Review and Analysis of Privacy Studies and Issues

General Accounting Office (GAO)

January 30, 2002

Final Report

Review and Analysis of Privacy Studies and Issues
Final Report

Submitted by:

Grant Thornton LLP
2070 Chain Bridge Road, Suite 300
Vienna, VA 22182

Members of the Study Team:

Privacy and Information Policy Consultant
Robert Gellman

Florida State University, Information Use Management and Policy Institute
Bruce T. Fraser
Paul T. Jaeger
Charles R. McClure
John Carlo Bertot

Grant Thornton LLP
Kristen M. Mattingly
Christina M. Sadlik
Alvin M. Pesachowitz
Natasha L. Watts

Sprehe Information Management Associates
J. Timothy Sprehe

January 30, 2002

Table of Contents

Executive Summary

Purpose, Scope, Goals

This report provides analytical input to the General Accounting Office's (GAO) examination of issues related to privacy and the Privacy Act of 1974. The study objectives were to identify leading strategies, principles or models for protecting and balancing privacy rights with other interests; and analyze these for their applicability to United States (U.S.) federal laws, policies, and organizational structure. Privacy in the sense of disclosure of personal information is the focus of this report.

Privacy is a multi-faceted concept difficult to define because it reflects values not directly translatable into consensus elements and not easily applied in practice. For privacy, context is critical to development of standards-the standards that work in one context may not work well in another.

Key Findings

Fair Information Practices. Constitute the most important concept in information privacy. Fair Information Practices (FIPs) are a set of principles for addressing concerns about information privacy and form the basis of many privacy laws in the U.S. and around the world. The FIPs are:

- ***Collection Limitation:*** Restricting collection methods for personal information.
- ***Data Quality:*** Ensuring personal information is relevant, accurate, complete and kept up-to-date.
- ***Purpose Specification:*** Specifying in advance the purposes for which personal information is collected.
- ***Use Limitation:*** Ensuring personal information is not used or disclosed for purposes other than specified.
- ***Security Safeguards:*** Protecting information with reasonable security safeguards.
- ***Openness:*** Making the existence and nature of personal information collected known.
- ***Individual Participation:*** According individuals the right to see and correct personal information.
- ***Accountability:*** Holding data controllers accountable for privacy policies.

The Privacy Act of 1974 was the first law anywhere in the world that expressly implemented FIPs. Because of its age and lack of updating, the Act does not meet the challenges brought on by computer networks.

The International Level. FIPs are core principles of information privacy in almost every country that has formally addressed privacy, forming the basis of an international consensus on privacy that is strong, deep, and more than two decades old. That consensus is at a high policy level, and the implementation of FIPs through national laws varies significantly. The European Union's *Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*, the most important privacy document today, is an effort to harmonize separate data protection laws among EU Member States.

As implemented by the EU Directive and national privacy policy instruments, FIPs can apply to both public and private sectors, whereas the U.S. Privacy Act applies only to the federal government. The EU Directive also increased pressure on other countries to pass compatible data protection laws, although the U.S. has not responded to the international pressure by passing EU-style privacy legislation. U.S. privacy laws apply some FIPs to some domestic record-keepers. For data transfers from the EU, the Department of Commerce negotiated Safe Harbor Principles, which are a version of FIPs, for use by some U.S. organizations for satisfying requirements governing EU data exports.

Challenges of Implementing FIPs. FIPs provide a common menu of information privacy principles for consideration by policy makers. Using FIPs to analyze and evaluate the degree of privacy in a law or set of practices is difficult because FIPs are not self-implementing. Implementation will depend on contextual factors such as the type of data involved, the type of record-keeper, the purpose of processing, the way in which the data will be used and disclosed, the technology employed, costs, and the traditions of the jurisdiction, industry, or record-keeper. No formulaic methodology exists for determining when a specific principle has been applied in a manner that conforms to FIPs.

Other Approaches to Privacy. Some reject the establishment of substantive privacy rules, proposing instead more procedural ways to allow record subjects and record-keepers to personal information private. Among these approaches are treating privacy as a property right, employing privacy enhancing technologies, favoring openness of information, self-regulating privacy, and adopting marketplace solutions.

Enforcement Mechanisms

Enforcement is a central issue in privacy, both domestically and internationally. Following are U.S. enforcement methods for privacy.

- ***Torts.*** American common law developed remedies for invasions of privacy in the last hundred years. However, tort law may not respond to increasing commercial processing of personal information.

- ***Constitutional Litigation.*** Constitutional litigation over some privacy rights is common but the scope of the constitutional protection for information privacy is uncertain. Constitutional litigation only has potential to impose constraints on government activities.
- ***Statutory Rights of Action.*** Lawsuits for violations of statutory standards are a traditional remedy for private violations of individual interests.
- ***Criminal Penalties.*** The Driver's Privacy Protection Act, the Privacy Act, and the Electronic Communications Privacy Act are the only privacy laws that include criminal penalties as enforcement tools.
- ***Administrative Enforcement.*** Some regulatory agencies have administrative enforcement authority for some privacy laws. Examples are the Family Educational Rights and Privacy Act and the Children's Online Privacy Protection Act.
- ***Self-regulation.*** Self-regulation for privacy can consist of individual company acceptance of complaints from individuals, independent resolution of complaints through private or government mechanisms, audits, privacy seal programs, and government supervision/certification of self-regulatory programs.
- ***Export Restrictions.*** The Safe Harbor framework negotiated between the EU and the U.S. allows participating companies to continue to import personal data into the U.S. from Europe in the absence of a generally adequate level of privacy protection in the U.S. The Safe Harbor principles require participants to assure compliance with established principles and to provide recourse for violations.

Structures

Organizational structures – the component units of an organization and their interrelationships – reveal how a government agency approaches privacy in its programs. Formal privacy structures are increasingly found in both the public and private sectors in the United States. Privacy structures (privacy agencies, commissions, chief privacy officers, ombudsmen, and dispute resolution mechanisms) have evolved as better understandings of privacy developed and a search for a higher-order approach to privacy intensified.

- **Overall Federal Structure.** The overall federal structure for privacy protection, regulation, and oversight is a composite approach with limited central coordination and management of governmental privacy. The Office of Management and Budget (OMB) provide some guidance on privacy but each agency has responsibility to implement and comply with federal mandates.
- **Federal Trade Commission.** With the growth of the Internet age and e-commerce in the 1990s, the Federal Trade Commission (FTC) began to devote new resources to addressing the misuse of online personal information. Actual enforcement actions in privacy matters have been relatively few in number.
- **An Example of Agency Office for Privacy Act Privacy Issues: Department of Defense.** The Defense Privacy Office (DPO) is perhaps the most formally structured

Privacy Act office in any federal agency. DPO sometimes addresses privacy issues beyond the Privacy Act.

- **An Example of Agency Office for Non-privacy Act Privacy Issues: Internal Revenue Service.** The role of the Internal Revenue Service's (IRS) Privacy Advocate is to ensure that IRS integrates privacy strategies into all business processes. The key to its activities is the Privacy Impact Assessment (PIA), which must be completed for new systems, systems under development, or systems undergoing major modifications.
- **State Structures.** States exhibit a variety of approaches to privacy protection, regulation, and oversight.
  - **California** has a newly created Office of Privacy Protection in the Department of Consumer Affairs.
  - **Connecticut** has a Freedom of Information Commission, an independent government oversight body concerned with open government and, to a lesser extend, privacy.
  - **Florida** will soon have a State Chief Privacy Officer (CPO) under the State's Chief Information Officer (CIO).
  - **Hawaii** is unique in having embodied FIPs in statute and having created an Office of Information Practices with both open government and privacy functions
  - **Minnesota** has a unit in the Department of Administration that oversees privacy matters.
  - **New York** has the Committee on Open Government, Department of State, which functions independently for oversight of open government laws, including privacy laws.
  - **Wisconsin** has a constitutional right to privacy and had an Office of the Privacy Advocate, which was abolished in 1995.
- **International Structures**. The EU Data Protection Directive places affirmative obligations on EU member nations to establish agencies with powers and duties to supervise national data protection. This report describes institutional structures in selected European nations. Many non-EU nations are implementing laws addressing privacy and data protection issues to meet EU standards in order to facilitate business transactions and ease future entry into the EU. Privacy agencies can also be found in non-EU nations.
- **Corporate Structure.** Most corporations that have decided to address privacy issues do so on a voluntary basis. Some have appointed a CPO to manage privacy activities. Some industry associations address privacy concerns by creating best industry standards and practices.

Section 1: Introduction

1.1 Purpose, Scope, Goals

The U.S. General Accounting Office strategic plan identifies six multiyear performance goals to achieve the strategic objective of facilitating government-wide management and institutional reforms needed to build and sustain high performing organizations and more effective government. One of these performance goals is to enhance efforts to manage the collection, use, and dissemination of government information in an era of rapidly changing technology and efforts to create electronic government initiatives that are focused on the citizen. Management of the federal government's information activities is governed by the Paperwork Reduction Act of 1995 and related laws, such as the Privacy Act of 1974, the Computer Security Act of 1987, the Freedom of Information Act, the Information Technology Management Reform Act of 1995 (Clinger-Cohen Act), and the Federal Records Act of 1950.

GAO, in support of Congress, is reviewing government practices and implementation of those laws in order to better understand the impact of new information technologies on federal information management.

This report provides analytical input to GAO in its effort to meet their strategic goals through the examination of the issues related to privacy and the Privacy Act. The study objectives include the following:

- Identify leading strategies, principles or models for protecting and balancing privacy rights with other interests;
- Analyze these strategies, principles, and models in terms of their application to the federal government in both the public and private sector for both the U.S. and countries outside the U.S.; and
- Analyze the possible applications and possible implications of such leading strategies, principles, and models to U.S. federal laws, policies, and organizational structures, including but not limited to the CIO Council, Office of Management and Budget (OMB), federal agency officials, and agency CIOs.

The report identifies and analyzes significant organizational elements and the major policies and practices associated with each leading strategy, principle, or model.

