ The rationale:

Cable systems, particularly those with a "two-way" capability, have an enormous capacity to collect and store personally identifiable information about each cable subscriber . . . subscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions.⁽²²⁸⁾

Although this statement is undeniably true, telephone billing records may similarly reveal intimate information about an individual (e.g., phone calls to a psychiatrist's office on a regular basis). One might expect similar standards to govern access to these records. Yet phone records are accessible with grand jury subpoenas; cable records require a court order.

The Act restricts the ways in which cable companies may collect, retain, and disclose personally-identifiable subscriber information, and requires industry to inform consumers of their rights and available remedies. The Act allows cable operators to disclose the names and addresses of subscribers as part of a mailing list if they have given subscribers the opportunity to prohibit such disclosures and the mailing lists do not reveal the nature or extent of subscribers' uses of services.⁽²²⁹⁾

The privacy provisions of the Cable Act apply only to cable-based communications--not to direct broadcast satellites and wireless transmissions. Thus, whether there are restrictions on the use of data, and whether the consumer has the right to opt-out, is determined by the type of technology used to transmit information, rather than the type of information being gathered.

3. Direct Marketing

The direct marketing industry has been a prime beneficiary of the technological advances in information processing. According to one industry commentator "the database revolution is the most significant recent arrival in the direct marketing industry...."⁽²³⁰⁾ New technologies that process, manipulate, combine, and exchange personal data both quickly and economically allow industry to target goods and services to consumers in new ways. Implementation of the NII will create even more opportunities to combine and exchange personal data as well as provide additional avenues for communication with prospective customers.

Direct marketing accounts for \$350 billion dollars in sales annually.⁽²³¹⁾ About half the people in the U.S. now shop by mail.⁽²³²⁾ Target marketing increases the likelihood that catalogs and other promotional material will end up in the hands of consumers who are genuinely interested in these materials. Industry and consumers gain: customer service can be improved by target marketing, shoppers are offered extended shopping hours and immediate delivery, and marketers save money by sending marketing materials only to

those consumers most likely to be interested in the advertised product.

But the proliferation of databases and lists of consumers they produce also implicates personal privacy.⁽²³³⁾ By collecting information regarding consumer preferences and purchases, marketers ultimately have possession of a person's name, address, buying habits, and other individual social and economic data. Individuals have no legally enforceable right to be notified when marketing data is collected, who has the data, who has organized it into lists, and with whom such personal data is being shared. No law prohibits the use of information gathered for one marketing purpose for any other purpose, compatible or not.

The leading consumer complaints about the direct marketing industry concern unsolicited mail and telephone calls.⁽²³⁴⁾ Consumers often complain about receiving flyers from stores never shopped in, catalogs from mail order companies never ordered from, and banks and card companies never communicated with.⁽²³⁵⁾ This problem appears to stem from the use of personal information by third parties, such as database compilers, credit reporters, or credit-card issuing banks.

The direct marketing industry has worked for years to balance consumer privacy concerns with its use of consumer data.⁽²³⁶⁾ The Direct Market Association (DMA)⁽²³⁷⁾ has, for example, established an ethical code and guidelines for self-regulatory action, and may refer members found in violation of the code to its ethics group or can suspend membership in the association.⁽²³⁸⁾ The DMA sponsors a Mail Preference Service (MPS) and a Telephone Preference Service (TPS) to handle, on a national level, unsolicited junk mail and telemarketing. Both are designed to help consumers decrease the amount of commercial and non-profit mail and commercial telephone calls they receive at home.⁽²³⁹⁾ Beyond the MPS and TPS, the DMA recommends that individual companies give consumers an opportunity to opt out of the exchange of marketing data through in-house suppression programs and disclosure notices.⁽²⁴⁰⁾

The DMA encourages its members to adopt its corporate information policies and programs to respond to consumer privacy sensitivities. Adoption of and adherence to the DMA's recommended privacy practices is currently voluntary for its members. Furthermore, not all direct mailers are members of the DMA. Nonetheless, many direct mailers have adopted individual privacy codes tailored to the DMA's recommendations, and DMA continues to update its guidelines to keep pace with digital technology.⁽²⁴¹⁾

While acknowledging the usefulness of self-regulation, some commentators have expressed concern about whether self-regulation adequately safeguards privacy. Others wonder whether the DMA does (or can) effectively enforce its fair information codes. For example, the fact that adherence to DMA's recommended privacy practices is voluntary has led one commentator to state that "[t]he only rules which limit the use of the most personal information by direct marketers are the rules which the marketers voluntarily choose to follow."⁽²⁴²⁾ Concerns have also been raised about whether information brokers will adhere to DMA's recommended practices. Indeed recent news reports illustrate these concerns.⁽²⁴³⁾ DMA is taking steps to address these criticisms. For example, it recently began digesting the existence and outcome of investigations and compliance hearings, and had upgraded its World Wide Web site to facilitate online development of compliant privacy policies.⁽²⁴⁴⁾ In November of 1996, DMA initiated a major education effort for DMA members and for consumers.⁽²⁴⁵⁾

The Federal Trade Commission (FTC) has recently assumed a key role in the privacy arena and indeed has

been identified as the most privacy active agency.⁽²⁴⁶⁾ The FTC's Bureau of Consumer Protection undertook a Consumer Privacy Initiative in 1995 to educate consumers and businesses about the use of personal information online. As part of this initiative, the Commission held several informal workshops and engaged in a series of discussions with privacy advocates and industry representatives. On January 6, 1997, the FTC issued a staff report entitled *The Public Workshop on Consumer Privacy on the Global Information Infrastructure*, concluding that notice, choice, security and access are recognized as necessary elements of fair information practices online.⁽²⁴⁷⁾

The FTC report highlights the potential for technological solutions, combined with self-regulation, to address online privacy concerns. The Bureau of Consumer Protection also devoted special attention to issues raised by data gathered from and about children online.⁽²⁴⁸⁾

The FTC has announced that it will hold a follow up workshop in June of 1997 to ascertain the status and effectiveness of self-regulatory and technological approaches to privacy protection. In the meanwhile, the Commission already has broad discretion to prosecute instances of misleading or unfair commercial practices. This authority extends to misleading or unfair practices involving the collection and re-use of personal data by third parties.

In a related development, by letter dated October 8, 1996, Senators Bryan, Hollings, and Pressler asked the FTC to investigate and report on the non-consensual compilation, sale, and usage of electronically transmitted data bases.

SUMMARY

Privacy is a core American value. Americans also value the free flow of information. In the United States we analyze and balance these sometimes competing values on a sector by sector basis, calibrating the balance point to fit a particular set of circumstances. As a result, protections vary from sector to sector. For example:

Federal law regulates the government's collection, use, and distribution of a significant amount of personal information. These protections are fairly comprehensive, although critics cite inadequate enforcement and note that the scope of protection may not be keeping pace with technology.

It is generally against the law to intercept the content of any communication without consent or specific authority. The 1996 Telecommunications Act extends comprehensive protection to transactional data held by common carriers. Online service providers and Internet access providers are not currently regulated by statute, but many contract with subscribers to provide privacy protections. In this area, the market appears to be providing a range of consumer choice.

Medical records are largely unprotected by federal law, governed traditionally by codes of professional conduct. But doctor-patient confidentiality safeguards may well be inadequate as cost containment pressures force the health care industry to maximize information technology use. Legislation passed in the 104th Congress, however, will produce important recommendations for comprehensive protection of medical

records and will lead, at a minimum, to enforceable protection for medical records transmitted for insurance claim administration.

Consumer privacy safeguards are much less predictable in the commercial marketplace. Federal law governs use and disclosure of credit information by credit agencies. The same information is unprotected in other hands. Traditional notions about financial privacy have limited disclosure of banking information in the past, but may not be adequate in the current marketing environment. Some lifestyle information, like video or cable viewing habits, are protected by law, while other lifestyle data is not protected. The direct marketing industry appears to be responding to consumer demand for adoption and enforcement of fair information practices involving notice, choice, access and security. The FTC is monitoring this response.

Critics of U.S. data protection policy tend to identify several structural characteristics of our approach as troublesome:

- (1) The sectoral approach protects privacy on a piece-meal basis. As a result, privacy rules are neither consistent nor predictable from sector to sector. This imposes compliance burdens on industry, and makes it more difficult for consumers to anticipate how their personal information will be used in any particular setting.
- (2) No federal agency currently has privacy as its primary, much less its only, mission. This means that privacy must compete, in terms of budget and staff resources with the other responsibilities of these agencies. It also means that our international trading partners have a harder time identifying the proper forum to raise concerns about privacy and transborder data flows.
- (3) No federal agency is responsible for articulating privacy values on an ongoing or proactive basis. Legislation is traditionally remedial in the United States, and government tends to intervene only when a specific problem is identified. Legislative solutions in the privacy area, moreover, tend to be narrowly tailored to deal with a specific type of information maintained by a particular sector of the economy.
- (4) No federal agency coordinates government privacy initiatives. Some privacy concerns are not within any particular agency's purview. Other areas of privacy straddle one or more agencies. Also, in the absence of overriding federal legislation, privacy concerns are often addressed by the fifty individual states either through laws or constitutional protections. Some states have been aggressive in this arena,⁽²⁴⁹⁾ but privacy protection varies widely from one state to another. This creates difficulties for businesses operating in today's networked environment, where transfers of personal data across state lines are commonplace.
- (5) Self-regulatory efforts are laudable, but unenforceable. Some segments of the private sector have taken affirmative steps to address privacy issues arising in the modern networked environment by adopting voluntary codes of conduct. Yet, unsolicited mail and telephone calls continue to be a major source of consumer dissatisfaction. Likewise, while major credit bureaus have adopted voluntary privacy standards, the credit reporting industry continues to be a leading source of complaints to the Federal Trade Commission.⁽²⁵⁰⁾ In any event, voluntary codes provide very little by way of judicial, or quasi-judicial, redress. Moreover, the codes are almost always voluntary, so non-compliance has little consequence. As with legislative responses, changes in private sector practices often occur only in response to some precipitating event.⁽²⁵¹⁾

But the current approach to data protection in the United States has admirers as well. Supporters of the sectoral approach remind us of several of its virtues:

- (1) The sectoral approach is more effective than an omnibus approach. One-size-fits-all privacy policies will inevitably constrain innovation and reduce competition, at the expense of the consumer.
- (2) Privacy is only one of a number of important policy issues. There is no reason why it should not compete with priorities for its share of budget and human resources. Moreover, the fact that several agencies may have authority or responsibility for privacy protection may result in healthy inter-agency competition to "do the right thing."
- (3) Our approach to privacy may have some inefficiencies, but it does avoid burdensome over-regulation. The reactive, rather than anticipatory, approach to privacy is consistent with our approach to lawmaking in other areas.
- (4) The status quo is anything but static. Awareness of and attention to privacy issues have risen dramatically in recent years, and real progress is being achieved. It's not clear what additional federal coordination would contribute to this process.
- (5) Self-regulatory efforts can work, and industry has demonstrated an admirable commitment to enhanced self-regulation. In recent months industry has also invested in the development of powerful technological tools to make the fair information principles of notice and choice a reality for consumers.

V.

OPTIONS FOR PROTECTING INFORMATIONAL PRIVACY ON THE NII

In the previous Section of this paper, we identified a number of places where the U.S. approach to information privacy embodies trade-offs that may have been acceptable in a world of physically discreet paper records. The consequences of these same trade-offs may prove too costly in the global, digital environment, however.

Thus, we turn to the core question: what is the best way to implement fair information practices in both the public and the private sector in order to better balance the needs of government, commerce, and individuals in the Information Age, keeping in mind both the interest in the free flow of information and the protection of informational privacy? This Section explores a number of alternative approaches to address the substantive and structural problems identified in Section III.

We could, at one end of the spectrum, continue to rely primarily on the current mix of policy and legislative initiatives to implement the Privacy Principles or similar articulations of fair information practices. Within this framework, there are a number of options for government activity that might enhance the success of industry-led, market-based approaches to fair information practices without undermining the core virtues of our sectoral approach to privacy protection.

At the other end of the spectrum, the federal government could establish a central government authority to

impose uniform privacy regulations based on the Privacy Principles (or another set of principles) across all sectors of the economy and enforce these regulations vigorously. Within this framework, there are a number of forms that such an entity might take.

We address both ends of the spectrum in turn, but urge readers to consider the entire range of options between them, for there is not any bright line that arbitrarily divides alternatives.

AN ENHANCED SECTORAL APPROACH

Most advocates of the sectoral approach to privacy protection concede that there is room for improvement. They believe, however, that the sectoral approach is fundamentally sound and should be preserved, but made to operate in a more cohesive fashion. Specifically, a decision to maintain a sectoral approach to privacy protection does not mean taking no new action. As set forth throughout this report, both the public and private sectors are responding to growing public concern about new threats to privacy. Solutions are on the horizon, or at least have been identified, for many of the substantive inadequacies of U.S. data protection policy.

Congress, for example, is debating several statutory solutions to problems associated with medical information, the collection of data from and about children, communications privacy, and consumer privacy issues arising, or expected to arise, in connection with electronic commerce. At the direction of Congress, an HHS Task Force is currently developing recommendations for comprehensive protection of medical records.