1.2 A Brief Discussion of Privacy as a Public Policy Issue

Privacy is a broad and elusive concept. Some see privacy as a legal right. To others, privacy is an essential component for the development of intimate human relationships. Privacy may mean keeping a secret. Privacy may be a protection against the exercise of arbitrary government power. Privacy may be control over personal information. Privacy may mean a lock on the bathroom door. Privacy may mean freedom from surveillance. Privacy may mean religious freedom. Privacy may mean being able to share intimate concerns with a physician. Privacy may mean not receiving unwanted telemarketing calls during dinner. Privacy may mean the right to educate your children as you see fit. Privacy may mean that some things are just nobody else's business.

Debates over privacy have few fixed boundaries. Many different fields of study contribute to the debate, including philosophy, psychology, law, sociology, political science, economics, and others. While the debates can be interesting and enlightening, they do not necessarily resolve the definitional problem. There is no consensus definition for privacy. Most debaters think that privacy is important, but they cannot agree on its scope or purpose.

Lawyers have not necessarily done better than others in resolving definitional issues for privacy. The Bill of Rights to the U.S. Constitution is filled with echoes of privacy rights and interests, but finding a clear and comprehensive theme that goes beyond control over government actions is difficult. That is important, but it only addresses a part of privacy. Much of the development of the legal right to privacy has taken place in law journals, but the many contributions have not produced a consensus.

One reason for the lack of agreement everywhere may be that privacy is a value that is not translatable into clear elements readily applicable to all situations. Objective standards can help to decide whether something is red or heavy, but there are no objective standards for complex value-laden concepts like ethics, justice, and privacy. For privacy, context is needed in order to develop standards, and the standards that work in one context may not work as well in the next. The task is even more challenging because of the need to balance privacy interests against other recognized and important public policy objectives.

Professor Priscilla Regan summarized the problem in these words:

> [I]t is difficult to pinpoint the types of claims that can be brought under the philosophical and legal rubric of privacy. Although privacy is widely recognized as an important value, neither philosophers nor jurists have been successful in converting the value into a clearly defined, protectable legal standard. Its contours have evolved, in part, in response to changing technological and social forces. . . [P]rivacy is not absolute but has to be balanced against other rights and interests and often loses to those right and interests. This is true both in the area of invasions of

> privacy for law enforcement purposes and in the area of information collection for public purposes.[1]

This report will not seek to resolve the broad definitional issues surrounding the notion of privacy, nor will it pause for long at the definitional stage.

An analysis of privacy by the Supreme Court from a case decided in 1976 is helpful in separating out privacy concerns for this analysis. In *Whalen v. Roe*, the Supreme Court described its own decisions involving privacy as protecting two kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and the other is the interest in independence in making certain kinds of important decisions (e.g., matters relating to marriage, procreation, contraception, family relationships, child rearing, and education).[2]

It is the first of these interests – involving the disclosure of personal information – that is the subject of this report. Information privacy is the main subject of most existing laws that address privacy rights and interests. Information privacy is also the central subject of most current privacy debates and of many of the privacy bills pending before the Congress and state legislatures. Information privacy is a common concern for record-keepers in both the public and private sectors. Information privacy is also the main theme for the international data protection movement that has influenced the law in many parts of the world since the early 1970s, and is the main subject of interest for data protection agencies now found in dozens of countries.

The breadth of the privacy issue area is illustrated in part by the high level of attention that the issue has received in Washington in recent years and by the growing amount of literature addressing privacy. Appendices to this report identify the numerous Congressional hearings relating to privacy from the last several Congresses (Appendix A) and the results of a review of recent secondary legal sources on privacy (Appendix B). The level of privacy activities is noteworthy politically and academically. It is also reflective of the scope of interest in privacy and the complexity and diversity of the subject.

1.3 Study Methodology

The several research and data collection techniques were applied in the study to develop findings and recommendations. The study team undertook an expansive literature review as part of the effort to fully analyze privacy issues. The team conducted site visits to selected federal agencies to discuss these issues with key federal officials having responsibility for privacy matters. In addition, interviews were held with state privacy officials to bring their perspectives and management models to inform the privacy management and policy process.

---

[1] Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy,* 40-41 (1995).
[2] 429 U.S. 589, 599-600 (1976).

1.3.1 Conduct a Comprehensive Literature Review and Policy Analysis

Many privacy organizations are relatively new, and the academic and professional literature is not well developed. For example, the first serious international study of data protection and data protection institutions was published in 1989.[3] Nonetheless, the study team conducted an exhaustive literature review to identify resources for consideration in the study.

Another source of useful information was the annual reports of national privacy agencies. Many agencies publish annual reports, and the reports sometimes include assessments of the successes and failures of the agencies. Evaluations of national privacy laws, such as periodic parliamentary review, offer insight into the operations of both standards and institutions. The study team also reviewed information on self-regulatory activities found on the Internet and from sponsoring trade associations as well as published items relevant to privacy policy and management disseminated by state government agencies, privacy policy organizations, and others.

1.3.2 Develop a Summary of Key Issues

Following the collection of materials from the literature, the Internet, and elsewhere, the study team developed a summary of key issues and developed a framework for evaluation. The framework was developed based on the categorization, organization, description, and other factors regarding the identified issues. Some privacy strategies, principles, or models in use were not examined further because of their limited relevance or applicability to the U.S. For example, constitutional principles (i.e., the First Amendment) excluded consideration of some approaches employed in other countries.

1.3.3 Conduct Interviews and Site Visits

The study team identified a small number of federal agencies that reviewed, adopted, or are developing privacy principles to guide agency activities. The ability and/or willingness of these agencies to participate in the study, uniqueness of privacy approach, regulatory scope, issues surrounding the development/consideration of privacy principles by the agency, and the potential for the agency's approach to inform the development of federal privacy principles was determined. The team developed an interview scripts (Appendix C) to provide a comprehensive and consistent approach to the interviews and site visits.

To obtain the federal government perspective, interviews were conducted with the Department of Defense (DoD) Privacy Review Office, the Internal Revenue Service Office of the Privacy Advocate, and Peter Swire, former Chief Counselor for Privacy at OMB. Privacy officials from California, Connecticut, Florida, Hawaii, Minnesota, New York and Wisconsin provided the viewpoint from the States.

Information on international organizations was obtained through brief interviews conducted at the 23rd International Conference of Data Protection Commissioners with foreign national and

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

provincial data protection officials from nine different national jurisdictions and seven provincial jurisdictions. The team interviewed the heads of eight national data protection authorities including five major EU Member States: France, Germany, Italy, Netherlands, and the United Kingdom.

1.3.4 Assessment

Based on the completion of the literature search, summarizing the key issues and conducting interviews and site visits the study team documented the elements of information privacy, methods of enforcement of privacy laws and policies, and the current institutional structures designed to address privacy. Examination of the complex three dimensional matrix of privacy elements, enforcement and structures led to no simple or holistic conclusion as to the ultimate solution to addressing privacy issues. In fact this complexity lead to the variability in the assessments presented in Section 5 as identified below.

However, some themes emerged during this study and are reflected in the chapters that follow. These themes are:

1. ***Acceptance of Fair Information Practices:*** Fair Information Practices have been widely accepted around the world as organizing principles for information privacy, with the United States being the principal outlier. Most international privacy laws are directly based on FIPs. Implementation of the principles of FIPs is complex and controversial, but the principles still offer a useful framework for evaluating the elements of information privacy even in the absence of a consensus on the FIP's elements or their content.
2. ***Wide Range of Enforcement:*** Enforcement of privacy laws can be accomplished in many different ways, including criminal and civil remedies, self-regulatory activities, and administrative remedies. There is no reason to expect that there is one right method. Generally, there has been little evaluation of all enforcement methods, however, and choices among the different methods can be hard to make. Enforcement choices are also heavily influenced by external political factors.
3. ***Diversity of U.S. Privacy Laws:*** Other countries with privacy laws usually have omnibus laws that apply common standards to most public and private record-keepers. The U.S. approach is sometimes called sectoral, which means that existing laws are decentralized and often uncoordinated. Privacy laws apply to some records and record-keepers, but not to others. State and federal privacy laws sometimes overlap. Significant differences among privacy laws exist.
4. ***Adoption of Structures:*** Privacy structures can include privacy agencies, privacy offices within government agencies, chief privacy officers in companies, and other institutional features that encompass formal or informal institutions with privacy responsibilities. Most other countries with privacy laws have national data protection agencies, and some countries also have provincial privacy agencies. In the United States, the evidence suggests that the creation of new privacy structures among federal agencies, state governments, and private companies may be a developing trend. Structures may be particularly useful in helping to

address many of the uncertainties that arise over interpretation, implementation, and enforcement of privacy laws and standards.

5. ***Impact of Technology:*** Technology has traditionally been a major undercurrent in privacy debates. The use of cameras by newspapers more than 100 years ago prompted an early proposal for an enforceable legal right to privacy. Today, the Internet may be recognized as the leading threat to privacy. Technology can be a double-edged sword, however, at the same time it can be a threat to privacy and a way to protect privacy. The response to technology is a major driver for privacy policy.
6. ***Lack of Consensus:*** Privacy remains a hotly contested issue in the United States, with many basic conflicts over policy, implementation, and enforcement. Support can be found for everything from doing nothing at all about privacy to enacting strong, omnibus privacy laws covering all public and private record-keepers. An almost infinite number of intermediate positions can be identified. Until there is more political agreement about the shape and direction of a U.S. privacy policy, it may not be worthwhile to develop detailed options for such a broad range of outcomes. However, it is possible to identify areas where more research, analysis, and fact-finding will assist policy makers in making basic choices about privacy or in drafting legislation.

1.4 Document Organization

This report presents the results of the privacy review and analysis activities in the following sections.