The President's Office of Consumer Affairs (OCA) has been active in educating the public about a variety of privacy issues and was instrumental in establishing the Privacy Working Group of the IITF. In addition, OCA has worked with industry to preserve consumers' privacy and control over the use of their personal data while encouraging both growth and innovation in the use of telecommunications and information management technology.⁽²⁵²⁾ Recently, the newly appointed director of OCA, Leslie Byrne, announced that consumer privacy issues would be a primary focus of her office in the Clinton Administration's second term.⁽²⁵³⁾

Several organizations have announced and demonstrated technology that consumers can use, or will soon be able to use, to protect their personal information online. Trade associations representing the advertising, marketing, and online service industries have announced new or revised privacy codes and consumer education programs for the information age. The FTC has indicated that it will monitor consumer privacy concerns, as well as the implementation of technological and self-regulatory tools to respond to consumer concerns.

Similarly, NTIA recently issued a White Paper on telecommunications privacy, and is now meeting with telecommunications providers to assess adherence to the privacy principles outlined in that paper. NTIA plans to report its findings, and to recommend statutory or regulatory changes if needed to ensure compliance. NTIA, with the Department of State, is also holding discussions with the European Union on the EU Directive. Finally, NTIA is evaluating a number of papers to identify the constellation of characteristics and circumstances that produce effective self-regulation.

Why are such initiatives under way now? There are probably a number of explanations for this phenomenon.

Now that the ease with which the NII allows data to be collected, distributed and analyzed has become clearer, there is greater demand for privacy enhancing products and policies. This can be viewed as an example of the free market in operation. In the Information Age, privacy may become a market commodity. Given adequate levels of consumer and government awareness, demand for privacy protection could continue to increase and a robust, competitive market for privacy protection could develop. Under this scenario, the market itself could protect privacy on a sectoral basis without the inevitable duplication of sectoral expertise required to administer government programs.

Government could facilitate the development of a marketplace for privacy in four distinct ways. First, the government could formally adopt the Privacy Principles. The Privacy Working Group issued its Principles for Providing and Using Personal Information nearly two years ago. To date, neither the executive or legislative branch has formally adopted them as official policy. An obvious first step is to do so.

Thus, the Office of Management and Budget might consider whether to direct all federal agencies to incorporate the Principles in their information management and procurement practices. In addition, the Administration could consider using its powers of persuasion to encourage state, local and tribal governments, as well as business leaders, to adopt and implement information practices that recognize the rights and responsibilities set forth in the Principles.

Congress might also consider formal adoption of the Privacy Principles as part of omnibus privacy legislation, in connection with agency specific legislation, or in the form of legislative resolutions. For example, Congress might direct the Federal Trade Commission to undertake rulemaking to ensure that the collection and use of personal data in the commercial setting occurs in a manner that comports with the core elements of fair information practices: notice, choice, access and integrity.

Second, the government could get its own house in order by ensuring that government data collection remains consistent with the Privacy Principles in the face of changing technology. The Office of Management and Budget, Office of Information and Regulatory Affairs (OIRA) has statutory responsibility with respect to the Privacy Act, the Paperwork Reduction Act and the Freedom of Information Act, for example, and might consider reviewing these statutes in light of the Privacy Principles. OMB could report its findings and recommend legislation, regulation, administrative action, or executive orders as appropriate to solve any problems it discovers. This kind of review could provide a model for the private sector organizations to undertake similar audits.

Recently, a number of federal agencies, including HHS and the IRS have established privacy offices. One option would be to expand this practice government wide and establish a formal Privacy Advocate in each agency to consider the privacy implications of particular public or private sector practices. An inter-agency committee of privacy advocacy offices could facilitate interagency coordination and cooperation on privacy-related issues as they arise. There is ample precedent for such councils: for example, the Office of Management and Budget administers a Chief Information Officer Council; likewise, the Office of Consumer Affairs chairs the Consumer Affairs Council, an inter-agency committee of consumer affairs officers.

Third, government could play a larger role in consumer and business education. Agencies could act as "bully pulpits" to raise consumer and business awareness of the issue. Consumer education is likely to raise demand for information privacy protection to its optimal level. Business education is also necessary to introduce technology entrepreneurs to consumer protection theory, which in turn could help industry anticipate the privacy implications of a new product. Government could also continue to facilitate dialogue among industry

representatives and consumer advocates that lead to early identification of emerging issues and that foster joint efforts to address privacy concerns as they arise. The expense associated with consumer and business education would be minimized if the industries that will benefit most directly from increased consumer confidence in the NII were to accept some responsibility for this program.

Fourth, government could enhance self-regulation by exploring enforcement deficiencies with industry. This would address the most oft-heard complaints about self-regulation; that industry codes of conduct are praiseworthy, but largely unenforced. Industry often responds that U.S. competition law limits their enforcement efforts. One option is to ask the anti-trust enforcement agencies, in conjunction with consumer protection agencies, to consider whether, and how, competition policy undermines privacy enforcement activities. Government and industry could then work together to resolve any conflicts between consumer protection and competition values raised by strong enforcement of self regulatory regimes.

Much can be done following this approach, but it may be viewed by some as little more than the status quo in a new package. For example, the increased legislative activity, while appropriate, is reactive. So too, the steps the government could reasonably take to protect privacy (i.e., getting its own house in order, playing a larger role in consumer and business education, and enhancing self-regulation by exploring enforcement deficiencies with industry) are all steps that could have been taken years ago. The sectoral approach, even enhanced, may continue to produce inconsistent privacy protections, or fail to anticipate future developments in a comprehensive, thoughtful way.

Continued reliance on the incremental, responsive mix of public and private action involves acknowledging that no agency has privacy as its primary mission. Privacy issues would continue to be one of many issues for which a particular agency is responsible. But, is it necessarily inappropriate for a policy concern such as privacy to compete, in terms of budget and staff resources, for government and industry attention? Such competition may minimize the threat of over regulation, ensuring that resources will not be devoted to problems that are merely theoretical. Moreover, allowing privacy to compete with other policy priorities makes it more likely that government will not intervene until there is clear evidence of a market failure -- a situation where government intervention is necessary to achieve an important policy objective that the unregulated marketplace cannot provide. Finally, the existence of a separate government entity to address privacy would not isolate it from the annual authorization and appropriation process, in which it would compete with other public priorities as a matter of course.

Reliance on an enhanced sectoral approach would also mean that no single federal agency would be responsible for articulating privacy values on an ongoing or proactive basis. New data technology, or a particular information practice could become prevalent without any consideration of privacy values. While it is costly and controversial to eliminate commercial practices that are already widely deployed, preventative privacy might find no champion without a federal agency to articulate privacy values.

Although market forces undoubtedly have played and will continue to play a critical role in protecting

privacy, relying too heavily on market forces is arguably a mistake in the privacy area, where externalities and/or inadequate information are likely to exist, or in cases where the consumer is not in an equal bargaining position with industry.⁽²⁵⁴⁾ Some argue that free market forces will not discipline commercial practices in the many instances when there is no relationship between the consumer and the private sector entity collecting or using personal information. For example, individuals cannot choose which credit bureau will maintain their credit report. And few consumers have even heard of the Medical Information Bureau. Neither education nor market forces are of much help here--a person suffering from cardiac arrest needs immediate medical care; there is not time to negotiate with the ambulance attendant over whether the hospital's records will be referred to the MIB.

Finally, none of the options described above facilitate better understanding of sectoral practices by extra-sectoral players, either domestic or international. In the absence of a centralized information resource, both governments and individuals will continue to experience difficulties finding the right place to resolve any particular set of privacy concerns. This is particularly troublesome in the inherently borderless domain of electronic commerce.

CREATION OF A PRIVACY ENTITY

As we have observed, the United States lacks a centralized entity either to (1) drive development of Federal data privacy policy, or (2) direct traffic for the various privacy initiatives now underway. One option is to create a federal privacy entity to achieve and maintain the optimal balance between the benefits and harms associated with the unrestrained flow of personal data in the information age.

Federal entities come in a variety of sizes and shapes, and perform a range of functions -- from providing advice, education, advocacy, coordination and representation through promulgating and enforcing regulations.

Such entities can be located in existing agencies, or newly created agencies. Alternatively, they can rely on government staff resources exclusively, or include private sector representatives.

In the following section, we examine the pros and cons of a number of possible combinations of the factors listed above. We assume, throughout the discussion that follows, that the jurisdiction of any such entity would encompass private sector data use. Such an entity would also have responsibilities for informing, coordinating, or directing government data practices in accordance with applicable law. The goal of a privacy entity would be to implement the Privacy Principles (or a similar articulation of fair information practices) at the national level. Its methods of achieving this goal would depend, of course, on the tools it is given to do this job.

Readers should keep in mind that we have not attempted to identify every possible combination of responsibilities, sphere of influence, placement, and authority that a federal privacy entity might possess. The discussion that follows is intended to be illustrative rather than exhaustive, and to spark discussion rather than to curtail it.

1. Creation of a Federal Entity with Regulatory Authority. —

Regulatory bodies are established to respond to complex issues of national importance. Typically, regulatory entities operate as quasi-legislative, quasi-judicial organizations empowered both to promulgate and enforce rules governing conduct within their sphere of jurisdiction.

Regulatory agencies may exercise broad powers. They are able to initiate, monitor, and coordinate the regulation of one or more sectors of the economy based on detailed experience with its particular characteristics. They control private conduct by promulgating and implementing regulations and by imposing sanctions on those who violate such rules and regulations. Often regulatory agencies are authorized to investigate and disclose information about private actors. Their sphere of influence may extend to both the public and private sectors as well as to the domestic and international arenas.

There are some regulatory agencies known as "independent agencies" that are isolated from the integrated administrative structure of the executive branch.⁽²⁵⁵⁾ Neither the President nor any cabinet secretary has direct supervisory authority for such agencies. Independent regulatory agencies are generally headed by three or more commissioners or board members, appointed by the President and confirmed by the Senate for fixed terms. Typically, such members may be removed from office only for cause.⁽²⁵⁶⁾ To further isolate independent agencies from political influence, membership qualifications or the partisan political balance of the agency may be established by law. Although agency adjudications are subject to judicial appeal, an independent regulatory agency is generally free to set its own agenda within the constraints of its organic statute.

Regulatory agencies may be placed within executive branch departments but remain "independent" if the head of the agency can not be terminated at will. The Federal Energy Regulatory Commission, for example, resides within the Department of Energy.⁽²⁵⁷⁾

Executive branch regulatory agencies also have broad powers to establish rules of conduct applicable to particular sectors. Executive branch agencies are less isolated from political pressure, however, because the agency head may be removed from office by the President at will. Executive branch agencies may be established by Congress, as well as by executive order, presidential reorganization plan, or departmental order so long as it is based on the requisite legislative imprimatur.

Regulatory agencies -- independent or otherwise -- are powerful and have the ability to change practices swiftly through rulemaking and adjudication. Creation of a regulatory agency to deal with privacy concerns is likely to respond to many of the objections listed in Section IV. It would reflect an omnibus rather than a sectoral approach to privacy, and would establish privacy as one of the primary missions of a federal agency. Such an agency's regulatory mandate would likely be proactive, based on a legislative articulation of fair information practices. Regulatory agencies usually have adequate tools, especially adjudicatory tools, to enforce regulations within their jurisdiction. Finally, especially in the case of an independent agency, the entity would have some protection from the ebb and flow of politics.

On the other hand, there are several significant drawbacks to creation of a new independent regulatory agency.

First, a centralized approach is inconsistent with our traditional sectoral approach to privacy protection. A one-size-fits-all alternative may not be sufficiently responsive to the sector specific implication of a particular information practice. Privacy today has become a complicated matter and is expected to become

increasingly so with the continued expansion of the GII. Different areas of information privacy raise very different concerns and priorities. They also require different types of expertise to address them in a meaningful manner. The agencies currently involved with privacy issues are dealing with specific areas of privacy that these agencies are uniquely qualified to handle (e.g. privacy issues arising in consumer transactions, in telecommunications, in law enforcement, in government records, etc.).

Second, independent regulatory authority is already vested in and exercised by a number of federal bodies. For example, the FTC's mandate is to protect consumers against unfair and/or deceptive commercial practices. The FCC has regulatory authority with respect to telecommunications, just as the Federal Reserve has rulemaking authority with respect to banking matters. Creating a separate privacy entity could produce confusing overlap, possible duplication of efforts, or even inconsistent rules and regulations.

Third, regulatory agencies with quasi-judicial and quasi-legislative authority tend to be expensive, and there is no reason to believe that this would not be the case here. Complex information issues arise across an increasingly diverse range of the public and private sectors. As such, a privacy entity tasked with regulating the privacy universe might be called upon simultaneously to regulate banks (because of financial records), private mail services (because they may possess transactional data), the telecommunications industry (because of electronic surveillance), the medical community (because of medical records), and catalog companies (because of targeted mail and transactional data). It would take a significant -- and expensive -- bureaucracy to carry out such a mandate.

A somewhat less costly alternative might be to house broader privacy responsibilities in one or more existing independent agencies. Some of these agencies are already involved with a variety of privacy issues both in-house and in interactions with the private sector and the international communities. As such, these agencies already have some knowledge of, and experience in, dealing with certain kinds of privacy issues. Additionally, it may well be easier and less costly to create an entity within an already existing organizational framework.

Placement of a privacy entity in an existing agency, however, has an additional drawback. No existing federal agency is dedicated exclusively to, or focused exclusively on, privacy; indeed, their primary mission is something other than privacy. As such, privacy would have to compete with other agency priorities for funding and personnel. The competing responsibilities of the larger organization could well dilute the effectiveness of the privacy entity.

Fourth, creation of a privacy entity with significant regulatory authority goes against the grain of a smaller government that is favored by the American public today. As President Clinton and Vice President Gore stated in connection with the National Performance Review:

The answer for every program cannot always be another program or more money. It is time to radically change the way the government operates -- to shift from top-down bureaucracy to entrepreneurial government that empower citizens and communities to change our country from the bottom up.⁽²⁵⁸⁾

Creation of a new government agency with regulatory authority is the antithesis of bottom up governance, and its likely that any effort to create a new regulatory body to enforce fair information practices would face considerable public resistance at this time.

2. Creation of a Federal Entity without Regulatory Authority

Several of our trading partners have demonstrated that a privacy entity need not have regulatory authority to be effective.

Non-regulatory agencies can be created either through Congressional action or by Executive Order. For example, the United States Office of Consumer Affairs (OCA) was created by Executive Order.⁽²⁵⁹⁾ The National Telecommunications and Information Administration (NTIA) as originally created by Executive Order to serve as the Executive Branch agency responsible for advising the President on telecommunications policies.⁽²⁶⁰⁾ Both the Office of National Drug Control Policy and the Domestic Policy Council were originally created by Executive Order.⁽²⁶¹⁾

There is a great deal of flexibility with respect to the functions that such agencies may perform, their placement in the government, and the formalities needed to establish such entities.⁽²⁶²⁾ Non-regulatory agencies reside either in the Executive Office of the President or in an existing executive branch agency, although in some cases they have been established in the legislative branch.⁽²⁶³⁾ A federal agency could have as much or as little independence as Congress or the President were willing to bestow. Likewise, the size of such an agency could be tailored to the functions assigned to it. This flexibility probably decreases the time needed to get such an entity operational.

Even without regulatory authority, federal offices can be quite influential. An entity with advocacy, ombudsman, representational, coordination and/or advisory responsibilities could still contribute significantly to the debate about information privacy in the digital environment. The "bully pulpit" role can extend to the private sector and into the international arena as well. Moreover, when an entity is established to serve as a focal point for government action in an area of serious public concern, it can be well positioned to achieve uniformity of approach among disparate agencies and to provide a single point of contact in the United States for dealing with state and foreign governments as well as international organizations.

On the other hand, offices created by Executive Order can be eliminated or moved to less visible positions as easily as they can be created. Lacking *de jure* authority, the influence of an office is dependent on the office-holder's connections with the President. And where office holders are appointed by and accountable to the President and serve at the pleasure of the President, they may be seen as lacking sufficient independence.

A non-regulatory privacy entity could have all, or some, of the functions described below.

Coordination. A privacy entity could coordinate domestic privacy policy as it applies to the public sector, the private sector, or both. A privacy coordinator could be tasked with ensuring that federal agencies protect privacy in consistent ways with respect to data held by the government. For example, many federal agencies collect debts owed to the government, an activity that relies on significant information about an individual's location and assets; a coordinating entity could ensure that agencies collect debts in ways that reflect an appropriate respect for privacy. A federal privacy coordinator might also have the task of coordinating federal agency privacy initiatives that affect the private sector to avoid duplicative efforts or unnecessary burdens on the privacy sector. In this task, a privacy coordinator might also help to ensure that important problem areas do not fall between the cracks at the federal level.

There appears to be little down-side to better coordination of privacy initiatives at the federal level, although coordination could probably be improved without creating a new entity.

Representation. A federal privacy entity might also represent the President's views on privacy both domestically and internationally. Domestically, a federal representative or spokesperson might work with state and local government representatives. Likewise, a privacy spokesperson could serve as the U.S. representative in international privacy disputes. This might help alleviate a current deficiency cited by numerous countries and international organizations: the lack of a single U.S. point of contact on privacy matters. Currently, if a foreign office wants to understand U.S. privacy policies, it must query literally dozens of federal agencies. A federal privacy representative could serve as a centralized location to which foreign governments could look when dealing with information privacy issues, which might well facilitate international relations with respect to transborder data flows.⁽²⁶⁴⁾ Finally, a privacy representative could fulfill a public speaking role to raise awareness of and promote the use of fair information practices in the public and private sectors.

Again, there appears to be little down-side to more coherent representation in addressing this increasingly global issue.

Advocacy. A federal privacy advocate might be given broad authority to advocate and promote the use of fair information practices by federal, state, and local governments, and the private sector. A number of our trading partners have adopted this approach by establishing data commissioners. A federal privacy advocate would have responsibility for articulating the privacy implications of proposed policy or legislation and would be, in effect, a privacy lobbyist. In the course of investigating citizen complaints, data commissioners typically perform a range of functions, including advocacy. For example, some conduct audits, provide advice to business and government, and make recommendations for improved data protection techniques.⁽²⁶⁵⁾ As advocates, the data commissioners might be called upon to testify about proposed regulations and legislation that will impact privacy values.

One drawback of this approach, however, is that industry might perceive a privacy "advocate" as having a predetermined bias in weighing privacy values with data flow values. This perception might diminish industry's recently demonstrated willingness to exchange ideas and information freely with federal representatives and privacy advocates.

Ombudsman. A federal privacy entity could itself act as the plaintiff's lawyer for a citizen whose privacy has been unfairly or unreasonably invaded. It could press individual cases or litigate on behalf of groups that have been harmed.⁽²⁶⁶⁾ In fulfilling an ombudsman function, the entity might simply advise parties on how to resolve their dispute, act as a prosecutor, or be the actual decision maker (as in binding arbitration). Again, our trading partners have followed this model where data commissioners act as agents of the legislature, and mediate relations between data subjects and data users.⁽²⁶⁷⁾

In a country with the population of the United States, the number of anticipated complaints would be extremely high, and the ombudsman role, if not limited, could quickly absorb all the resources of a privacy entity. Even if the entity could choose which disputes to handle, the mere processing of the requests would likely be time consuming and costly. Additionally, any entity that precluded or decreased access to the courts runs contrary to the U.S. tradition of self-help and judicial enforcement and could well prove counterproductive by reducing the likelihood that unfair information practices are prosecuted.

Advice. A privacy entity could perform an advisory function in the public sector, the private sector or both. Such an advisory role could be confined to coordinating domestic policy or could extend to the international arena. Advisory commissions can be composed of governmental or non-governmental representatives who are tasked to study a particular federal issue. They may be temporary or permanent. At the government level, advisory committees often consist of a special purpose inter-agency task force, consisting of representatives of agencies that play a major role in the development and implementation of federal policy in a particular area. The President's Information Infrastructure Task Force is an example of this type of advisory organization. To the extent that specific issues can be identified for inter-agency consideration, interagency task forces can be effective.

Education. A privacy entity could be created to conduct (or fund) research designed to assist policy makers and educate consumers and businesses about personal privacy. Such an entity might issue periodic reports on the state of privacy in the United States and propose solutions for any problems identified. Most privacy organizations in other countries prepare such reports. For example, the French National Commission on Informatics and Freedoms submits an annual report to the President and to Parliament. The Data Protection Commission in Germany publishes an annual report to the national legislature, and the British Data Protection Registrar reports annually to the House of Commons.

Public education efforts, aimed at both business and consumers, might facilitate a market-based response to those who ignore reasonable consumer expectations about the use of personal data. And, in the event that market based solutions fail, the research would be available to inform the development of legislative or regulatory responses.

Education and research efforts of this sort are both useful and worthy. But it must be recognized that agencies with privacy responsibilities are already undertaking research of this sort to fulfill their statutory obligations. For example, the FTC's Privacy Initiative has, to date, involved a significant research and education function. With this research in hand, the FTC is in a better position to pursue its consumer protection mission in cooperation with business and consumer advocates. Likewise, the NTIA is currently collecting valuable information about effective self-regulation that will inform government privacy policy in the telecommunications sector. A centralized privacy think tank would likely duplicate or replace research and education programs currently underway. To the extent that additional funding and personnel are devoted to privacy, they may be better applied to roles not currently filled by government agencies with specific sectoral responsibility and expertise.

3. Creation of a Non-Governmental or Advisory Entity

As discussed above, a privacy entity could perform an advisory function in the public sector, the private sector, or both. One advantage of advisory entities is that they may utilize private sector expertise that would not otherwise be available to the government. Several examples demonstrate the broad and varied role of federal advisory bodies today.

The U.S. Advisory Commission on Intergovernmental Relations (ACIR) is an example of a long-lived advisory commission. ACIR, an independent, bipartisan intergovernmental agency, was established by Congress in 1959 to identify emerging issues, trends and turning points in intergovernmental relationships, to

stimulate discussion about these issues, and to educate leaders and the public for the purpose of promoting stronger intergovernmental communication, cooperation and coordination. To this end, in accordance with its authorizing legislation, ACIR convened government officials and private citizens, monitored events in the federal system, provided technical assistance to the executive and legislative branches, and recommended changes in law and regulation to improve intergovernmental relations. ACIR's funding came from Congressional appropriations, state government contributions, the sale of Commission reports, and intergovernmental contracts.

Alternatively, temporary advisory committees may be established under the Federal Advisory Committee Act.⁽²⁶⁸⁾ FACA bodies provide advice and recommendations to the Executive branch with respect to specific issues of importance.⁽²⁶⁹⁾

The National Security Telecommunications Advisory Committee (NSTAC) was created in 1982 to advise the President on national security/emergency preparedness telecommunications (NS/EP) matters. Its membership consists of 30 appointed industry leaders representing major carriers, information service providers, manufacturers, electronics firm, and aerospace firms. The NSTAC's principal working body, the Industry Executive Committee, supervises subgroups that address specific issues in more detail. The NSTAC works in conjunction with the National Communications System (NCS). The NCS is comprised of 23 federal departments and agencies and is the government equivalent of the NSTAC. The NCS has a small permanent staff that functions as the Executive Secretariat for the NSTAC. The two organizations can coordinate their activities to ensure both public and private sector coverage.

Advisory bodies are generally quite independent, which gives them greater credibility with the public. For example, the Committee members often represented very disparate but strongly held views. Based on their composition and expertise, such committees' spheres of influence can extend to both the public and private sectors. This type of entity can be quite effective in facilitating dialog among interested parties. For example, NSTAC has been extremely effective addressing telecommunications security issues by opening lines of communication between government and industry.⁽²⁷⁰⁾ Also, costs are generally quite limited.

Both the public and private sectors may view an advisory board as less intrusive, and therefore more acceptable, than a regulatory agency. Additionally, if the board is structured to offer advice across a broad spectrum in both the public and private sectors, it is less likely to be viewed as a spokesperson for any particular interest group. For example, an advisory commission might be created to assist both government agencies and the private sector to comply with the Privacy Principles as an aid to ensuring even implementation of a uniform set of information use standards and thereby increasing public trust in the NII.

On the downside, an advisory body generally works well because it focuses on a narrow range of issues (for example, in the case of NSTAC--national security/emergency preparedness telecommunications). Privacy issues, as we have seen, are potentially quite far reaching. Advisory committees typically can recommend certain action, but they do not create rights, benefits or responsibilities that are enforceable at law or equity.

Advisory commissions may also be criticized as inefficient or ineffective by those who want to see quick action on privacy issues. As a practical matter, an advisory commission may not be able to bring about specific desired changes as rapidly as a regulatory agency might, since it would have to build a consensus and influence change by persuasion over time rather than by mandate. Others, however, may believe that having privacy experts lending advice would significantly balance and promote important interests without

burdening society with the costs and intrusiveness generally associated with a regulatory function.

VI.

CONCLUSION

Data is the commodity that will fuel the information superhighway.

Consumers want to control what personal information is disclosed about them, to whom, and how that information will be used. As a result, electronic commerce will flourish only if we are able to agree on, and implement, fair information practices for the information age.

The Privacy Principles articulate a methodology for determining, in any particular circumstance, whether an information practice is fair. In this Options Paper we have attempted to set the stage for a thoughtful debate on how best to implement that methodology across disparate economic and social sectors in simple, unobtrusive, and predictable ways.

Our task has been, and will continue to be, complicated by the ubiquitous presence and rapid evolution of information technology, by the changing value of information itself, and by the complexity and variety of privacy perspectives around the globe. Every day, a new information gathering technology emerges, its virtues and vices are hailed, and a new technological response or governance norm is conceived. The desire to issue a complete, and completely current, Options Paper began to stand in the way of issuing any Options Paper at all.

But it is time now to begin the debate in earnest, keeping in mind always that a solution that is not sufficiently flexible to keep pace with the rate of change in the digital environment is no solution at all.

We hope that this Options Paper will elicit comments, ideas, and suggestions from a broad range of respondents and provoke a lively public discussion on the best way to balance competing values of personal privacy and the free flow of information in a digital democratic society. The Information Policy Committee will consider all comments carefully, and use them to inform the policies and practices it will subsequently recommend to the Information Infrastructure Task Force.