- ***Section 1*** provides the project scope, goals, and purpose; a brief privacy discussion; the methodology used; and the document organization.
- ***Section 2*** presents the elements of information privacy, including a discussion on the Fair Information Practices and other approaches to privacy.
- ***Section 3*** describes the available methods for enforcing the privacy laws and policies of various entities.
- ***Section 4*** outlines the institutional structures used to address privacy policy and related privacy functions, including federal, state, international, and corporate structures.
- ***Section 5*** documents the privacy research and analysis findings, and identifies possible applications and implications of leading strategies.
- ***Appendix A*** is a compendium of selected Congressional hearings involving privacy-related issues since 1995.
- ***Appendix B*** lists selected current secondary legal sources concerning privacy between 1991 and 2001.
- ***Appendix C*** provides the interview script used during the interviews with State Privacy office staff.

- ***Appendix D*** presents a selected list of international privacy laws and policies, and data protection agencies.
- ***Appendix E*** provides a list of selected GAO reports involving privacy issues.

Section 2: Fair Information Practices and Other Approaches to Privacy

2.1 Introduction

This report approaches information privacy from three different perspectives. The first is the substance of privacy. What does it mean to say that a data processing activity or technology is either protective of privacy or invasive of privacy? This question cannot be answered effectively or consistently without decomposing the concept of information privacy into smaller elements. The analysis requires identifying relevant rules, policies, and standards that are in use or are under discussion. Because of the lack of a consensus definition of privacy, it is not surprising that there are multiple sources of privacy substance, including laws, self-regulation, standards, technology, and international agreements. In some instances, of course, specific statutes establish clear policies, but the question remains whether those policies are sufficiently protective of privacy.

At the broadest policy level, a meaningful degree of international consensus exists. Despite the consensus, some disagreements over basic principles still can be found, and the differences grow sharper as policies and principles are translated into implementation requirements. Everyone can agree on the principle, but the agreement sometimes disappears when putting the principle into practice.

Context is important for privacy. An activity that draws relatively few or mild objections in one context (e.g., the disclosure of a list of sports magazine subscribers for use in direct marketing) may draw intense opposition in another (e.g., the disclosure of a list of prescription drug recipients from a pharmacy for use in direct marketing[4]). Similarly, a surveillance activity acceptable for one class (e.g., employees) may not be acceptable for another (e.g., website visitors).

Details matter as well. Is a weblog that automatically records information about all website visitors invasive of privacy? The answer may depend on whether identifiable information is stored in the weblog, the percentage of Internet Protocol (IP) addresses that are static (i.e., more readily identifiable) rather than dynamic, the length of time that the data is stored, and how the data will be used and disclosed. The ratio of static to dynamic IP addresses is a factor external to a website and

[4] Robert O'Harrow, Jr., *Prescription Sales, Privacy Fears-CVS, Giant Share Customer Records with Drug Marketing Firm*, Washington Post, Feb. 15, 1998, at A01.

may vary over time. A practice that raises few privacy concerns at one time may present new problems later although the website's processing activities have not changed.

The result of these many layers of complexity is a policy arena that cannot be assessed through mechanical formulas or equations. The weighing and balancing of competing interests routinely requires the exercise of judgment. The judgments become even harder because nearly every discussion of privacy recognizes the need to balance privacy against other values. The consideration of multiple competing values only makes the analysis of privacy that much more complicated and may call for additional types of expertise, technical skills, and political assessments. While the issues are complex, they can still be subjected to formal analysis and evaluation.

The second perspective taken in this report is the enforceability of privacy laws and policies. Institutions of all types, public and private sector alike, engage in activities that affect personal privacy. When laws or policies for privacy exist or are proposed, the available methods for enforcement are always a major issue. Current law and practice provide a multitude of enforcement methods. To some extent, choices about the type of enforcement can be made separately from choices about substantive privacy policies. The debates over privacy enforcement are part of the larger national and international debate over the role of courts, lawyers, administrative agencies, and other oversight and dispute resolution methods.

The third perspective is the structures supporting privacy. Public and private institutions of all types address privacy policy, implement privacy laws, conduct oversight, resolve disputes, sponsor research, and perform other functions. In many countries, a national privacy office is a primary feature of privacy law and regulation. In the United States, dedicated governmental privacy organizations are rare. Here, privacy functions are more likely to be distributed throughout public or private organizations that have responsibilities other than privacy.

Different types of institutions offer different options for addressing privacy substance and for implementing privacy enforcement. The role of privacy institutions has increased in recent years as corporations began to establish chief privacy officers and as non-governmental privacy dispute resolution services emerged. The interplay between structure on the one hand and substance and enforcement on the other is an aspect of privacy that receives considerably less attention in the United States than elsewhere in the world. Structure is an important feature of privacy in most other countries that have addressed privacy at a national, and in some cases provincial, level.

One threshold issue for information privacy is the definition of *personal information*. The protection of personal information is an important goal of information privacy. What exactly is it that privacy policy seeks to protect? The Privacy Act of 1974 defines the term *record* to mean "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular

assigned to the individual, such as a finger or voice print or a photograph."[5] Other comparable definitions are in use elsewhere, but this one will serve adequately for purpose of this discussion.

The most important word in the definition is *identifying*. When is information identifiable to a specific individual? This is a surprisingly difficult question to answer at times. One reason for the difficulty is that public and private institutions maintain so much personal data about individuals. Even individual level data (*microdata*) that does not include an overt personal identifier (e.g., name, social security number, email address) may still be identifiable by matching the non-identifiable elements – such as date of birth, gender, and zip code– with an available database. Whether an item of data is identifiable may depend on the knowledge of the recipient, the type of information available to that recipient, and the effort that a person is willing to invest to connect the available data to a known individual.

Professor Latanya Sweeney, a leading researcher on statistics and public policy, has demonstrated that it is possible to match non-unique identifiers with public records to identify nearly every individual in some circumstances. The Cambridge, Massachusetts, voter registration list has approximately 55,000 voters and is publicly available. Twelve percent of the voters on the list have unique birthdates. So if it is known that a registered voter lives in Cambridge, the person might be identifiable just from the birthdate by using the publicly accessible voter registration database. With birthdate and gender, 20 percent of voters are uniquely identified. With birthdate and five-digit zip code, 69 percent are unique. With birthdate and nine-digit zip code, 97 percent are unique.[6] More broadly, 87 percent of Americans can be uniquely identified just by birthdate, five-digit zip code, and gender, each a non-unique characteristic.[7]

As the amount of personal data available in public and private databases increases, it becomes less likely that non-identifiable data will remain non-identifiable. Professor Sweeney said: "I can never guarantee that any release of data is anonymous, even though for a particular user it may very well be anonymous."[8]

The meaning of *identifiable* and *non-identifiable*, like so many other aspects of information privacy, has a range of alternatives. Except in the health arena, the subject has received little legislative attention.[9] Further discussion of the issue is not essential to this report. The important point is that attempts to avoid privacy concerns by using non-identifiable data will not always succeed. Even data stripped of overt identifiers may still be identifiable and may still raise privacy concerns.

---

[5] 5 U.S.C. §552a(a)(4).

[6] National Research Council, *Summary of a Workshop on Information Technology Research for Federal Statistics,* at box 2.3 (1990), at http://www.nap.edu/html/itr_federal_stats/ch2.html.

[7] Available at http://www.heinz.cmu.edu/researchers/archive/00nov.html.

[8] National Committee on Vital and Health Statistics, Subcommittee on Privacy and Confidentiality, *Roundtable Discussion: Identifiability of Data,* (Jan. 28, 1998), at http://ncvhs.hhs.gov/980128tr.htm

[9] Recent health privacy rules issued by the U.S. Department of Health and Human Services attempt to establish a more sophisticated – and controversial – standard for de-identification of health records. 45 C.F.R. §164.514(a).

2.2 Introduction to Fair Information Practices

The most important concept in information privacy today is FIPs. FIPs are a set of principles for addressing concerns about information privacy. FIPs are especially significant because they form the basis of many privacy laws in the United States and, to a much greater extent, around the world.[10] The international policy convergence around FIPs is broad and deep, and the agreement has remained substantially consistent for more than two decades.

Professor Colin Bennett, author of a study of international data protection policies, described the scope of the international policy consensus:

> Many participants in, and observers of, the data protection movement have remarked on the similar content of the laws passed from country to country. . . . These impressions rest mainly on the detection of a common set of principles for the treatment of personal data. Names range from "principles for privacy safeguards" to "principles for handling personal information" to the "principles of fair information practice" to "data protection principles" to the most commonly used "fair information principles." I will show that, while the nomenclature and codification may vary from country to country, the substance and purpose of these principles are basically the same.[11]

Because of the importance of FIPs, their background and history are worthy of an extended discussion. Before beginning that discussion, however, some cautions should be introduced and briefly recognized. First, while a policy consensus exists, statements of FIPs vary considerably in format. The number of principles and the words used to describe them are often different, but the content is nevertheless quite similar. Second, in recent years, the term *Fair Information Practices* has been increasingly applied by some in the United States to shortened or amended collections of principles that diverge significantly from the international consensus. Third, despite agreement on the broad principles, national policy instruments implementing and enforcing FIPs vary widely. Fourth, FIPs have some critics both among those who are more supportive of privacy protections and among those who are less supportive. Finally, FIPs offer a framework for privacy policy, policy discussions, and legislation. However, the resolution of conflicts over privacy necessarily requires values and judgments from other spheres. All of these cautions will be discussed in some detail below.

2.2.1 Origins and Spread of Fair Information Practices

The United States was an early leader in privacy. David Flaherty, a Canadian data protection scholar, wrote that the United States invented the concept of a legal right to privacy.[12] The cause of action for invasion of privacy has been called the *American tort* because Louis Brandeis and Samuel

---

[10] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States,* 6 (1992) [hereinafter cited as "*Bennett*"]. See also Privacy Rights Clearinghouse, *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy*, at http://www.privacyrights.org/ar/fairinfo.htm.

[11] *Bennett* at 95-96.