END NOTES

1. Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens 41 (1973).
2. *Id.* at 40.
3. The Privacy Protection Study Commission was created by the Privacy Act of 1974, Pub. Law. No. 93-579, 5 U.S.C. § 552a (1994). The Commission issued its report, including over 160 recommendations, in 1977. *See* Privacy Protection Study Commission, Personal Privacy in an Information Society (1977).
4. Organization for Economic Cooperation & Development, Guidelines for the Protections of Privacy and Transborder Flow of Personal Data, OECD Doc. No. C(80)58 (1981).
5. *Id.*
6. *See* General Accounting Office, Computers and Privacy: How the Government Obtains, Verifies, Uses, and Protects Personal Data, GAO/IMTEC-90-70BR (1990).
7. *Id.*
8. Privacy Working Group, Information Infrastructure Task Force, Principles for Providing and Using Personal Information (1995) (hereinafter Privacy Principles) available at *IITF Principles* (visited 4/3/97) <<http://www.iitf.nist.gov/ipc/ipc-pub.html>>.
9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995). For a comparison of the US/EU approaches to information privacy, see generally, Paul M. Schwartz & Joel Reidenberg, Data Privacy Law (1996).
10. EU Directive, *supra* note 9, at art. 6(1)(b).
11. *Id.* art. 6(1)(c)-(e).
12. *Id.* art. 7.
13. *Id.* arts. 22-24.
14. *Id.* art. 28.
15. *Id.* art. 25.
16. *Id.*
17. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1891).
18. *See* William Prosser, *Privacy*, 48 Calif. L. Rev. 383 (1960). Prosser's torts included: intrusion upon the

list. Hospitals subsequently use these lists to solicit business for the hospital. *See Using Medical Information for Marketing*, 16 Privacy J. 1, Feb. 1990.

(3) Even local supermarkets can use computers to track the exact nature and frequency of an individual's purchases. *See* Connie Koenenn, *Junk Mail: Guess Who's Giving Out Your Address*, L. A. Times, June 17, 1993, at E1, available in 1993 WL 2303036. *See also*, Carrie Teegardin, *Keeping Tabs on Shoppers: Ad&P Membership Card Records Each Purchase in a Database*, Atlanta J.-Const., July 2, 1994, at B1, available in 1994 WL 4469745.

27. *See* H. Jeff Smith, *Managing Privacy - Information Technology and Corporate America* 7-8, 124-25 (1994) (discussing the distinction between information existing in separate, distinct pieces and the same information combined and available in one place); Colin Bennet, *Regulating Privacy* 35-37 (1992) (discussing implications of increased computerization for data protection).

28. "As we see a convergence between telecommunications, computers and information processing, almost any transaction you enter into is leaving some kind of trace." reported in Kinsey Wilson, *Your Life as an Open Book - Digital Wizardry that Promises to Make Life More Convenient Could Threaten your Privacy*, Newsday, July 21, 1993, at 8, available in 1993 WL 11382702 (Comments of Prof. Joel Reidenberg, Fordham U. School of Law).

29. For a representative sampling of the types of databases that are being compiled and the kinds of information they contain, see Thomas B. Rosenstiel, *Someone May Be Watching - Everywhere We Go, We're Increasingly Under Surveillance: Employers, Marketers, even Private Detectives Use High-Tech Tools and Scan Mostly Unregulated Databases to Pry into our Daily Lives*, L. A. Times, May 18, 1994, at A1, available in 1994 WL 2166435; Larry Tye, *List-Makers Draw a Bead on Many*, Boston Globe, Sept. 6, 1993, at A1, available in 1993 WL 6607597.

30. *See* Jay Greene, *They're Selling Your Secrets*, Orange County Reg. (Calif.), Apr. 21, 1996, at A01, available in 1996 WL 7023494; Jim Donaldson, *You Can Keep Your Privacy But it Will Take Some Doing*, Gannett News Service, Mar. 6, 1996 (page unavailable online), available in 1996 WL 4375432 (reporting that the typical shopper is in at least 25 corporate databases).

31. Mary Zahn & Eldon Knoche, *Electronic Footprints: Yours Are a Lot Easier to Track than You May Think*, Milwaukee J. & Sentinel, Jan. 16, 1995, at A1, available in 1995 WL 2967415.

32. For a collection of industry guidelines, see Federal Trade Commission, Staff Report on Public Workshop on Consumer Privacy on the Global Information Infrastructure Appendix C (1996), available at Federal Trade Commission Home Page, *Workshop on Consumer Privacy on the Global Information Infrastructure*, (visited Apr. 3, 1997). <<http://www.ftc.gov/bcp/privacy/privacy.htm>>.

33. *See* Smith, *supra* note 27, chs. 3 & 4.

34. *See generally*, G. Bruce Knecht, *Privacy: A New Casualty in Legal Battles*, Wall St. J., Apr. 11, 1995, at B1, available in 1995 WL-WSJ 2126406 (reporting on the "data that is held -- in staggering amounts -- by private-sector companies" and on the fact that "[v]ast amounts of consumer information are entirely unprotected").

35. *See* Louis Harris and Associates, *supra* note 24, at 16.

36. *See* Privacy Principles, *supra* note 8, at 2.

37. *Id.*

38. *See* U.S. Const. preamble.

39. The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, 5 U.S.C. § 552a (1994).

40. *See* Bennet, *supra* note 27, at 72-73 ("The Privacy Act would not have been passed in 1974 had it not been for Watergate. Its enactment was seen as part of a wider effort to open up the executive establishment and cleanse the government of the murky and conspiratorial influences of the Nixon White House."); James T. O'Reilly, Federal Information Disclosure § 20.01, at 20-5 (2d ed. 1995) ("Computerization had an essential role in passage of the Privacy Act because record retention systems were less threatening to the public and Congress when hand-held index cards required hours of search and retrieval.")

41. 5 U.S.C. § 552a(e)(1).

42. 5 U.S.C. § 552a(e)(10).

43. 5 U.S.C. § 552a(b).

44. The provisions relating to disclosure of Social Security Numbers, contained in Section 7 of the Act, however, apply to federal, state, and local government agencies. 5 U.S.C. § 552a (note).

45. Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28951 (1975).

46. 5 U.S.C. § 552a(d)(1).

47. 5 U.S.C. § 552a(d)(2).

48. 5 U.S.C. § 552a(g).

49. 5 U.S.C. § 552a(i).

50. 5 U.S.C. §§ 552a(a)(7) & (b)(3).

51. *See* Privacy Protection Study Commission, the Privacy Act of 1974: An Assessment 91-93 (1977); Committee on Government Operations, *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by Congress*, H. Rep. No. 98-455, at 41-5 (1983); Bennett, *supra* note 27, at 108-09; David Flaherty, Protecting Privacy in Surveillance Societies 323-24 (1989).

52. Schwartz & Reidenberg, *supra* note 9, at 96-98.

53. O'Reilly, *supra* note 40, at 20-1 & 20-5.

54. Pub. L. No. 100-503, 102 Stat. 2507, 5 U.S.C. §§ 552a(a)(8)-(13), (e)(12), (o)-(r), (u).

55. Schwartz & Reidenberg, *supra* note 9, at 101.

56. This automated comparison is called a "matching program." 5 U.S.C. § 552a(a)(8).

57. 5 U.S.C. § 552a(u)(4).

58. 5 U.S.C. § 552a(p). Following adoption of the Matching Act, Congress passed the Computer Matching and Privacy Protection Amendments of 1990, which further clarified the due process provisions of subsection (p). Pub. L. No. 101-508, tit. VII, subtit. C, 104 Stat. 1388-334 (1990).

59. 5 U.S.C. § 552a(u).

60. *See* General Accounting Office, Computer Matching: Quality of Decisions and Supporting analyses little affected by 1988 Act (1993).

61. Schwartz & Reidenberg, *supra* note 9, at 101.

62. Paperwork Reduction Act, Pub. L. No. 96-511, 94 Stat. 2812, 44 U.S.C. § 3501 - 3520 (1994).

63. Pub. L. No. 96-511 § 3501(b), 94 Stat. at 2813 (quoting the original language of the PRA). The PRA was significantly rewritten, dropping this phrase, in 1995. Paperwork Reduction Act of 1995, Pub. L. No. 104-13, 109 Stat. 163, 44 U.S.C. §§ 3501-3520 (1996).

64. A "collection of information" from individuals refers to an agency's collection of information in response to identical questions posed to, or identical reporting or recordkeeping requirements imposed on ten or more persons. 44 U.S.C. § 3502(3).

65. 44 U.S.C. § 3504(a)(3).

66. 44 U.S.C. § 3504(g)(1).

67. Interviews with Ronald Kelly, Regulatory Information Service Center, General Services Administration, and Jefferson B. Hill, Branch Chief, Office of Information and Regulatory Affairs, Office of Management and Budget, in Washington, D.C. (April 15, 1997).

68. 44 U.S.C. § 3506(c)(1)(B).

69. 5 U.S.C. § 552.

70. 5 U.S.C. § 552(b)(6).

71. 489 U.S. 749 (1989).

72. *Id.* at 773. *See also* Office of Information and Privacy, U.S. Dep't of Justice, Freedom of Information Act

Guide and Privacy Act Overview 220-31, 243 (1996) (discussing privacy considerations and FOIA).

73. Pub. Law. No. 83-740, § 214, 68 Stat. 1023; Pub. L. No. 94-521, § 12(a), 90 Stat. 2464, 13 U.S.C. §§ 9, 214 (1994).

74. *Id.* §§ 8(a), 8(c), & 301(g).

75. Pub. L. No. 94-455 § 1202, 90 Stat. 1520, 1667, 26 U.S.C. § 6103 (1994).

76. 26 U.S.C. § 6103(a). The statute permits disclosure to third parties under certain exceptions, including for tax administration purposes, to persons with material interest in the data (such as an heir of a deceased taxpayer), and to federal, state, and local agencies under specified circumstances. 26 U.S.C. § 6103(c)-(n).

77. 26 U.S.C. § 6103. Several years ago it was widely reported that more than 1,300 IRS employees had been investigated for improperly accessing private taxpayer files. *See* Stephen Barr, *IRS Vows "Zero Tolerance" For Snooping in Tax Records*, Wash. Post, July 20, 1994, at A4; Stephen Barr, *Probe Finds IRS Workers Were "Browsing" in Files; Security Review Points to Fraud*, Wash. Post, Aug. 3, 1993, A1. As of July 31, 1993, 397 instances of questionable access to taxpayer records were referred to IRS management. The IRS reported to Congress in 1993 that eleven employees resigned, five employees were removed, sixty-three employees were suspended or demoted; ninety-three employees were reprimanded or admonished; twenty employees were counseled or given caution letters; and that management action was pending in fifteen cases. *See*, Auditing the Auditors: Waste and Abuse at IRS and Customs? Hearing Before the Senate Committee on Government Affairs, 66, 103d Cong. (1993)); *see also* S. 522, *A Bill to amend the Internal Revenue Code of 1986 to impose civil and criminal penalties for the unauthorized access of tax returns and tax return information by Federal employees and other persons, and for other purposes*, 105th Cong. 1st Sess., introduced Apr. 9, 1997.

78. 26 U.S.C. § 6103(p).

79. Schwartz & Reidenberg, *supra* note 9, at 130.

80. *Id.* at 150.

81. *See* Family Educational Rights and Privacy Act (FERPA) (Buckley Amendment), Pub. L. No. 93-380, Title V, § 513, 88 Stat. 571, 20 U.S.C. §§ 1221(note), 1232g.

82. *See* Child Abuse Prevention and Treatment Act, Pub. L. No 102-586 § 9(b), 106 Stat. 5037, 42 U.S.C. § 5106a(b)(4) (1994).

83. *See* Drivers Privacy Protection (Boxer-Moran) Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 to 2102, 18 U.S.C. §§ 2721-2725 (1994).

84. *Id.*

85. 18 U.S.C. § 2510, *et seq.* (1994).

86. *See* 39 U.S.C. § 3623(d) (1994).

87. 18 U.S.C. § 2511.

88. 18 U.S.C. § 2510(2).

89. 18 U.S.C. § 2510(1).

90. 18 U.S.C. § 2510(12).

91. *See* 18 U.S.C. § 2516. To obtain such a court order, the government must show that both probable cause and necessity exist. To prove necessity, the government must show that "other investigative procedures have been tried and failed or why [such procedures] reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(c). Even after these requirements are satisfied and the interceptions begin, the government must actively "minimize" interceptions; that is, agents must stop listening (and stop recording) any conversation where criminal activity is not being discussed. *Id.*

92. *See* 18 U.S.C. § 2511(c) & (d). Some states require that all parties to a communication consent to its interception.

93. *See* 18 U.S.C. § 2510(5)(a).

94. *See* 18 U.S.C. § 2511(2)(a)(I).

95. *See* 18 U.S.C. § 2516(1) (providing list of offenses).

96. *See* 18 U.S.C. § 2516(3).

97. *See* 18 U.S.C. § 2515 (1994).

98. *See* 18 U.S.C. § 2701 *et seq.* (1994).

99. 18 U.S.C. § 2510(17).

100. *Id.*

101. Such storage would be subsequent to the transmission and, accordingly, the definition of "electronic storage" is not satisfied. *See* United States Dep't of Justice, Federal Guidelines for Searching and Seizing Computers 86-87 (1994).

102. *See* 18 U.S.C. § 2701 (1994).

103. A "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system. *Id.*

104. *See* 18 U.S.C. § 2702 (1994); 18 U.S.C. § 2711(2) (1994).

105. *See* 18 U.S.C. § 2702(b)(3).

106. *See* 18 U.S.C. § 2702(b)(5).

107. *See* 18 U.S.C. § 2702(b)(6).

108. 18 U.S.C. § 2703(a).

109. 442 U.S. 735, 744 (1979).

110. The Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, 18 U.S.C. §§ 1367, 2232, 2510-2511, 2701-2711, 3117, 3121-3127 (1994).

111. 18 U.S.C. § 2703.

112. 18 U.S.C. § 2703(c)(1)(C).