[12] David Flaherty, *Protecting Privacy in Surveillance Societies* 306 (1989) [hereinafter cited as "*Flaherty*"]

Warren proposed it in 1890 through a Harvard Law Review article.[13] A 1976 book by a British privacy expert asserted that America was the country with the most highly developed law of privacy.[14]

Fair information practices themselves are an American invention. A U.S. government advisory committee first proposed FIPs in a 1973 report. Health, Education and Welfare (HEW) Secretary Elliot Richardson established the Secretary's Advisory Committee on Automated Personal Data Systems as a response to the growing public and private use of automated data systems containing information about individuals. Richardson worried that automated personal data systems presented a serious potential for harmful consequences, including infringement of basic liberties.[15]

The scope of the Committee's work included both the public and private sectors, and the Committee's recommendations addressed both public and private records. However, it appears that the Committee was principally concerned with government records and did not focus much attention on the effect of its recommendations on private record-keepers

The primary contribution of the Advisory Committee was the development of a code of fair information practices[16] for automated personal data systems. According to Committee Chairman Willis Ware, the name *Code of Fair Information Practices* was inspired by the *Code of Fair Labor Practices*.[17] The Committee's original formulation of the Code was:

> Safeguards for personal privacy based on our concept of mutuality in record keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice.
>
> - There must be no personal-data record-keeping systems whose very existence is secret;
> - There must be a way for an individual to find out what information about him is in a record and how it is used;
> - There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;
> - There must be a way for an individual to correct or amend a record of identifiable information about himself; and

---

[13] Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy,* 4 Harvard Law Review 193 (1890).
[14] Paul Sieghart, *Privacy and Computers,* 11 (1976).
[15] Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens,* (1973) (Department of Health, Education & Welfare), at http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm, [hereinafter cited as "*HEW Report*"].
[16] The basic principles that formed the HEW Committee's code of fair information practices were also put forward at the same time in Great Britain in the *Report of the Committee on Privacy,* (1972), known more popularly as the *Younger Committee.* According to privacy scholar Colin Bennett, it is impossible to judge which committee came first or how the work of one committee may have influenced the other. *Bennett* at 99.
[17] Willis Ware, *An Account of the HEW Advisory Committee,* (1993) (RAND Document P-7846).

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[18]

Privacy scholar David Flaherty observed that this fair information practices code "greatly influenced the Privacy Act and subsequent data protection legislation in other countries."[19] Even a cursory review of the Advisory Committee's report and the Privacy Act of 1974 show a striking similarity in content and organization. The Congress enacted many of the Committee's legislative proposals almost verbatim in the Privacy Act of 1974.[20]

The United States was not the only nation concerned about privacy in the 1970s. European countries began to pass national privacy laws, beginning with Sweden in 1973 and the Federal Republic of Germany in 1977. Both laws incorporated the same fair information practice concepts included in the U.S. Privacy Act of 1974.[21] Several other European countries passed comparable privacy laws in the late 1970s or early 1980s.

In some ways, leadership in privacy passed from the U.S. to Europe at some point after the Privacy Act of 1974. In remarks at the 23rd International Conference of Data Protection Commissioners held in Paris in 2001, the Chairman of the Italian Data Protection Commission commented on the respective contributions of the U.S. and Europe. Stephano Rodotà observed that if the U.S. invented the right to privacy, Europeans invented data protection. It took the European data protection movement to create permanent institutions and broad legislation addressing privacy concerns. The developments in Europe expanded upon privacy work that started in the United States in the form of the development of privacy torts and a few narrowly focused privacy statutes. Rodotà concluded that privacy is better protected in Europe because of data protection activities.[22]

As privacy laws spread throughout Europe, international institutions showed interest, beginning with work initiated by the Council of Europe in 1973. Ultimately, the Council adopted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* in 1980.[23] The Organization for Economic Cooperation and Development (OECD) issued privacy guidelines around the same time.[24] Both documents were similar, and both relied upon the concept of FIPs. These two documents were highly influential in creating greater international recognition of FIPs as core privacy policies during the 1980s.[25] The international organizations expanded upon and

---

[18] *HEW Report* at 41.
[19] *Flaherty* at 310. Colin Bennett called the Committee's report "surprisingly coherent and influential." *Bennett* at 70.
[20] Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 Software Law Journal 199, 211 (1993). HEW Report at chapter III.
[21] *Flaherty* at 21, 107.
[22] Available at http://www.paris-conference-2001.org/eng/contribution/rodota_contrib.pdf.
[23] 20 I.L.M. 317 (1981), at http://conventions.coe.int/treaty/en/treaties/html/108.htm.
[24] Organization for Economic Cooperation and Development, *Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* 20 I.L.M. 422 (1981), O.E.C.D. Doc. C (80) 58 (Final) (Oct. 1, 1980), at http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM.
[25] *Bennett* at 130-139.

reworded the original statement of FIPs produced by the HEW Advisory Committee seven years earlier. The 1980 restatements of FIPs might be viewed as a new edition of the principles.

An academic study[26] by Professor Colin Bennett of the development of privacy policy found five major reasons for the international convergence around FIPs. The first reason is the spread of computer technology. Everyone around the world faces the same revolution in information technology. Privacy was a concern before the computer, but there was no data protection movement before computer use became widespread. Second, countries study the experiences of others and emulate the solutions found elsewhere. Especially in Europe, countries drew from other experiences in the sense of learning and not imitation. Third, an international policy community with shared interests and some domestic political and policy influence helped to spread common ideas and responses. Fourth, privacy work undertaken by international organizations, such as the OECD and the Council of Europe, put pressure on governments to conform to international policies. Finally, actions taken by one country can pressure another to adopt a conforming policy. As discussed below, the EU Data Protection Directive is having this effect.

Of the two early-1980s international documents, the OECD Privacy Guidelines proved to be the most widely cited.[27] For this reason, this report uses the statement in OECD Guidelines as an exemplar for FIPs. (See Sidebar 2.1 on Fair Information Practices.) The eight principles set out in a few pages appear simple, but both the OECD Guidelines and the Council of Europe Convention contain considerable amounts of accompanying explanatory materials and implementation advice. The international agreement on basic principles should not obscure the complexity of some of the policies, the considerable variation in their application, and the controversy about their implementation in different contexts and to different record-keepers. Implementation issues are discussed later in this chapter.

The United States, which is a member of the OECD, formally embraced the OECD Guidelines in 1981 and 1982. During the Reagan Administration, the National Telecommunications and Information Administration (NTIA) at the Department of Commerce actively supported the guidelines and urged corporations to voluntarily comply with them.[28] NTIA's support was part of an effort to show a serious commitment to privacy through voluntary action rather than legislation.[29] More than 180 major U.S. multinational companies and trade associations endorsed the guidelines. NTIA dropped its interest in the guidelines by 1983. The sincerity of the NTIA effort has been

---

[26] *Bennett* at chapter 4.

[27] This is not to suggest that the Council of Europe Convention is irrelevant. The Convention remains an important and influential European document. For example, the data protection law in Ireland includes the text of the Convention as a schedule in the Act. See Data Protection Act, 1988 (Ireland), at First Schedule http://www.dataprivacy.ie/6ai.htm.

[28] See *Report on OECD Guidelines Program*, Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce, to Interagency Committee on International Communications and Information Policy (Oct, 30, 1981), reprinted in *International Telecommunications and Information Policy*, Hearings before a Subcommittee of the House Committee on Government Operations, 97th Congress at 27-58 (1981-82).

[29] General Accounting Office, *Privacy Policy Activities of the National Telecommunications and Information Administration,* (Aug. 31, 1984) (GGD-84-93).

questioned, and the effect of the endorsements was unclear at the time.[30] The corporate endorsements have long since been forgotten. Regardless, the early widespread showing of support for the OECD Guidelines by the federal government and by private industry shows that the guidelines were not inconsistent with American values at the time of their issuance.

The OECD Guidelines have remained relevant to national and international privacy policy for two decades. National laws and international instruments continue to be based on the OECD Guidelines. Even Internet privacy matters can be analyzed under the same framework. A 1998 meeting of the OECD Ministers illustrates the point. The Ministers adopted a *Declaration on the Protection of Privacy on Global Networks* that took note of the continued relevance of the Privacy Guidelines to the collection and handling of personal data in any medium, including global networks. The *Declaration* also without dissent reaffirmed the objectives in the 1980 Guidelines.[31] The Secretary of Commerce represented the United States at that meeting.

[30] Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, VI Software Law Journal 199, 227-33 (1993).
[31] OECD Ministerial Conference, *Conference Conclusions*, SG/EC(98)14/FINAL (October 1998) (Ottawa, Canada), at http://www.oecd.org//dsti/sti/it/ec/prod/sgec_14e.pdf.

Sidebar 2.1 Fair Information Practices

Taken from the Organization for Economic Cooperation and Development's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[1]

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures, which give effect to the principles stated above.

2.2.2 The European Union Data Protection Directive

Perhaps the most important international privacy document today is the European Union's *Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*.[32] The Directive was a response to the enactment of separate data protection laws by some EU Member States. As these countries passed national privacy laws, the differences began to create obstacles to the flow of personal information from one country to another within the EU.

The Directive sought to *harmonize* European data protection laws by requiring all EU Member States to meet minimum requirements for data protection laws. *Harmonization* is an EU term that refers to formal attempts to increase the similarity of legal measures among Member States. Harmonization does not seek absolute uniformity of laws.[33] The purpose of the Directive was to orchestrate the passage of fifteen similar and compatible national data protection laws. As discussed below, the Directive also effectively creates an international legal standard that pressures other nations to pass similar data protection laws or possibly lose the ability to process personal data imported from Europe.

When negotiating the Directive, EU Member States with existing laws sought to have the Directive reflect those laws.[34] While FIPs were at the core of those existing laws – and form the core of the Directive as well[35] – considerable differences in national implementation strategies and statutory language created complications and made the negotiations lengthy (five years) and difficult. The Directive's history and content illustrates several important points.

First, the EU Directive and the process that led to its adoption demonstrate clearly that FIPs can be implemented in many different ways. EU Member State data protection laws are compatible with the Directive and with FIPs, yet the laws differ from one another. Some national laws require registration by data controllers (personal record-keepers)-some do not. Exemptions from privacy laws vary. National laws provide different types of remedies for data subjects. National laws establish privacy supervisory authorities with different structures and powers, although all national (and many provincial) supervisory authorities have a significant degree of political independence.[36] National laws define different roles for industry codes of practice. The challenges of implementing FIPs are discussed in a separate part of this chapter.

Second, while the Directive is often referred to as the *Data Protection Directive*, its official title has two equally important elements: *Directive on the Protection of Individuals with Regard to the Processing of Personal*

---

[32] Council Directive 95/46/EC, 1995 O.J. (L 281) 31, at http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm.

[33] See Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows,* 80 Iowa Law Review 471, 480-81 (1995).

[34] See generally Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 Iowa Law Review 445 (1995).

[35] Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Privacy?*, Technology and Privacy: The New Landscape 99, 106 (Philip E. Agre & Marc Rotenberg eds., 1997).

[36] The EU Directive requires that supervisory authorities have the ability to "act with complete independence in exercising the functions entrusted to them." *EU Data Protection Directive,* at Article 28(1).

Data and on the Free Movement of Such Data. The first element relates to the protection of personal data. The second element refers to the *free movement* of the data. The EU saw that a core level of privacy was essential to permit the movement of data between Member States with different privacy laws. With the harmonization achieved by the Directive, a company in one EU country can move personal data to another EU country without having to comply with the details of the privacy law in that second country. EU record-keepers need only comply with the data protection law in the country in which they are located. Each Member State's law provides a sufficient baseline of FIP protections.

While allowing the free flow of data within Europe, the Directive also sought to protect the rights of individuals by restricting the flow of personal data to a third country that did not have adequate levels of protection. This made the Directive controversial internationally because it created the possibility that personal data could not be lawfully exported to other countries, notably the United States. The point here is that FIPs do not expressly mention the issue of *onward transfer* to other record-keepers or to other jurisdictions. The use and disclosure restrictions in FIPs can readily be interpreted to cover onward transfers, but those transfers are not specifically addressed in the OECD Guidelines or in most other statements of FIPs. How to treat onward transfers is a matter of *implementation* of the principles of *purpose specification* and *use limitation*, rather than a separate policy principle.[37] Differences in national privacy laws have resulted in international conflicts over transborder data flows. The issue of international restrictions on the flow of personal data is discussed in more detail elsewhere.

Third, as implemented by the EU Directive and national privacy policy instruments, FIPs can apply to both public and private sectors. The original U.S. implementation of FIPs through the Privacy Act of 1974 covered only the federal government. Some later U.S. privacy laws extended FIP principles to selected private sector record-keepers, but Congress never considered the omnibus application of FIPs broadly throughout the United States. However, national privacy laws in other countries apply FIPs to public and private sectors alike, although in a few cases, the laws apply only to the public sector. Privacy laws in Canada and Australia only applied to national governments until recent amendments broadened their scope to cover the private sector as well.

The principles in FIPs may have different implementation schemes for public and private organizations. For example, applications to national security and law enforcement establishments are likely to include much broader exemptions than for segments of the private sector, although broad private sector exemptions for journalistic, artistic, or literary data processing[38] are common. However, at the highest level of principle, FIPs work equally well for governmental and non-governmental record-keepers, as illustrated by most national data protection laws.

---

[37] For example, the New Zealand law implements the OECD Guidelines, but it does not apply when personal data is exported to an entity that is not otherwise covered by the law directly. See Privacy Act 1993 (New Zealand) at Article 10, at http://www.knowledge-basket.co.nz/privacy/recept/rectop.html. A change in the export provisions to conform to EU standards is under consideration.

[38] See *EU Data Protection Directive,* at Article 9.

This is not to suggest that public sector and private sector privacy rules need be the same or that they could be precisely identical. In the United States, the federal Constitution – in particular, the Bill of Rights – establishes rules for government conduct that do not apply to the private sector. While the Constitution does not include the word *privacy*, protections for personal privacy are found in many places. These protections protect personal privacy by prohibiting or regulating government actions. Some of these actions are uniquely governmental. For example, only the government would invade privacy by quartering soldiers in a private home without the consent of the owner.[39] However, for many other privacy rights and interests – particularly those pertaining to information privacy – common principles will work for both government and private sector record-keepers.

Finally, the EU Directive increased pressure on other countries to pass compatible data protection laws.[40] Commercial demands for statutory and regulatory compatibility helped the spread of data protection laws within Europe in the 1980s.[41] The Directive – and particularly its potential restrictions on data exports – provided an incentive to non-EU countries to pass conforming laws so that personal data flows from Europe to those countries would not be disrupted. For example, in 2000, Canada enacted a private sector privacy law[42] that was motivated in part by concern about the effect of the EU Directive.[43] Canada previously enacted a privacy law based on FIPs and the OECD Guidelines only for the federal government.[44] On December 20, 2001, the European Commission formally determined that the new Canadian privacy law "covers all the basic principles necessary for an adequate level of protection for natural persons."[45]

The U.S. has not responded to the international pressure by passing EU-style privacy legislation. However, concerns over the possibility that the flow of personal data from Europe to the United States might be disrupted by the lack of adequate privacy in the United States led to lengthy negotiations between the European Commission and the Department of Commerce to find a way to facilitate data exports from Europe to the United States. The problem arose because U.S. privacy laws are not as broad in scope as European laws and because U.S. laws that do exist do not necessarily address all FIP elements. The export of personal data from Europe to the United States

---

[39] U.S. Const. Amend III.

[40] See generally Joel R. Reidenberg, *The Globalization of Privacy Solutions: The Movement towards Obligatory Standards for Fair Information Practices*, in *Visions of Privacy: Policy Choices for the Digital Age,* (Colin J. Bennett & Rebecca Grant eds., 1999).

[41] See *Bennett* at 89-94 (concluding that the 1984 British data protection act was passed for economic reasons and at the behest of the computer hardware and software manufacturers who felt that they might be adversely affected internationally by the absence of a law).

[42] Personal Information Protection and Electronic Documents Act, R.S.C., ch. 5 (2000), at http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

[43] Colin J. Bennett, *Rules of the Road and Level Playing-Fields: The Politics of Data Protection in Canada's Private Sector* 62 *International Review of Administrative Sciences* 479, 484 (1996) ("The impact of the EU Data Protection Directive on Canada has been a constant underlying theme within the recent debates.").

[44] Stephanie Perrin et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide,* xii (2001).

[45] Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (2002/2/EC) [document number C(2001) 4539)], at http://europa.eu.int/eur-lex/en/dat/2002/l_002/l_00220020104en00130016.pdf.

has been a matter of concern ever since promulgation of the Directive in 1995 and its implementation in 1998. The Commerce Department delicately phrased the issue in these terms:

> While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Union to the United States.[46]

The result of the negotiations was a *Safe Harbor* framework for data transfers from EU Member States to the United States. The Safe Harbor Privacy Principles (see Sidebar 2.2) are for use by U.S. organizations receiving personal data from the EU for satisfying requirements governing data exports. Companies can voluntary join the Safe Harbor by complying with the principles and by publicly declaring that they are doing so. The Commerce Department facilitates the public declaration by maintaining an official list of Safe Harbor participants.[47]

The Safe Harbor Privacy Principles consist of seven elements: notice, choice, onward transfer, security, data integrity, access, and enforcement. The application of the principles is explained in a set of *Frequently Asked Questions* that accompanied the principles.[48] The seven Safe Harbor Privacy Principles represent yet another version of FIPs, this one hammered out between the United States and Europe in order to solve political and economic problem that might have resulted from a prohibition on data exports.

[46] Department of Commerce, *Safe Harbor Privacy Principles,* (July 21, 2000), at http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.
[47] Available at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
[48] Available at http://www.export.gov/safeharbor/sh_documents.html.

Sidebar 2.2: Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000[49]

Notice: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

Choice: An organization must offer individuals the opportunity to choose (opt-out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt-in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt-in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

Onward Transfer: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data Integrity: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible

[49] Available at http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.

with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

(1) It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

It would be unfair, however, to suggest that the Safe Harbor Principles represent an official adoption of FIPs by the United States for any purpose beyond relieving the pressure of looming European data export prohibitions. Nevertheless, the agreement by the Department of Commerce to sign on to a FIPs document may be reasonably cited as evidence of the difficulty of avoiding FIPs in defining substantive privacy principles.

More than 30 countries (including EU Member States) now have some type of omnibus national data protection law, with FIPs as the common organizing principles.[50] In the words of one privacy scholar: "Today, data protection is not an innovation. It is an expectation that works in favor of the majority of countries, producing a desire to 'keep up with Joneses' in every country except in the United States."[51]

2.3 Fair Information Practices and Federal Privacy Laws

The Privacy Act of 1974 was the first law anywhere in the world that expressly implemented FIPs. As discussed above, the Advisory Committee that developed FIPs recommended the enactment of a privacy law for federal agencies, and the Act passed in the following year. All provisions of the Privacy Act of 1974 fit reasonably neatly into the FIPs framework. Sidebar 2.3 offers a summary of the Act's provision set out under the eight FIPs as defined by the OECD.

The Privacy Act is sufficiently consistent with current international standards for FIPs that it is possible to suggest that the Act meets the standards of the EU Directive for international transfers. If a third country provides adequate privacy protections through a general or sectoral law, then the Directive allows the export of data to that third country. If the federal government is viewed as an identifiable sector, the Privacy Act of 1974 comes close to meeting all EU requirements. As Sidebar 2.3 illustrates, each FIP element has a meaningful counterpart in the Privacy Act. A formal assessment of adequacy calls for a more detailed review than is appropriate here. However, an informal assessment identifies two notable shortcomings, one relating to the lack of rights for foreign nationals and one regarding the lack of onward transfer provisions.