113. Pub. L. No. 103-414 Title II, 108 Stat. 4290, 18 U.S.C. § 2510 *et seq.* (scattered sections) (1994) (also known popularly as the Digital Telephony Bill). The Digital Telephony Bill, which was heavily debated, requires telecommunications carriers to design switches that will permit law enforcement personnel to (1) conduct court-authorized interceptions of wire and electronic communications handled by those carriers and, (2) obtain call set-up information (transactional data about the call).

114. 18 U.S.C. § 2703(c)(1)(C).

115. *Id.*

116. 18 U.S.C. § 2703(c)(1)(B)(ii).

117. 18 U.S.C. § 2703(c)(2).

118. 18 U.S.C. § 2703(d).

119. 18 U.S.C. § 2703(c)(1)(A).

120. TRPI is not message content. *See* National Telecommunications and Information Administration, U.S. Dep't of Commerce, Privacy and the NII: Safeguarding Telecommunication-related Personal Information (1995).

121. Pub. L. No. 104-104, 110 Stat. 56 (1996).

122. Pub. L. No. 104-104 § 702, 110 Stat. 56 at 148, 47 U.S.C. § 222. A "common carrier is a person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or . . . radio transmission of energy . . .". 47 U.S.C. § 153(h). Common Carrier status arises out of the "quasi-public character, which arises out of the undertaking to carry for all people indifferently." *National Ass'n of Reg. Util. Comm'rs v. FCC*, 533 F.2d 601, 608 (D.C. Cir. 1976).

123. Prior to passage of the 1996 Act, in its Computer II and Computer III proceedings, the FCC

promulgated some rules governing use of CPNI. For a background discussion, see 61 Fed. Reg. 26483, May 28, 1996.

124. 47 U.S.C. § 222, 110 Stat. at 148.

125. *See*, NPRM FCC 96-221, 61 Fed. Reg. 26483, May 28, 1996.

126. *See*, 61 Fed. Reg. 43031, Aug. 20, 1996.

127. *See* Gautam Naik, *New FCC Rules To Let Caller ID Run Nationwide*, Wall St. J., Dec. 12, 1995, at B8, available in 1994 WL-WSJ 9910068.

128. *See* Debra Berlyn, *Protecting Telecommunication Consumers, Privacy in the National Information Infrastructure*, The National Association of State Utility Consumer Advocates, Jan. 27, 1994, at 5.

129. u.s. Dep't of Commerce, Nat'l Telecomm. & Info. Admin., Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995), available at NTIA Reports, Filings, and Related Materials (last modified Apr. 2, 1997) <<http://www.ntia.doc.gov/ntiahome/policy/privwhitepaper.html>>.

130. *Id.* at 19-27.

131. *Id.* at 25.

132. Available in Federal Trade Commission, *supra* note 32, at Appendix C.

133. *See* Ctr. for Democracy & Tech., *CDT Privacy Demonstration* (visited 3/26/97) <http://www.cdt.org/privacy/online_services/chart.html>.

134. 39 U.S.C. § 3623(d) (1994).

135. 19 U.S.C. § 482 (1994).

136. 39 C.F.R. § 233.3 (1994).

137. There are limited exceptions to this requirement, such as for situations involving recovery of stolen mail, dealing with damaged mail, or involving an immediate threat to persons or property. *See* 39 C.F.R. § 233.3(f).

138. *See* Al Gore & Ronald H. Brown, *The national Information Infrastructure: Agenda for Action* 14-15 (1993).

139. *See* Office of Technology Assessment (OTA), *Protecting Privacy in Computerized Medical Information* 33-34 (1993) (hereinafter OTA Report); *Physicians Computer Network, Inc., Company Information* (updated Feb. 5, 1997) <<http://www.pcn.com>>.

140. Eighteen percent of the respondents to the 1996 Equifax Survey consider use of the patient records -- even for medical research -- "very acceptable." Thirty nine percent consider this use "somewhat acceptable." Both groups considered its use appropriate without prior permission only as long as no information released

39
18
57

identifies an individual patient. Nearly one-third of the survey respondents characterized even that use as "not at all acceptable." Lou Harris & Associates, Inc., *supra* note 24.

141. Alan Westin has noted that information contained in medical records can have "an enormous impact on people's lives" and that such information "affects decisions on whether they are hired or fired, whether they can secure business licenses and life insurance, whether they are permitted to drive cars, whether they are placed under police surveillance or labeled a security risk, or even whether they get nominated for and elected to political office." Jeffrey Rothfeder, *Privacy for Sale* 181 (1992) (quoting comments of Alan Westin).

142. *See Medicine: No Restrictions on Drug Data*, L. A. Times, May 18, 1994, at A12.

143. *See* Institute of Medicine, Nat'l Academy of Science Health Data in the Information Age - Use Disclosure and Privacy 190-91 (1994).

144. National Research Council, Report of Privacy and Computerized Records (1997). *See*, Warren E. Leary, *Panel Cites Lack of Security on Medical Records*, N.Y. Times, Mar. 6, 1997, at A1.

145. *See* Privacy Protection Study Commission, *supra* note 3, at 290.

146. *Id.* at 290-91.

147. *See* John Riley, *Changes in Health Care are Eroding Medical Records Privacy Protection*, Com. Appeal (Memphis, Tenn.), Apr. 23, 1996, at A5, available in 1996 WL 9903637; Jay Greene, *Your Medical Records - Perhaps Your Most Personal Information - Also are the Most Vulnerable to Public Scrutiny*, Orange County Reg. (CA.), April 24, 1996, at C01, available in 1996 WL 7023964.

148. *See* Leary, *supra* note 144.

149. MIB maintains health records on 15 million Americans for 600 member insurance companies. *See* Greene, *supra* note 144.

150. *See* Melanie Hirsch, *Protecting Your Privacy - Make Sure Your Medical Records Are Accurate and Confidential*, The Syracuse Post-Standard, Mar. 25, 1994, at C1, available in 1994 WL 5620138.

151. *See* OTA Report, *supra* note 137, at 2. One study found that consumers were unaware of the extent to which health insurance companies shared information concerning employees' health claims with their employers and were also unaware of the amount of information now being required in the health claims review process. *See* Smith, *supra* note 27, at 148; Leary, *supra* note 144.

152. *See* Rothfeder, *supra* note 139, at 180; *see also*, *Commentary: Keeping Medical Secrets a Secret*, Chi. Trib., Apr. 5, 1996, at 17, available in 1996 WL 2659263 (reporting on the erosion of medical records privacy with the growth of HMOs and health networks, the rise of commercial information companies and medical information increasingly becoming a commodity); Mike Woods, *Plug Leaks on Medical Records*, Plain Dealer (Clev.), Feb. 6, 1996, at 6E, available in 1996 WL 3534915, (reporting on specific examples of misused medical record information appearing in a recent article in Medical Economics).

153. Medical records held by federal government agencies are protected by the Privacy Act of 1974, 5 U.S.C.

§ 552a. Section 543 of the Public Health Service Act (42 U.S.C. § 290dd-2) provides protection for records of patients in federally-assisted treatment programs for alcohol or drug abuse. Additionally, medical records generated by the Department of Veterans Affairs for the treatment of alcohol or drug abuse, sickle-cell anemia, or H.I.V. are accorded special confidentiality under 38 U.S.C. § 7332. One survey of this area, however, noted that only about five percent of all medical records in the United States come under these limited federal statutory protections. *See* Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 Vand. L. Rev. 295, 315 (1995). *But see* discussion *infra* page 34, discussing proposed legislation.

154. *See* OTA Report, *supra* note 137, at 11.

155. CPRI is a non-profit membership organization representing all stakeholders in health care focusing on clinical applications of information technology. *See* *Computer-based Patient Record Institute* (last modified Mar. 3, 1997) <<http://www.cpri.org/msgnls.html>>.

156. *See* OTA Report, *supra* note 137, at 77.

157. *See* *AHIMA'S Role in Health Information Confidentiality Issue* (visited Apr. 11, 1997) <<http://www.ahima.org/media/press.releases/history.html>>.

158. While 34 states have laws covering the use and dissemination of medical information, most are not comprehensive. for example, only 28 such laws enable the patient to review their records and correct errors. *See*, Leary, *supra* note 144.

159. *See* *Consumer Rights Expanded Under Reporting Rule Effective in October*, FTC News Sept. 29, 1995, at 1; Greene, *supra* note 147.

160. OTA Report, *supra* note 137, at 44.

161. *See* Debra Beachy, *A Private Matter/Reform Raises Worry About Medical Records*, Hous. Chron., Nov. 21, 1993, at 1, *available in* 1993 WL 9634705.

162. For example, although Wisconsin has strong medical confidentiality laws, computerized medical data flows freely to other states that may not have similar protection. Mary Zahn and Eldon Knoche, *States' Public Records Policies Inconsistent*, Milwaukee J. & Sentinel, Jan. 21, 1995, at A1, *available in* 1995 WL 2968305. This led Wisconsin privacy advocate Carole Deoppers to comment: "[i]f your prescriptions are sent electronically to some sort of company in Battle Creek, Mich., which processes HMO claims, are they protected from re-release? I don't know the answer. Federal protections are needed. You can't legislate the practices of national companies on a state level." *Id.* Likewise a Massachusetts state law gives residents of that state the right to challenge the data maintained by the Medical Information Bureau. Josh Kratka, an attorney with the Massachusetts Public Interest Research Group stated that "[i]n Massachusetts, we have a very strong privacy protection law for life and health insurance applicants" but also noted that "[n]o one else in the nation is covered by the law." *Id.*

163. *See* *Computer Based Patient Record Institute* (last modified Mar. 3, 1997) <<http://www.cpri.org>>.

164. Other bills addressing these issues in the 104th Congress included the Fair Health Information Practices Act of 1995, H. R. 435 (introduced by Rep. Condit) and the Medical Privacy in the Age of New

Technologies Act of 1996, H.R. 3482 (introduced by Rep. McDermott).

165. Pub. L. No. 104-191 (1996) (Kassebaum-Kennedy Act).

166. *See National Committee on Vital and Health Statistics* (visited Apr. 13, 1997)

<<http://aspe.os.dhhs.gov/ncvhs/index.htm>>.

167. Pub. L. No. 104-191 § 264.

168. *See discussion supra* at 19.

169. Pub. L. No. 95-630, 12 U.S.C.A. §§ 3401-22, 92 Stat. 3697, *as amended* Pub. L. No. 101-647, 101 Stat. 4908, 12 U.S.C.A. §§ 3401-22 (1989 & Supp. 1997).

170. In 1970 Congress imposed record keeping requirements on banks because it found that such records "have a high degree of usefulness in criminal, tax, or regulatory investigations and proceedings." Bank Secrecy Act, Pub. L. No. 91-508, 12 U.S.C. § 1951(a), 84 Stat. 1114-1124 (1994). In 1976, the Supreme Court held that a bank customer has no constitutionally protected right of privacy in his or her bank records because these records are the "business records of the bank." *United States v. Miller*, 425 U.S. 432 (1976). The Court concluded that the lack of any expectation of privacy in such records was assumed by Congress when it passed the Bank Secrecy Act. *Miller*, 425 U.S. at 441-442. In 1978, Congress passed the RFPA in direct response to this decision: "The title is a congressional response to the Supreme Court decision in *United States v. Miller* which held that a customer of a financial institution has no standing under the Constitution to contest government access to financial records. The Court did not acknowledge the sensitive nature of these records" H. R. Rep. No. 95-1383, at 34 (1978), *reprinted in* 1978 U.S.C.C.A.N. 9273, 9306.

171. 12 U.S.C. §§ 3403, 3412.

172. 12 U.S.C. § 3404.

173. 12 U.S.C. § 3410.

174. Delay in notice may occur when there is reason to believe that notice will result in endangering life or physical safety, flight from prosecution, destruction or tampering with evidence, intimidation of potential witnesses, or will otherwise seriously jeopardize an investigation. 12 U.S.C. § 3409.

175. 12 U.S.C. § 3417.

176. 12 U.S.C. § 3402.

177. *See BankAmerica Corporation Privacy Code 48, quoted in* Bell Atlantic, Handbook of Privacy Codes (1994).

178. *See* Kristen Davis & Scott Nelson, *Safe Travel on the Info Superhighway: Measures to Protect Individuals' Privacy when Paying Bills Electronically*, Kiplinger's Pers. Fin. Mag., Jan. 1994, at 34.

179. *See* Marianne Kyriakos *et al.*, *Netting a Loan*, Wash. Post, May 8, 1995, at F03.

180. See Sylvester Flood, *Smart Cards: U.S. Banks Take Wait and See Approach to Tomorrow's ATMS*, Bank Marketing, Sept. 1992, at 51.

181. See Smith, *supra* note 27, at 27 & 80-83.

182. See JoAnne S. Barefoot, *The Next Compliance Controversy: Privacy*, ABA Banking Journal 22 (Jan. 1997).

183. *Id.*

184. See discussion of direct marketing *infra* at 45.

185. See Saul Hansell, *Getting to Know You*, Inst. Investors, June 1991, at 71.

186. See Robert E. Kearney, *Keep Your Hands Off My Data*, Bank Marketing, May 1995, at 19. As of June 1996, neither the American Bankers Association or its affiliate, the Bank Marketing Association, had established privacy guidelines for banks to follow. See John N. Frank, *The Brouhaha over Privacy*, Credit Card Management, May 1996, at 32. The 850 member Consumer Bankers Association recently promulgated voluntary privacy guidelines for its members. See Darryl Hicks, *CBA Issues Privacy Guidelines for Lenders*, Nat'l Mortgage News, Feb. 3, 1997 at 35.