The Privacy Act grants rights only to U.S. citizens and to aliens lawfully admitted for permanent residence.[52] That means that most foreign nationals have no rights under the Privacy Act and no ability to make or enforce requests for access or correction.[53] That limitation is not likely to be

---

[50] The countries include Argentina, Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Luxembourg, The Netherlands, New Zealand, Norway, Poland, Portugal, Russia, Slovenia, South Africa, Spain, Sweden, Switzerland, Taiwan, Thailand, and United Kingdom. Available at http://www.privacyexchange.org/legal/nat/omni/nol.html. A more complete list of national laws can be found at Mark Rotenberg, *The Privacy Law Sourcebook 2001* 598-606 (2001). Additional countries are Albania, Brazil, Cyprus, Hong Kong, Lithuania, Macedonia, Monaco, Paraguay, and South Korea.

[51] Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Privacy?*, Technology and Privacy: The New Landscape 99, 112 (Philip E. Agre & Marc Rotenberg eds., 1997).

[52] The Privacy Act of 1974, 5 U.S.C. §552a(a)(2).

[53] Access requests might be possible under the Freedom of Information Act, 5 U.S.C. §552.

acceptable to an EU country worried about the privacy protections for information about its citizens that is exported to the U.S. It could be cured by legislation.

The other shortcoming is a lack of any application of the Act's privacy principles to data disclosed to others. Onward transfer control is not an express part of FIPs, but it is clearly an important concern and an issue directly implied by the *purpose specification* and *use limitation* principles. For example, onward transfer is a major element in the Safe Harbor agreement between EU and the Department of Commerce. The Privacy Act only applies to federal agencies. When a federal agency transfers personal information to a third party, the Act does not apply to the data in the hands of that third party, and the Act's protections are not available.[54] Even if the third party is another federal agency, the Act may not apply if the recipient does not maintain the information in a system of records. The lack of onward transfer provisions in the Act is not something that could be easily fixed through amendment of the law.[55]

[54] The Act may apply in whole to some federal contractors, 5 U.S.C. §552a(m), and in part to some recipients under computer matching agreements, 5 U.S.C. §552a(o).

[55] There are other potential differences between the EU Directive's implementation of FIPs and the Privacy Act. The Act does not cover all personal data held by federal agencies but only applies to personal data held in systems of records. The *routine use* provision in the Privacy Act, 5 U.S.C. §552a(b)(3), might allow more disclosures than would be permitted under EU standards. Also, the lack of an independent supervisory authority could be an issue, although the Office of Management and Budget has a limited supervisory role. Whether any of the differences would be enough to result in a finding of inadequacy is uncertain. A law need only be adequate and not identical in all respects to EU standards.

Sidebar 2.3: The Privacy Act of 1974 Summarized Using FIPs

The Privacy Act of 1974 (5 U.S.C. §552a) applies to all federal agencies and to some agency contractors. The Act does not apply to federal grantees, recipients of federal funds, nonprofits, or other non-federal institutions such as corporations, state government, unions, or individuals. This summary lists each provision of the Act under only one Fair Information Practice Principle. Some provisions could have been listed under more than one principle.

Collection Limitation Principle

Subsection (e)(1) requires an agency to maintain only information about an individual that is relevant and necessary to accomplish an agency purpose.

Subsection (e)(2) requires an agency to collect information to the greatest extent practicable directly from the data subject if the information may be used in an adverse way.

Subsection (e)(7) prohibits an agency from maintaining a record describing how an individual exercises rights guaranteed by the First Amendment unless expressly authorized by law or pertinent to an authorized law enforcement activity.

Data Quality Principle

Subsection (e)(5) requires an agency to maintain all records used to make determinations about an individual with sufficient accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness.

Subsection (e)(6) requires an agency, before disseminating records to any person other than another agency, to make reasonable efforts to assure accuracy, completeness, timeliness, and relevance.

Subsection (p) requires an agency participating in a computer-matching program to verify data used to make adverse decisions and to provide an individual with an opportunity to contest an adverse finding. Subsection (q) prohibits disclosures of records if the requirements of subsection (p) are not being met.

Purpose Specification Principle

Subsection (b) establishes conditions for disclosure of information about an individual to any person outside an agency. The Act specifies disclosures that may be made without the consent of the individual, and it authorizes an agency to define other appropriate disclosures ("routine uses") for each system of records.

Subsection (e)(9) requires an agency to make reasonable efforts to notify an individual when that individual's record is disclosed pursuant to compulsory process.

Use Limitation Principle

Subsection (b)(1) allows an agency to share records about an individual with officers and employees of the agency who have a need for the record in the performance of their duties.

Security Safeguards Principle
Subsection (e)(10) requires an agency to establish appropriate administrative, technical, and physical safeguards to assure the security and confidentiality of personal records and to protect against anticipated threats or hazards.

Openness Principle
Subsection (c) requires an agency to maintain an audit trail ("accounting") of disclosures of personal information from a system of records, including the date, nature, and purpose of the disclosure.

Subsection (e)(3) requires an agency to tell an individual asked to provide personal information about the authority for and purpose of the request, the disclosures permitted, and the effects of not providing the information.

Subsection (e)(4) requires an agency to publish in the Federal Register a complete notice describing the existence and character of each system of records. Subsection (e)(11) requires publication of any new routine uses.

Subsection (e)(12) requires an agency participating in a matching program with a non-federal agency to publish a notice in the Federal Register.

Subsection (o) establishes procedural rules for an agency that uses personal information for computer matching programs

Subsection (r) requires an agency to report new systems of record and about computer matching programs to the Congress and to OMB about.

Individual Participation Principle
Subsection (d) requires an agency to permit each individual to obtain a copy of records about him or herself and to propose amendments to the records if the information is not accurate, relevant, timely, or complete.

Subsection (f) requires an agency to publish rules for the exercise of access and correction rights.

Accountability Principle
Subsection (e)(9) requires an agency to establish rules of employee conduct for, and to provide training on, the privacy rules and requirements.

Subsection (g) establishes civil remedies for an individual whose rights under the Act were violated.

Subsection (i) establishes criminal penalties for violations of the Act.
`
Subsection (u) requires an agency participating in a matching program to establish a Data Integrity Board.

Subsection (v) directs OMB to provide guidance and assistance to agencies.

This summary includes all provisions of the Privacy Act of 1974, except for the exceptions [(subsections (j) and (k)] and the provision regulating transfer of records for archival purposes [(subsection (l)].

The illustration of how the Privacy Act conforms to FIPs should not be taken to suggest that the Act is without its problems. The law is more than 25 years old, and Congress only once amended the law significantly by adding rules governing computer-matching activities.[56] The only independent and comprehensive study of the Act was undertaken by the Privacy Protection Study Commission (PPSC) in 1977,[57] just a few years after the law took effect. A series of reports by the General Accounting Office illuminated the operations of various aspects of the Act in subsequent years.[58] A complete review of the law is beyond the scope of this report, but five of the Act's broader problems will be highlighted. This discussion includes some ideas for change, but these are presented as alternatives for consideration and debate and not as recommendations.

First, the law only applies to agency records maintained in a *system of records*. A *system of records* is a group of records containing personal information from which information is retrieved by individual identifier.[59] The test of whether a set of records is a *system of records* and therefore subject to the Privacy Act is a *factual* test. The answer depends on how the records are actually retrieved. The Privacy Act does not protect a modest (but unknown) amount of personal information maintained by federal agencies if the information fails to meet the retrieval test.

When records were kept in paper files or on mainframe computer systems, the *system of records* approach had its attractions. The concept of *system of records* is unique to the Privacy Act, and it provided a useful way of applying privacy rules broadly to a complex federal bureaucracy maintaining thousand of different types of personal records. However, the shortcomings of the approach were quickly noted. The PPSC's 1977 report suggested abandoning the system of records approach and broadening privacy coverage to all accessible personal information.[60]

Over time, the shortcomings of the system of record concept have become even more apparent. With modern computers and database technologies, record retrieval is no longer a threshold activity that can be clearly predicted in advance. Often, any item of data can be readily retrieved from a database with a few keystrokes. Anyone with access to a database can readily create, augment, merge, or eliminate compilations of personal data. Regardless of its utility when the Act passed in 1974, the modern computer made the *system of records* notion obsolete.

---

[56] Computer Matching and Privacy Protection Act Amendments of 1988, Public Law 100-503.

[57] Privacy Protection Study Commission, *Personal Privacy in an Information Society,* chapter 13 (1977).

[58] See General Accounting Office, *Peer Review: Compliance With the Privacy Act and Federal Advisory Committee Act,* (1991) (GGD-91-48); *Privacy Act: Privacy Act System Notices,* (1987) (GGD-88-15BR); *Privacy Act: Federal Agencies' Implementation Can Be Improved,* (1986) (GGD-86-107); *Privacy Act of 1974 Has Little Impact on Federal Contractors,* (1978) (LCD-78-124); *Impact of the Freedom of Information and Privacy Acts on Law Enforcement Agencies,* (1978) (GGD-78-108); *Data on Privacy Act and Freedom of Information Act Provided by Federal Law Enforcement Agencies,* (1978) (LCD-78-119); *Agencies' Implementation of and Compliance With the Privacy Act Can Be Improved,* (1978) (LCD-78-115); *Federal Bureau of Investigation's Handling and Responsiveness to Freedom of Information Act and Privacy Act Requests,* (1978) (105692); *Timeliness and Completeness of FBI Responses to Requests Under Freedom of Information and Privacy Acts Have Improved,* (1978) (GGD-78-51); *FBI Taking Actions To Comply Fully With the Privacy Act,* (1977) (GGD-77-93); *National Security Agency's Compliance with the Privacy Act of 1974,* (1976) (LCD-77-103).

[59] 5 U.S.C. §552a(a)(5).

[60] Privacy Protection Study Commission, *Personal Privacy in an Information Society,* 504 (1977).

The notices required for a system of records provide a useful way of identifying most federal agency practices for personal data. While the notices might benefit from additional or revised content, preparation of the notices helps agencies organize and identify record-keeping activities affecting privacy. The notices also allow the public to learn about agency data handling practices. Finding another organizing principle for describing federal personal data activities has not been explored. Data that is in a system can be readily described. Unorganized data outside of systems is much harder to find and describe, and the descriptions might be less understandable.

The EU Directive's transparency requirement[61] ties disclosure obligations to the collection of personal data and calls for notices to be provided directly to data subjects. The Privacy Act does that when data is collected directly from a data subject, but its notice[62] is more limited in scope and distributed differently than the *system of record* notice that appears in the Federal Register. Some EU countries require notification, registration, or licensing of personal information processing activities, with the data protection supervisory authority serving as the recipient of notices or registrations or as the issuer of licenses.[63] The publication of system notices is roughly equivalent to notification, and it is possible that *systems of records* could be replaced with published notices that describe personal data processing activities functionally or programmatically rather than by the filing system used for the data. In searching for alternatives, further study of notification systems in other countries might be profitable.[64]

Second, the Act regulates disclosures of personal information from systems of records in several ways. The law identifies a dozen permissible disclosures for all systems of records.[65] However, each record system has its own disclosure characteristics, and it is not practical to define through a general statute how the records from each system can be disclosed. For this reason, Congress gave each agency the authority to define appropriate *routine uses* for each system of records. A *routine use* is a disclosure that is compatible with the purpose for which a record was collected.[66]

The flexibility that the routine use concept gave agencies was important to the functioning of the government. However, the lack of clarity in the statute combined with unclear guidance by the Office of Management and Budget and the lack of continuing oversight may have allowed agencies too much discretion in establishing routine uses that may not be appropriate or necessary. Some see

---

[61] *EU Directive,* at Articles 10-11.

[62] See 5 U.S.C. §552a(e)(3).

[63] The Directive allows considerable flexibility on notification, allowing for simplification or exemption in many instances. *EU Directive,* at Article 18.

[64] The practice of some EU countries of using notification, registration, or licensing has never attracted much interest or support among U.S. privacy advocates. Any such requirement applying to private sector record-keepers would be certain to attract widespread and strong opposition on First Amendment and other grounds. However, any requirement limited to the federal government only would be considerably less controversial, in part grounds because of the existing precedent in the Privacy Act. In Europe, interest in notification, registration, and licensing of private sector databases has diminished somewhat over time because of the cost and complexity of the requirements.

[65] 5 U.S.C. §552a(b).

[66] *Id.* at §552a(a)(7).

the Act's substantive restriction on disclosure as a procedural one only.[67] The *routine use* notion is in need of review and revision.

It is almost certainly necessary to have some administrative mechanism that allows for the identification of permissible disclosures. It would be impossible to rely on the Congress to approve disclosures for all agencies. However, the flexibility in the current approach could be restrained and channeled in a variety of ways, including: 1) clearer statutory standards for what constitutes an allowable disclosure; 2) more standardization of routine uses through OMB mandates; 3) clearer guidance by OMB; 4) more review of new routine uses by OMB, the Congress, or the public; or 5) more advance consultation about routine uses with affected constituencies. In other countries, privacy agencies sometimes serve as independent constraints on overly broad disclosure practices.

Third, the Privacy Act of 1974 and the Freedom of Information Act[68] have some overlapping common purposes. Both laws include records management provisions that direct agencies to publish descriptions of their information processing and record keeping activities. Both laws define procedures under which individuals can request copies of government records. The overlap between the laws is sufficiently large that some agencies combine their FOIA and Privacy Act operations in a single office. It may be possible to achieve greater administrative efficiency and to reduce public confusion by restructuring the two laws to combine common elements. Whether it is actually possible to accomplish a legislative restructuring is uncertain. Proposals for broad changes in access and privacy laws would be certain to attract widespread opposition on many fronts. Narrow proposals for changes in administrative processing of requests or in affirmative publication requirements might be less controversial.

Fourth, oversight and enforcement of the Privacy Act has contributed to many of the ongoing problems with administration of the law. The Office of Management and Budget, which has oversight responsibilities under the Act, has not shown much interest in this mission. The enforcement structure for the Act is discussed later in more detail.

Finally, the Internet created new challenges and opportunities for the Privacy Act. The Internet forced agencies maintaining systems of records on the Internet to provide new types of security. In many respects, however, the security requirements for the Privacy Act are not significantly different or greater than those under other security laws or policies. The Internet provided new opportunities for the covert collection of personal information using cookies and other technologies. The Office of Management and Budget eventually responded, for example, with new directions to agencies on the use of cookies.[69] The Internet also provided opportunities for expanded public notices about privacy. OMB reminded agencies about the need to comply with the notice requirements of the Act

---

[67] Robert Gellman, *Does Privacy Law Work?*, Technology and Privacy: The New Landscape 198 (Philip E. Agre & Marc Rotenberg eds., 1997); *Privacy Protection Study Commission*, Personal Privacy in an Information Society at 517-21 (1977).
[68] 5 U.S.C.§552.
[69] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies on Privacy Policies and Data Collection on Federal websites (June 22, 2000) (M-00-13), at http://www.whitehouse.gov/OMB/memoranda/m00-13.html.

and told them to go beyond its narrow requirements to provide additional online privacy information.[70]

Changing the Privacy Act to reflect changes in information technology resulting from personal computers and computer networks would not be easily accomplished. Changes to the system of records concept, already discussed, would likely be one element. Another complex challenge would be adjusting the exemptions to the Act.[71] Because the exemptions are tied to system definitions, any change in the way that systems are defined would require changes to the exemptions. Freedom of Information Act style exemptions tied to records rather than systems might work for regulating first party access, but it is not clear how such an approach would work for the many systems exempted from other requirements. Also, the existing provision now in the law[72] that depends on an agency official responsible for a system of records probably would require reconceptualization.

To date, there has been little discussion about a new model for regulation of agency privacy activities in the Internet era. The lack of a new model is a significant impediment to updating the Act. Computer networks have fundamentally changed the way that personal information is handled by federal agencies. Networks offer new threats to privacy that existing legislation or practice does not address. Networks also offer greater opportunities for control and oversight of activities affecting privacy. For example, the Act requires that agencies maintain disclosure histories for personal records,[73] but it appears that compliance with this requirement has been spotty. A computer system can readily meet this requirement if properly programmed. The Internet may also allow agencies to tailor some privacy activities more to individual needs. For example, an agency may disclose personal information from a system of records with the written consent of an individual.[74] Agencies do not appear to make widespread use of this authority. However, the Internet would make it easier to collect and manage consents to make disclosures.

Turning to other federal privacy laws, most of these laws apply to non-federal record-keepers. Even the privacy laws enacted before the creation of FIPs contain FIP elements. Only a few other U.S. laws fill the FIPs framework as completely as the Privacy Act of 1974. The accompanying chart in Sidebar 2.4 lists major privacy laws and indicates whether they address each element of FIPs.

---

[70] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies on Privacy Policies on Federal Websites (June 2, 1999) (M-99-18), at http://www.whitehouse.gov/omb/memoranda/m99-18.html.
[71] 5 U.S.C. §552a(j) & (k).
[72] 5 U.S.C. §552a(e)(4)(F).
[73] 5 U.S.C. §552a(c).
[74] 5 U.S.C. §552a(b).

Sidebar 2.4: Major Federal Privacy Laws And FIP Principles

PrivacyLaw	Collection Limitation	Data Quality	Purpose Specification	Use Limitation	Security Safeguards	Openness	Individual Participation	Accountability
Privacy Act of 1974 (1)	X	X	X	X	X	X	X	X
Fair Credit Reporting Act (2)	X	X	X	X		X	X	X
Family Educational Rights and Privacy Act (3)	X		X	X		X	X	X
Cable Communications Policy Act (4)	X	X	X	X	X	X	X	X
Video Privacy Protection Act (5)		X	X	X		X		X
Driver's Privacy Protection Act (6)			X	X				X
Telecommunications Act (7)			X	X			X	
Children's Online Privacy Protection Act (8)	X	X	X	X	X	X	X	X
Gramm-Leach-Bliley (9)			X	X	X	X		X
Health Insurance Portability & Accountability Act (10)	X		X	X	X	X	X	X

(1) 5 U.S.C. §552a.
(2) 15 U.S.C. §1681 et seq.
(3) 20 U.S.C. §1232g. Also known as the Buckley Amendment.
(4) 47 U.S.C. §551.
(5) 18 U.S.C. §2710. Also known as the Bork Bill.
(6) 18 U.S.C. §2721 et seq.
(7) 47 U.S.C. §222.
(8) 15 U.S.C. §6501 et seq.
(9) 15 U.S.C.§6801 et seq. Also known as the Financial Institutions Modernization Act.
(10) 42 U.S.C. §1320d-2 note; 45 CFR Parts 160 & 164. The 1996 Act (often referred to as HIPAA) established a three-year timetable for health privacy. If Congress did not pass legislation within three years, the Act authorized the Secretary of Health and Human Services to issue health privacy regulations. On December 28, 2000, the Secretary published final regulations establishing standards for the privacy of individually identifiable health information. The chart reflects the requirements in those regulations. The HIPAA health privacy rule is the only rule included in the chart.

Chart Notes

This chart summarizes how major privacy laws and rules address Fair Information Practices. Each marked box means that some provision of the law/rule covers the corresponding Fair Information Practice principle in some way. For example, both the Privacy Act of 1974 (a law that applies to federal agencies) and the Family Educational Rights and Privacy Act (a law that applies to educational agencies and institutions receiving federal funds) contain at least one provision for accountability. The Privacy Act of 1974 achieves accountability through several measures, including a requirement for employee training, civil remedies, criminal penalties, and administrative oversight. The Family Educational Rights and Privacy Act achieve accountability through the termination of federal financial assistance and administrative oversight. Each law has accountability measures, but the measures differ considerably.

The scope of some laws is limited. For example, the Privacy Act of 1974 applies to personal records maintained by federal agencies (and some federal contractors) in *systems of record* but not to personal information maintained in other ways. The Cable Communications Policy Act applies to personal information collected by

cable operators, but others who provide similar television services through direct broadcast satellite or in other ways are not subject to the same rules.