187. See Cynthia Graham, *Banks Must Address Consumer Privacy Concerns*, Privacy & Am. Bus., Mar. 1995, at 23.

188. American Express, Citicorp, Chemical Bank and Visa International have all adopted privacy policies. Citicorp, for example, promises its credit card users that it will use Visa and MasterCard data only in connection with Visa or MasterCard business. *Citibank Visa and MasterCard Privacy Policy*, 1993. See also, Hansell, *supra* note 180, at 22 (discussing bank privacy policies).

189. See Smith *supra* note 27, at 17-27 (noting that although banks are some of the most highly regulated institutions in the U.S., most federal banking regulation has focused on issues related to solvency and to fairness in lending).

190. See Editorial, *Financial Services Can Now Be Offered On Internet*, Bank Marketing, May 1995, at 82.

191. See Rothfeder, *supra* note 139, at 32.

192. See Consumer Rep., *What Price Privacy?* May 1991, at 356; Ann Merrill, *Credit Bureaus Continue to be Leading Source of Complaints About Privacy*, Star-Trib. (Minneapolis - St. Paul), Feb. 1, 1996, at 4D, available in 1996 WL 6900979.

193. Pub. L. No. 91-508, 84 Stat. 1127 as amended by Omnibus Consolidated Appropriations Act for Fiscal Year 1997, Pub. L. No. 104-208, div. A, tit. II, § 2402(a)-(g), 110 Stat. 3009-____, 15 U.S.C.A. §§ 1681-1681u (1986 & Supp. 1997).

194. 15 U.S.C. § 1681b.

195. There are two exceptions: there is a 10 year limit for bankruptcies and no time limit for certain transactions involving substantial amounts of money. 15 U.S.C. § 1681.

196. 15 U.S.C. § 1681d.

197. 15 U.S.C. § 1681m.

198. *See* 15 U.S.C. §§ 1681c-k.

199. *See* 15 U.S.C. § 1681b.

200. *See* Rothfeder, *supra* note 139, at 56-57.

201. *See* 15 U.S.C. § 1681b.

202. *Id.*

203. *See* Rothfeder, *supra* note 139, at 56-57.

204. *See* Cheryl B. Preston, *Honor Among Bankers: Ethics in the Exchange of Commercial Credit Information and the Protection of Customer Interests*, 40 Kans. L. Rev. 943, 995 n.31 (1992).

205. *Id.* at 947.

206. *See* Elwin Griffith, *The Quest for Fair Credit Reporting and Equal Credit Opportunity in Consumer Transactions*, 25 U. Mem. L. Rev. 37, 46 (1994).

207. *See* Barry Connelly, *Credit Bureaus Adopt Initiatives in the Absence of a New Law*, Credit World, July/Aug. 1993, at 7.

208. *See* Kenneth Solomon, *Consumer Dispute Verification*, Credit World, Mar./Apr. 1994, at 28.

209. *See, e.g.*, Mitch Betts, *Credit Industry Employs E-Mail Address to Address Dispute Resolution Woes*, Computerworld, Apr. 4, 1994, at 61; *see also* Gary Belsky, *Junk Mailers Lose One in the Privacy Battles*, Money, Dec. 1994, at 46.

210. *See* Equifax Agrees to Info Gathering Standards, Info. Indus. Bull., July 2, 1992, at 5.

211. *See* Fair information Values, July 1994, available at Experian, Inc., (visited Mar. 24, 1997) <<http://www.experian.com>>.

212. *See* Bell Atlantic, *supra* note 177, at 34-43.

213. *See, e.g.*, Lou Harris & Associates, Inc., *supra* note 24.

214. *See* Rothfeder, *supra* note 139, at 58.

215. See James J. Daly, *One Hand Clapping*, 8 Credit Card Management 52-55 (July 1995); *Privacy Top Credit Reporting Concern*, 6 Credit Risk Management Report (Jan. 29, 1996).

216. Prescreening is a process whereby a credit reporting agency compiles or edits lists of consumers who meet specific criteria and then sells the lists to a credit grantor or marketer. *Id.*

217. Omnibus Consolidated Appropriations Act, Pub. L. No. 104-208, tit. 2, 110 Stat. 3009 (1996). See also *Fair Credit Reporting Act of 1996*, 17 ABA Bank Compliance 4-5.

218. Bd. of Governors of the Fed. Reserve Sys., Report to Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud, 1997.

219. *Id.* at 3, 21.

220. Pub. L. No. 100-618, 102 Stat. 3195, 18 U.S.C. §§ 2701-11.

221. "[T]he [Video Privacy Protection Act]...was written [by Congress] after a weekly Washington newspaper obtained and published the video rental records of Bork." L. A. Times, Oct. 20, 1988, at 2, available in 1988 WL 2197371.

222. 18 U.S.C. § 2710(a) & (c).

223. 18 U.S.C. § 2710(b)(2)(B).

224. 18 U.S.C. § 2710(b)(2)(C) & (F).

225. Pub. L. No. 98-549, 98 Stat. 2779, 47 U.S.C. § 551.

226. 47 U.S.C. § 551(h).

227. 47 U.S.C.A. § 551(c) (1991 & Supp. 1997).

228. H.R. Rep. No. 98-934, at 29 (1984) reprinted in 1984 U.S.C.C.A.N. 4655, 4666.

229. See Ronald L. Plesser, Esq., Testimony before the Privacy Working Group of the National Information Infrastructure Task Force, Jan. 27, 1994.

230. See Gary Levin, *Database Draws Fevered Interest*, Advertising Age, June 8, 1992, at 31.

231. Rosenstiel, *supra* note 29 (reporting comments of Direct Marketing Association spokeswoman Lorna Christi).

232. See Judith Waldrop, *The Business of Privacy*, Am. Demographics, Oct. 1994, at 47.

233. Upwards of five billion records exist in the United States containing personal information about individuals. This information about each person is moved from one computer to another on the average of

five times per day. *See* Rothfeder, *supra* note 139, at 17, 90.

234. Privacy Rights Clearing House, Second Annual Report, Jan. 1995, at 23.

235. *See* Henry Hoke, editorial, Direct Marketing, Oct. 1994, at 82.

236. *See* Tim Little, *Privacy vs. Data Use: A Matter of Survival*, Catalog Age, May 1992, at 103.

237. The Direct Marketing Association (DMA), with a membership of some 3,500 manufacturers, wholesalers, and retailers, is the largest national trade association serving this industry. For information on DMA, see generally, Direct Marketing Association, Privacy Action Now! (1996); Privacy, The Key Issue of the 90's: A Direct Marketer's Guide to Effective Self Regulatory Action in the Use of Information (1993); and see the Direct Marketing Association Home Page at <<http://www.the-dma.org>> (visited Mar. 24, 1997).

238. *See* Rosenstiel, *supra* note 29.

239. *See* Direct Marketing Association, Fair Information Practices Manual 7-11 (1994).

240. *Id.*

241. *See* Federal Trade Commission, *supra* note 32, at 27 n.152.

242. *See* Rosenstiel, *supra* note 29 (reporting statement of Professor Mary J. Culnan, Georgetown U.); *see also* Wilson, *supra* note 23 ("It costs pennies to draw a list of names from a computer data base and start assembling a marketable profile that can be sold for as much as \$200 per thousand names. There is only one other industry that operates on that kind of markup, and that's illicit drugs. So long as the list business is that profitable, it is going to spawn greed, and privacy invasion and corruption, just as illicit drugs do." Reporting comments of Denison Hatch). *See also*, Shelly Reese, *Future Shop Customers Draw Line on Privacy Issue*, Cincinnati Enquirer, May 24, 1994 (reporting on the fact that there are currently about 10,000 lists which get sold and rented to other retailers usually at a rate of about \$50 or \$55 per 1,000 names).

243. Metromail, a subsidiary of R.H. Donnelley and Sons Company, maintains mail-order and telephone information on 92 million households, broken down by consumer tastes and demographics. Metromail has recently been involved in a number of privacy related controversies; for example, the release of information concerning 5000 Los Angeles households, including the addresses and ages of children, to a television reporter using the name "Richard Allen Davis" (Davis was recently convicted in San Jose for the kidnap and murder of 12 year old Polly Klaas). *See* Kathryn Dore Perkins, *Huge Market in Data on Kids*, Sacto. Bee (Calif.), June 24, 1996, at A1. Metromail was also sued by an Ohio woman who received sexually offensive mail from a Texas prison inmate who was provided access to a consumer questionnaire she had filled out. The questionnaire had originally been sent to Metromail who in turn passed it on to a contractor for further processing. The contractor, in turn, passed this information on to the Wynne prison unit in Huntsville, Texas for prisoners to process the questionnaires. The woman asserts that this use of her personal information was done without either her knowledge or consent. *Id.*

244. *See* DMA, *supra* note 237.

245. *See* Dan Harrison, *DMA Initiates Major Privacy Push; Self-Policing Seen Essential to Blunt*

Government, DM News at 1 (Nov. 4, 1996).

246. See 2 Priv. & Am. Bus. Vol. 2, Aug., 1995, at 4-5. See also, Jay Greene, *Eluding Their Gaze/The Way to Protect Personal Info is to Leave No Trace but Remember - The Rules Aren't In Your Favor*, Orange County Reg. (Calif.), Apr. 25, 1996, at C01, available in 1996 WL 7024132 (reporting that in privacy matters "[t]he FTC, which regulates unfair and deceptive trade practices, has been perhaps the most aggressive federal agency in reining in credit bureaus, medical-records gatherers and others").

247. Federal Trade Commission, *supra* note 32.

248. See Federal Trade Commission, *supra* note 32 at 41-50. See also, Gary Chapman, *Protecting Children Online is Society's Herculean Mission*, L. A. Times, June 24, 1996, at D14.

249. California, for example, has a state constitutional right to privacy as well as statutory privacy protection. See Calif. Const. art. I., § 1; Calif. Civ. Code § 1798 (West 1995). In 1994, a California court, relying on these statutory and constitutional protections, ruled against an individual who sought a county's entire municipal court information database because of the privacy implications inherent in the aggregate nature of the personal information contained in that database. *Westbrook v. County of Los Angeles*, 27 Cal. App.4th 175, 32 Cal. Rptr. 2d 382 (1994).

250. Merrill, *supra*, note 192.

251. For example, in the early 1990s, mounting consumer dissatisfaction, adverse media coverage and highly publicized lawsuits preceded changes in how the credit reporting industry dealt with consumer access to credit reports and ultimately led to amendments to the Fair Credit Reporting Act. See Rothfeder, *supra* note 139, at 58-62.

252. See *Hearings Before the Subcommittee on VA-HUD-Independent Agencies of the House Committee on Appropriations*, 104th Cong. 2d sess. (1996) (statement of Bernice Friedlander, Acting Dir., Office Of Consumer Affairs), available in 1996 WL 5511468.

253. See statement of Leslie Byrne, Director, Office of Consumer Affairs, at Privacy and American Business -- Third Annual Conference, Managing Privacy in Cyberspace and Across National Borders, Washington, D.C., Oct. 10, 1996.

254. Externalities occur when neither the buyer nor the seller of a product pays a price that reflects the costs that its use and production imposes on society. For example, when list brokers sell information to direct marketers, the data subject may not be fully compensated for the cost that the transfer of data will impose on the data subject. Different but equally troubling concerns exist with respect to inadequate information when available legal remedies are expensive or impractical or the market fails to furnish the information necessary to evaluate a particular product.

255. Kenneth Culp Davis & Richard J. Pierce, Jr. I Administrative law 46 (3d ed. 1994). For example, The Federal Trade Commission Act created the Federal Trade Commission to prevent unfair methods of competition and unfair or deceptive business practices. 15 U.S.C. §§ 42-58 (1994). Likewise, The Commission on Civil Rights Act of 1983 established the Commission on Civil Rights. 42 U.S.C. § 1975 (1994).

256. For example, members of the National Labor Relations Board may be removed only for "neglect of duty or malfeasance in office, but for no other cause." 29 U.S.C. § 53(a) (1994).

257. Department of Energy Organization Act, Pub. L. No. 95-91, § 204, 91 Stat. 565, 571-72.

258. National Performance Review, *From Red Tape to Results: Creating a Government that Works Better & Costs Less*, (1993), available at *National Performance Review Reports* (visited Apr. 4, 1997) <<http://www.npr.gov/library/nprpt/annrpt/redtpe93l>>.

259. Exec. Order No. 12160, 44 Fed. Reg. 55787 (1979) ("Providing for Enhancement and Coordination of Federal Consumer Programs").

260. Exec. Order No. 12546, 43 Fed. Reg. 13349 (1978) ("Relating to the Transfer of Telecommunications Functions"). The NTIA Organization Act of 1992 subsequently codified these responsibilities. Pub. L. No. 102-538, 106 Stat. 3533, as amended by Pub. L. No. 103-66, Title VI, § 6001, 107 Stat. 379-87.

261. *See* Exec. Order No. 12590, 52 Fed. Reg. 10021 (1987) ("National Drug Policy Board"); Exec. Order 12859, 58 Fed. Reg. 44101 (1993) ("Establishment of Domestic Policy Council").

262. For example, although OCA and NTIA can perform advisory and educational functions in both the domestic and international arena, OCA focuses on both the public and private sectors, whereas NTIA focuses primarily on the private sector.

263. The now-defunct Office of Technology Assessment (OTA) was located in the legislative branch.

264. Formal international negotiations are usually in the province of the State Department, which in turn coordinates the participation of relevant executive branch agencies.

265. *Id.*

266. The Equal Employment Opportunity Commission, for example, investigates discrimination; makes determinations based on gathered evidence; attempts conciliation when discrimination has taken place; files lawsuit; and conducts voluntary assistance programs for employers, unions, and community organizations.

267. Bennet, *supra* note 44, at 160.

268. 5 U.S.C. App.2

269. The Advisory Commission on Gulf War Veterans Illness is one such example.

270. NSTAC and NCS publish regular reports, recommend legislation, collect information about network incidents, and coordinate joint government-industry responses to telecommunications issues.



ELECTRONIC PRIVACY INFORMATION CENTER

| [Latest News](#) | [Resources](#) | [Policy Archives](#) | [About EPIC](#) | [Search epic.org](#) |



Latest News July 10, 1997

- ❑ **Senate Committee Debates Key Escrow Encryption.** The Senate Judiciary Committee debated S. 909 and key escrow on July 9. FBI Director Louis Freeh pushed for domestic controls on encryption. See the EPIC [Crypto Policy Page](#) for details.
- ❑ **Framework for Internet Censorship?** The White House announces a [policy for global commerce](#) that encourages content blocking across the Internet.
- ❑ **High Court Rejects Internet Censorship.** In a [landmark decision](#) issued on June 26, the United States Supreme Court struck down the Communications Decency Act as an unconstitutional infringement of free speech. See the [EPIC CDA Page](#) for complete information on the historic Reno v. ACLU lawsuit.
- ❑ **Take the First Amendment Pledge!** To celebrate the demise of the CDA, and to defend against new attempts to restrict online speech, EPIC and the ACLU have launched a grassroots campaign to support free speech on the Internet. Check out www.firstamendment.org for details ... and take the pledge!
- ❑ **Two Federal Courts Strike Down Net Censorship Laws.** Just days before the Supreme Court's decision in the CDA case, the Internet community won [two stunning victories](#) in court challenges to a "mini-CDA" law in New York and a Georgia law that criminalized anonymous and pseudo-anonymous speech.
- ❑ **EPIC Testifies on Computer Security.** EPIC recently testified before the House Science Committee in support of the [Computer Security Enhancement Act of 1997, H.R. 1903](#). EPIC said the measure would help restore public confidence in decision-making on technical standards by federal agencies.

- **Senate Committee Endorses Key-Escrow.** In a setback for efforts to reform U.S. encryption policy, the Senate Commerce Committee has passed the Secure Public Networks Act, which was introduced by Sens. Bob Kerrey and John McCain on June 18. The bill contains a number of coercive measures that would force widespread domestic adoption of key escrow encryption techniques. Check CNET's coverage for more details.
- **EPIC Files Suit for Crypto Czar Travel Records.** The Electronic Privacy Information Center has filed a Freedom of Information Act lawsuit in federal district court, seeking the disclosure of the travel records of Ambassador David Aaron. The suit was filed on the eve of the G-7 summit where it is expected that the White House will be pushing for international acceptance of key escrow encryption. The multi-nation OECD earlier this year rejected a similar proposal.
- **"Surfer Beware" Report Available.** EPIC has released a major report on consumer privacy and the Internet. "Surfer Beware: Personal Privacy and the Internet" is based on a review of the privacy practices of top Internet web sites. The report examines the current state of privacy policies on the Internet and includes recommendations to protect online privacy. Also, the seventh annual Gvu survey finds user support for privacy legislation and anonymity.

EPIC Resources

The EPIC Alert. The current and back issues of EPIC's award-winning newsletter on civil liberties in the information age. Subscribe now.

EPIC Bookstore. Browse the cyber shelves of good books on privacy, free speech, and civil liberties at the Internet's only bookstore devoted to online freedom. Shipping, discounts, and gift wrapping provided!

Former Secrets. View scanned images of previously classified government documents obtained by EPIC under the Freedom of Information Act.

EPIC's Online Guide to Legislation. Track pending legislation on Privacy and Cyber-Liberties in the 105th Congress.

EPIC's Online Guide to Practical Privacy Tools. Information on how to get PGP, RSA SecurPC, and other encryption programs, anonymous remailers and surfing the net anonymously.

EPIC's Online Guide to Privacy Resources All the best sites, newsletters, conferences, and organizations on and off the net.

EPIC Policy Archives

Computer Security. Is Cyberspace secure? Hackers, information warfare, laws and guidelines.

Cryptography Policy. Who holds the keys to online privacy? Clipper Chip, key escrow, export controls, reports and more.

Free Speech. Freedom of Speech issues on the Internet including anonymous speech, liability, censorship, and the successful challenge to the Communications Decency Act.

Freedom of Information. How to use the Freedom of Information Act and other laws to obtain information on government activities. See documents EPIC has obtained. Learn how to get your own files.

Privacy. The A to Z's of privacy. From airline passenger profiling and Caller ID to Social Security Numbers and Wiretapping.

About EPIC

EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC is a project of the **Fund for Constitutional Government**. EPIC works in association with **Privacy International**, an international human rights group based in London, UK and is also a member of the **Global Internet Liberty Campaign** and the **Internet Privacy Coalition**.

EPIC's Litigation Docket. Learn about the privacy, First Amendment, and Freedom of Information Act court cases brought by the legal team at EPIC. Defending your rights in cyberspace!

EPIC Advisory Board and Staff. The people behind EPIC and their pages.

Contribute to EPIC. We have no clients, no customers, and no shareholders. We need your support. Here's how to help out. Information Society Leadership Fund The foundations, companies and individuals who support EPIC.

Praise for EPIC and the EPIC site cited (and sighted) -- Kind words and places to find EPIC.ORG.

EPIC Privacy Policy. What we don't do with your personal information.

Search epic.org

Please enter one or more key words separated by
'and' or 'or'.

Example: privacy and wiretap

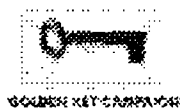
Search:

[More options.](#)

Electronic Privacy Information Center * 666 Pennsylvania Ave., SE, Suite 301 * Washington, DC 20003
+1 202 544 9240 (tel) * +1 202 547 5482 (fax) * <http://www.epic.org/> * info@epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

CRYPTOGRAPHY POLICY



Link your site to the [Internet Privacy Coalition](#) homepage for information about crypto policy including recent developments in Congress.

Recent Crypto News and Documents

Senate Committee Debates Key Escrow Bill. The Senate Judiciary Committee debated S. 909 and key escrow on July 9. The FBI pushed for domestic controls on encryption.

NYT Cybertimes [article](#) on the hearing

Statement of Judiciary Committee Chairman [Orrin Hatch](#)

Testimony of FBI Director [Louis Freeh](#)

Testimony of EPIC Advisory Board Member [Peter Neumann](#)

Testimony NRC Panel Chairman [Kenneth Dam](#)

Senate Committee Endorses Key-Escrow. In a setback for efforts to reform U.S. encryption policy, the Senate Commerce Committee has passed the [Secure Public Networks Act](#), which was introduced by Sens. Bob Kerrey and John McCain on June 18. The bill contains a number of coercive measures that would force widespread domestic adoption of key escrow encryption techniques.

Leading Cryptographers Question Key Escrow. Several distinguished cryptographers and computer scientists have released a new report, "[The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption](#)." The report follows an earlier recommendation of the [OECD](#) that the risks of key escrow encryption be considered before key escrow infrastructures are established. The report concludes "The deployment of a global key-recovery-based encryption infrastructure to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased costs to the end-user."

Encryption Bill Advances. The House Judiciary Committee has approved the [SAFE encryption bill](#). A provision that would have criminalized the use of encryption "in furtherance of the commission of a criminal offense" was substantially narrowed after a [broad-based coalition](#) expressed its concern. See coverage from [CNET](#) and the [Washington Post](#) for more details.

Schlaflly on Crypto. In a column titled Encryption is Essential to Freedom, Phyllis Schlaflly argues "it should be the policy of the United States to encourage wide dissemination of strong encryption technology."

Digital Security. The Washington Post has produced a good [primer on encryption policy issues](#).

OECD Releases Crypto Guidelines. The Organization for Economic Cooperation and Development released Cryptography Policy Guidelines on March 27. The leading industrial democracies rejected key escrow and instead recommended voluntary, market driven development of crypto products. The OECD member countries also emphasized privacy protection, user confidence, and urged removal of restrictions on cryptography. Check out the new section on OECD Crypto Policy below.

Draft Bill on Crypto Restrictions Sent to Congress. The DOJ has sent a draft bill to Congress to create a key recovery infrastructure. The bill also allows access to keys in many circumstances without a warrant and criminalizes the use of crypto in a crime.

Digital Cell Phone Encryption Algorithm Cracked. Several cryptographers, including EPIC Advisory Board member Bruce Schneier, have discovered weaknesses in the encryption algorithm in new digital cell phones. According to sources, the weaknesses are due to US Government pressure on the cell phone industry.

Export Control Bills Introduced. Senators Burns and Leahy and Rep. Goodlatte have introduced legislation to relax export controls on encryption software. See EPIC's testimony on the House bill.

1996 EPIC Crypto Sourcebook Available -- The 1996 edition of EPIC's highly regarded Cryptography and Privacy Sourcebook is now available. A must for the serious student of crypto policy.

Policy Areas on Cryptography

Banning Cryptography. US Government efforts to restrict use of cryptography.

The Clipper Chip. Information on the 1993 US Government computer chip with a back door for easy surveillance.

The Computer Security Act of 1987. Information on the law that regulates who protects computer systems and developed cryptography in the US Government.

Digital Signatures.

Export Controls.

[International Cryptography Policy](#).

[Key Escrow](#) (Government-proposed alternatives to Clipper including "key management" and "key recovery")

[OECD Cryptography Policy Guidelines](#) Information about the recent recommendations of the Organization for Economic Cooperation and Development concerning cryptography policy. NEW

[Reports on Cryptography Policy](#).

Other Materials on Cryptography

[Links](#) to obtaining cryptography for your own use.

Return to the [EPIC Home Page](#)

Last modified: July 10, 1997



Some Online Sources of Information on Privacy

Computer Professionals for Social Responsibility

<http://www.cpsr.org/home.html>

CPSR Electronic Privacy Guidelines

<http://www.cpsr.org/dox/program/privacy/privacy8.htm>

The Electronic Privacy Information Center

<http://www.epic.org>

Privacy Rights Clearinghouse

<http://www.privacyrights.org/>

Privacy Rights Clearinghouse, *Employee Monitoring: Is There Privacy in the Workplace?*, Fact Sheet #7

<http://www.privacyrights.org/fs/fs7-work.html>

Privacy Rights Clearinghouse, *A Checklist of Responsible Information-Handling Practices*, Fact Sheet #12

<http://www.privacyrights.org/fs/fs12-ih2.html>

Privacy Rights Clearinghouse, *Privacy in Cyberspace: Rules of the Road for the Information Superhighway*, Fact Sheet #18

<http://www.privacyrights.org/fs/fs18-cyb.html>

Data Surveillance and Information Privacy

<http://www.anu.edu.au/people/Roger.Clarke/DV/>

Privacy Law & Policy Reporter's World-Wide Privacy Guide

http://www2.austlii.edu.au/~graham/PLPR_world_wide_guide.html

The Consumer Project on Technology

<http://www.essential.org/cpt>

CNET special report on Privacy //

<http://www.cnet.com/Content/Features/Dlife/Privacy/index.html>

Anonymity, Privacy, Security Web page

<http://www.stack.urc.tue.nl/~galactus/remailers/>

MIT PGP Home Page

<http://web.mit.edu/network/pgp.html>

The Federal Trade Commission
<http://www.ftc.gov>

Assembled by Harry Hochheiser, harry@tiger.jvnc.net, and Andrew Oram, andyo@ora.com, of the Cyber Rights Working Group of CPSR, with input from Mary Connors, Craig Johnson, and Christine Mailloux of CPSR, Audrie Krause of NetAction, and Marc Rotenberg of the Electronic Privacy Information Center (EPIC). This document was last updated on 10 September 1996 and is stored on the World Wide Web at http://www.cpsr.org/dox/program/privacy/privacy_links.htm.





ELECTRONIC PRIVACY PRINCIPLES

The CPSR Cyber-Rights Working Group, with input from NetAction and EPIC, created the following Cyberspace Privacy Paper, edited and approved by the CPSR Board.

The team has also assembled some online sources of information on privacy.

Electronic Privacy Guidelines

Electronic mail, web surfing, and other online resources open the door to a whole new world of computer-mediated communication. However, these conversations are not conducted in private: employers, advertising companies, government officials, information providers, and others are watching the net to see what is being said and who is saying it. This monitoring is easily carried out, and often impossible to detect.

Technology currently facilitates massive invasions of privacy that were never possible in the days of traditional sealed envelopes and locked filing cabinets. Both data collectors and governments are taking advantage of these technical possibilities, and neither is doing enough to guarantee the privacy rights of the public. A new commitment to providing technology for privacy protection is needed among software developers and information providers. Governments must also guarantee the rights of individuals and organizations to communicate without risk of unwittingly disclosing information to unknown parties.

Protection of privacy is best achieved through cooperation between employers, service providers, software developers, governments, and information collectors. The burden of protection should fall on those collecting or using data, not on the multitudes of scattered individuals who are using a variety of electronic systems to go about their daily activities. Anonymity is a critical goal: every user should be able to conduct activities without the knowledge of uninvolved parties, and without the risk of having these activities or their embedded information logged for unrelated purposes.

Accomplishing this goal is a complex technical and social matter, requiring an industry-wide effort that governments, at best, should help to coordinate and, at the very least, should not hinder. This document provides guidelines that might be used by principled institutions to guarantee proper respect for the privacy and dignity of employees, customers, and citizens.

While we call on governments and data collectors to promote privacy-protecting technology and to offer guaranties that electronically exchanged information will not be misused, we recognize that they are not doing so adequately at present. Users should therefore protect themselves by learning about the risks of using networks and by employing available software solutions. Technologies exist today to protect and preserve privacy. These include encryption products like PGP, anonymous remailers, and a variety of security and privacy mechanisms built into commonly-used software. Some of these resources have

been attacked at the federal level as dangerous to national and internal security. The real danger is that the world of networked communication will be one in which users can be monitored in their every move. These privacy resources must be protected for the benefit of all.

Guidelines

Employer providers

Many employers have no standing policy on employee privacy. In the absence of any statement to the contrary, users should assume that they have no privacy in their workplace. From a legal perspective, employees have few privacy rights. Courts have upheld the right of the employer to monitor any and all employee communications over the employer's computer system regardless of implied or explicit statements regarding employee message privacy. To alleviate this situation, the following steps are recommended.

- ☐ Each employer should provide and act on clear policies regarding the privacy implications of the computing resources used in the workplace. The policies should explicitly describe:
 - ☐ acceptable use of electronic mail and computer resources, including personal use;
 - ☐ practices that may be used to enforce these policies, such as the interception and reading of electronic mail or scanning of hard disks;
 - ☐ penalties for non-compliance with these policies.
- ☐ Employees should be informed of any electronic monitoring systems that might be used on workplace computers.

Service providers

When an individual signs up for Internet access through an Internet Service Provider, behavior is governed by their contract. No clear laws exist that require an ISP to protect an individual's privacy rights or to notify users of ISP policies. We recommend that providers fill the gap with the following responsible contract policies.

- ☐ Service providers must provide users with a clear understanding of privacy implications of the service contract, including:
 - ☐ the intended use of any information collected as part of the subscription to an ISP, such as mailing address, phone number, credit card information, and software used;
 - ☐ whether the user can choose to stop the use of the information for purposes not immediately required for operation of the service, or better yet, whether the user must explicitly permit the use before it takes place.
- ☐ Demographic or identifying information gathered at servers that is not actively provided by the user should not be used beyond the analysis of site activity; in particular, no attempt should be made to identify individual users or to pass this information on to other parties. Beyond the needs of system administration, information should not be collected or stored on usage patterns of individuals, such as time of day usage, sites visited, and downloads.

Web page owners and other information providers

- ☐ Web sites should describe the intended use of "registration" information required by some prior to access or to downloading of information.
- ☐ Internet white pages services should use only legitimate sources for information. For example, Usenet posts and home pages might be appropriate, while service provider customer lists would not be. These services should provide automated "delete me" services suitable for eliminating present and future inclusions of an individual's identifying information.
- ☐ Individuals should be able remove their names from mass electronic mailing lists.

Mailing list operators, database managers, and other information collectors

- ☐ When individuals log into any Internet site or bulletin board, they should be provided with descriptions of potential uses of any personal information. These potential uses should be narrowly and clearly defined and no commercial use outside of those described should be permitted. Whenever possible, the site should give the individual the choice as to whether to opt in to the use of this personal information.
- ☐ Information collected should be limited to that which is necessary for the described uses, and all personal information should be accurate and up-to-date.
- ☐ Individuals should have easy and immediate access to copies of any information that data collectors may have regarding them. Individuals should be allowed to dispute and correct any inaccuracies.
- ☐ Information collectors should take appropriate technical measures to insure the protection of individual privacy and to safeguard the integrity of the stored information.
- ☐ Information from multiple sources should not be stored in large centralized databases where access is too easy for unauthorized people; nor should large quantities be keyed by a single identifier (such as a social security number in the United States).
- ☐ Data collected about individuals should be sold for commercial purposes only after they give their informed consent.

Software developers

- ☐ Network software should provide users with the ability to take active measures to protect their privacy. These measures might include:
 - ☐ support for strong encryption, such as Pretty Good Privacy (PGP);
 - ☐ mailer/news-posting options that might be used to exclude items of information from automated search services;
 - ☐ automatic and explicit notification of any cases where a user's identity might be explicitly or implicitly revealed.
 - ☐ Privacy protection should be a design goal incorporated into any software that could entail an interaction between a user and a system or network that others have access to.

Governments

At a minimum, governments at any level--national, state, or municipal--should observe the laws and regulations currently on the books (for instance, limitations on the use of social security numbers, restrictions on database matching, etc.) Although this guideline is obvious, it is often violated. In addition

to meeting minimal legal requirements, governments should offer the following guarantees:

- Attempts at protecting individual privacy and anonymity must not be hindered by government interference or legislation.
- Strong encryption, and the ability to use communication facilities such as electronic mail and discussion groups anonymously, should be available without restriction.
- Law-enforcement efforts must not be used as a pretext for invasion of privacy rights. Investigations online must be narrowly tailored to accomplish an explicit, legitimate government purpose.
- Universal standards should be adopted that define privacy rights and the technical and legal means of securing them.
- Laws must make it clear that the use of information stored in computers and on networks should be limited to the use for which the information was collected, and should include both civil and criminal penalties for misuse of that information by individuals, private institutions, or government agencies.

Conclusions

The ethical responsibility for privacy protection lies with those who would violate that privacy, and with those who design and provide the systems where the violations can occur. While electronic data is currently more vulnerable to misuse and secondary use than data exchanged and stored through traditional means (paper and telephone), it could and should be made more secure than those media. More work is needed on both the technical and the social/legal aspects of protecting electronic privacy.

At every step, the public should challenge information collectors and users regarding privacy issues, and not simply accept a dismissive explanation of "company policy."

Computer, network, and software developers should make their systems as secure as is technically possible, and should make privacy protection a built-in feature that is transparent or easily used. Access providers should then use these secure systems and guarantee that they will guard against privacy breaches. Governments must remove barriers to the use of technical solutions and must adopt and enforce civil and criminal penalties for privacy violations. Data collectors must allow individuals access to the data about themselves, and must restrict use of the data to activities of which the individual is aware.

Our society depends on the notion of privacy. It is the ability to maintain privacy, ironically, that allows individuals to participate in the daily activities of their communities. Without guarantees, people will feel inhibited in sending electronic mail, researching in online libraries, shopping at electronic stores, or voicing opinions in political forums. Strong policies protecting and valuing privacy must be put in place now, while the electronic systems that will define commerce and communication in the coming decades are being developed.

Some Online Sources of Information on Privacy

Written by Harry Hochheiser, harry@tigger.jvnc.net, and Andrew Oram, ando@ora.com, of the Cyber Rights Working Group of CPSR, with input from Mary Connors, Craig Johnson, and Christine Mailloux of CPSR, Audrie Krause of NetAction, and

Marc Rotenberg of the Electronic Privacy Information Center (EPIC). This document was approved by the Cyber Rights Working Group of CPSR on 9 September 1996 and stored on the World Wide Web at <http://www.cpsr.org/dox/program/privacy/privacy8.htm>.



News from Ed Markey



United States Congress

Massachusetts Seventh District

FOR IMMEDIATE RELEASE June 19, 1997 CONTACT: Colin Crowell (202) 225-2836

MARKEY PROPOSES NEW CYBERSPACE POLICY

Lawmaker says Action Needed on Privacy & Encryption Issues to Protect Consumers & 'Cybertots', Spur Electronic Commerce

WASHINGTON, DC -- U.S. Representative Edward J. Markey (D-MA), Ranking Democrat on the House Telecommunications, Trade, and Consumer Protection Subcommittee, today introduced the "Communications Privacy and Consumer Empowerment Act." This legislation addresses cyberspace privacy, encryption, and e-commerce issues.

"I believe that we need to overhaul U.S. privacy and encryption policy to create the trust and security that is necessary for families and businesses to find cyberspace a friendly place for play and commerce," Markey said. "The issue of privacy in the information age and in particular, children's privacy protection, is quite timely as the nation becomes ever more linked by communications networks, such as the Internet. There will not be consumer confidence in the Internet, or other electronic media, as marketplace vehicles for electronic commerce if people feel that they cannot trust that their personal data or their transactions are secure."

"People have a right to exercise control over the collection and dissemination of their personal data and parents must be given the tools and the legal rights to protect their kids from online personal data pillaging and from objectionable content for minors," Markey continued. "I believe that technological empowerment tools, an industry embrace of a code of electronic ethics, and cyberspace-savvy Federal guidelines can help reassure parents and put control back into their hands."

"In addition, I believe that our national encryption policy remains rooted in a Cold War, anti-digital worldview and has not adjusted to the reality of cyberspace. It is clear that encryption, privacy, security, trust, and electronic commerce all go hand-in-hand. American companies will suffer the economic consequences of the current "rear-view mirror" policy and unless policy changes are made, I believe that economic growth will be threatened, jobs lost, innovation stultified and important civic freedoms infringed upon," Markey added.

Key Provisions of the Markey legislation:

1) **Electronic Privacy.** Federal Communications Commission (FCC) and Federal Trade Commission (FTC) shall conduct analysis of whether and to what extent consumers can exercise 3 core "Privacy Bill of Rights" in electronic communications. Where gaps exist, agency guidelines are called for to safeguard consumer privacy. The 3 core rights are the following:

1. KNOWLEDGE that personal information is being collected;
2. Adequate and conspicuous NOTICE that any personal data collected is intended by the recipient

for reuse or sale; and,

3. the right of a consumer to exercise choice, to say "NO" and to curtail or prohibit the unauthorized collection, use, reuse or sale of their personal information.

2) **Encryption.** The legislation contains encryption provisions that state, quite simply, that governmental entities cannot condition or restrict the use or sale in interstate commerce of encryption software regardless of the medium used or length of encryption key. Further, the government is prohibited from conditioning certificates of authority or certificates of authentication upon any key escrow system. This provision will help to foster privacy and security in cyberspace and will assist in promoting electronic commerce and economic growth for our country.

3) **Parental Empowerment.** The legislation would require that the FTC and FCC ensure that parents are able to exercise control over attempts to collect personal data from children. Parents must be able to determine when "cybertot" information is permissible to disclose to corporations and others online and how that information will be used by such entity. In addition, Internet access providers are required to offer parents so-called "E-chips" for free or at cost. "E-chips" is a shorthand term for software blocking technology. This software must be made available to parents at the time they subscribe to service, and subsequently upon request, so that parents can shield their children from indecent or inappropriate online content.

4) **Internet Infrastructure Enhancement.** The legislation proposes permitting information service providers to buy the individual elements of the local phone network a la carte -- as needed -- to bundle together and customize their network needs. If all an Internet services company needed was the right to access the telephone switch, or to purchase use of a certain transport line, or dialtone or call routing services, then that's all the company should have to buy. An Internet company executive or an online entrepreneur could then customize a local telecommunications network to meet her or his network and marketplace needs.

5) **Scanner Eavesdropping Provision.** The legislation will extend the prohibition on the manufacture, sale, or modification of radio scanners capable of receiving cellular phone frequencies to also cover PCS, and other mobile radio frequencies. The rationale behind this policy is that as technology evolves from wireline to wireless technologies, consumers should not lose privacy protections as a result of changing technology.

The United States House of Representatives

FOR IMMEDIATE RELEASE

February 14, 1997

SANDERS INTRODUCES BILL TO BAN ATM SURCHARGE ON CUSTOMERS: Already many customers charged twice for ATM usage

Rep. Bernie Sanders (I-VT) today reintroduced legislation that would prohibit automated teller machine (ATM) owners from levying an additional surcharge on customers for accessing their bank accounts through an ATM machine. Sanders stressed the importance of passing this legislation as many ATM owners around the nation are already surcharging.

On April 1st, 1996, the national communication networks for ATMs - Cirrus and Plus - terminated their policy which prohibited ATM owners from surcharging consumers for using their machines. As a result of this policy change, when a customer needs to withdraw money from his/her account and the customer uses a machine which is not part of his/her bank's network, the customer may be charged twice for withdrawing the funds.

Sanders stated, "At the time of this policy change, experts estimated that within the first 18 months, 80% of ATM owners would impose a surcharge. In actuality, only 6 months after the policy change, 71% of ATM owners were assessing surcharges in North Carolina, 69% in Arizona and 60% in Virginia. While the nationwide figure has only reached 23%, a recent study of banking practices in Texas indicates that the percentage will continue to grow; Texas' largest 10 banks have been allowed to surcharge since 1987 and all 10 banks now assess a surcharge for non-customer ATM withdrawals."

In practice, banks enjoy tremendous savings by conducting customer transactions through ATMs because ATM transactions are less costly to a bank than teller transactions. An ATM withdrawal on a non-owned machine may cost a large bank between \$.50 and \$.60. By contrast, a teller transaction with a customer costs the large bank between \$.90 and \$1.15. A consumer study indicates that in 1995, banks avoided 2.6 billion teller transactions because consumers used ATMs.

Sanders concluded, "At a time when banks are making record profits and one third of those profits - tens of billions of dollars a year - come from fees, it is outrageous that these same banks and other ATM owners are charging consumers even more to access our money. This bill will eliminate these additional surcharges and help protect the customer from another needless expense."

Contact: Tina Wisell (802) 862-0697
Cynthia Weglarz (202) 225-4115