The Privacy Act of 1974, the Cable Communications Policy Act, the Children's Online Privacy Protection Act, and the Fair Credit Reporting Act reflect the broadest coverage of FIPs. Congress originally passed the Fair Credit Reporting Act in 1970, three years before the first definition of FIPs.

The element of FIPs most often missing is *security safeguards*. The laws that address security do so in a summary fashion by requiring record-keepers to maintain adequate security. None of the laws includes detailed security requirements.

The chart identifies a law as addressing a FIP principle as long as it includes even a minimal reference to the policy. For example, the Cable Communications Policy Act directs cable operators to take "such actions as are necessary to prevent unauthorized access." [(47 U.S.C. §551(c)(1)]. This was sufficient to qualify as addressing the *security safeguards* principle.

Several privacy laws have not been included in the chart. The Right to Financial Privacy Act (29 U.S.C. §3401 et seq.) establishes procedural rules governing access by federal government agencies to customer records of a financial institution. The Electronic Communications Privacy Act of 1986 is a complex criminal law with titles addressing the interception of electronic communications, stored wire and electronic communications and transactional records access, and pen registers and trap and trace devices. The Privacy Protection Act (42 U.S.C. §2000aa et seq.) establishes procedures for searches and seizures of work product materials from newsrooms and does not address the protection of individually identifiable personal information. These three laws were omitted because they primarily regulate the conduct of government in seeking access to information from designated third party record-keepers. The Telephone Consumer Protection Act (47 U.S.C. §227) contains several specific restrictions on the use of automated telephone equipment that might be characterized as privacy protections. The one provision expressly identified in the law as a protection of subscriber privacy rights [(§227(c)] requires the Federal Communications Commission to establish a *do-not-call* system for telephone solicitations. Of all these privacy-related statutes, only the Electronic Communications Privacy Act imposes a more general duty on electronic communication service providers to limit the use and disclosure of the content of communications.

Three major lessons can be learned from the chart. First, the chart shows the value of FIPs for describing common features of privacy laws and for easily identifying broad differences. To be sure, not all of the laws implement common privacy principles in the same way. For example, the FIP principle of accountability can be accomplished in many different ways. Accountability can be addressed or accomplished through criminal penalties, civil or administrative remedies, cutoff of federal funds, arbitration, staff training and discipline, or in other ways. A mark in the accountability box on the chart simply means that some accountability measure is included in the law.

Second, nothing in FIPs mandates either a broad or narrow application of the principles. Most other national privacy laws apply FIPs across the board to public and private record-keepers. This is not the case in the United States. U.S. private sector privacy laws are usually narrow in scope, applying to a defined class of record-keepers and to a specific set of records.[75] Only the Privacy Act of 1974 applies broadly to many types of records, albeit only records maintained by a single class of record-keepers, namely federal agencies. FIPs are compatible with across-the-board application to multiple record-keepers both public and private. FIPs are also compatible with narrow application to specific public or private sector record-keepers. FIPs are a reasonable starting point for privacy analysis no matter how broad or narrow the scope of the inquiry is.

Third, FIPs do not have to be implemented as a complete set. U.S. privacy laws use elements of FIPs in different combinations. It is possible to mix and match FIPs in almost any combination. Whether this produces more effective privacy laws is a separate question. Privacy laws passed by the Congress and other U.S. legislative bodies typically incorporate FIPs to some degree, but official recognition of FIPs as reflecting core values has been only occasional, at best.[76]

Bringing existing U.S. privacy law into full compliance with FIPs could present major substantive and political challenges. Existing laws offer significant diversity in their implementation of FIP elements. Aside from political opposition, attempts to change the laws would need to confront the absence of any formal agreement on what the United States wants to accomplish through its privacy legislation. The discussion later in this report about the challenges of implementing FIPs illustrates the wide range of policy choices that would be required. If the laws were to be changed piecemeal, existing differences in approach would likely be extended, and the problems raised by conflicts between the laws in areas where they overlap would be exacerbated. Changing a law to meet FIP standards would be difficult enough as a technical matter of finding ways to implement specific

---

[75] In some instances, sectoral borders in U.S. laws are drawn so precisely that the law applies to one set of record-keepers and not to another despite fundamental similarities in the records that both maintain. For example, the Video Privacy Protection Act limits the use and disclosure of records pertaining to the sale and rental of videos. The law is intended to protect the First Amendment interests of video customers. However, no federal law affords similar protection to the First Amendment interests of book or magazine consumers. See Robert Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules,* 41 Villanova Law Review 129, 146 (1996). Whether the result is a shortcoming or a careful application of privacy policy to a specifically defined problem is a matter of judgment.

[76] See, e.g., H.R. Rep. No 103-601 Part 5, 103rd Congress at 81-82 (1994) (Report to accompany H.R. 3600, the Health Security Act).

policies. Given the political interest in reforming any existing law, however, the necessary choices could be accomplished through familiar mechanisms.

The larger challenge would be making privacy laws compatible with common standards. If U.S. privacy laws were to be changed to meet common standards, the standards would first have to be chosen. However, there has been little movement in the United States toward agreement on common privacy standards. The legislative process does not readily provide a way for legislation originating in different committees and in different Congresses to be compatible. The absence of any fundamental consensus about the objectives of a U.S. privacy policy is the most significant impediment. The United States can learn much from the way that other nations have written and implemented their privacy laws, but the development of a political consensus must be accomplished in other ways.

2.4 Criticism of Fair Information Practices

Privacy laws and policies have their share of critics. It is not the purpose of this report to evaluate arguments about the merits of privacy. However, because of the broad international acceptance of FIPs as an organizing methodology for information privacy policies and laws, it is worthwhile to consider some of the criticism of FIPs. The goal is to provide other perspectives on the international consensus by looking at supposed shortcomings of the principles as opposed to criticism of how FIPs are interpreted and applied. Any discussion about the criticism of implementation of FIPs under various laws would be considerably longer.

2.4.1 Critics Who Believe that FIPs are Incomplete

One of the leading critics of the OECD Guidelines and of FIPs is Roger Clarke, an Australian privacy and security consultant.[77] Clarke has written[78] and spoken about inadequacies with FIPs. He organizes his criticism into broad categories: fundamental deficiencies known at the time of the OECD Guidelines, and deficiencies that emerged over time.

Clarke's analysis of the fundamental deficiencies with the OECD Guidelines (and with FIPs) include:

1. The permissive approach taken to exemptions and exceptions, including the possibility of exemptions for national defense, national security, and law enforcement. Every national law, including the U.S. Privacy Act of 1974, contains multiple exemptions for some government functions.
2. The danger that privacy protections may be subverted through the concentration of business functions into large, multi-function organizations that share personal data broadly. The current U.S. debate over privacy protections for financial institutions included in the

[77] Available at http://www.anu.edu.au/people/Roger.Clarke.
[78] See, e.g., *Beyond the OECD Guidelines: Privacy Protection for the 21st Century,* (2000), at http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html.

Gramm-Leach-Bliley legislation centers in part over proper scope of data sharing between affiliates of a bank or other covered organization. The law gives consumers a choice about sharing with third parties but not with affiliates.

3. The failure to address the potential inadequacies of uncontrolled self-regulation. The OECD Guidelines support self-regulation with little qualification and without specifying standards for appropriate self-regulation. Implementation of self-regulatory regimes under some national laws includes some constraints and controls.
4. The failure to require the creation of a privacy agency. The EU Directive, however, requires each Member States to have a *supervisory authority,*[79] and most national privacy laws (and some provincial laws) include a requirement for a privacy agency.
5. The general policy of openness with respect to data processing does not require *justification* of processing, purpose, or function. Clarke notes, as have others, that the U.S. Privacy Act of 1974 gives agencies nearly boundless discretion to define new disclosures ("routine uses") for existing record systems.[80]

The OECD Guidelines and FIPs both reflect the information technology of the 1960s and 1970s. Clarke's identification of deficiencies with the OECD Guidelines (and with FIPs) that emerged over time and because of changing technologies and institutions include:

1. The failure of the openness principle to keep up with the convergence of communications and computing technology, and the resulting blossoming of data sharing among and between organizations.
2. The use of automated processes to make decisions about individuals based on their personal information. The EU Data Protection Directive places some limitations and requirements on automated decision-making about individuals.[81]
3. The failure to adequately address the use of multipurpose identifiers or to recognize the right of individuals to use different identifiers for different purposes. The current debate in the United States over the widespread use of the Social Security Number as a universal identifier is evidence on the relevance of this point.
4. The failure to address the use of identification tokens (e.g., identification cards) or biometrics.
5. The failure to establish a right to conduct transactions anonymously or pseudonymously. The scope of any anonymity rights would be highly controversial.

---

[79] *EU Data Protection Directive,* at Article 28.
[80] See, e.g., House Committee on Government Operations, *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress*, H.R. Report No. 98-455 (1983).
[81] *EU Data Protection Directive,* at Article 15.

6. The concentration on information privacy and the failure to recognize other elements of privacy, including freedom from surveillance, the need for private space to conduct personal affairs, and the need for physical privacy of an individual or bodily sample.

In 1999, the former chair of the OECD Committee that developed the 1980 Privacy Guidelines spoke at an international privacy conference about the adequacy of the Guidelines.[82] Mr. Justice Michael Kirby of the High Court of Australia took note of the many changes brought about by new computer and communication technologies. He said that the Guidelines were showing their age and suggested that it may be time for a review. Among new rights that he mentioned as ripe for review were:

1. A right not to be indexed.
2. A right to encrypt personal information effectively.
3. A right to fair treatment in key public infrastructures so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy.
4. A right to human checking of adverse automated decisions and a right to understand such decisions.
5. A right, going beyond the aspiration of the 'openness principle', of disclosure of the collections to which others will have access and which might affect the projection of the profile of the individual concerned.

Some of the points made by both Mr. Justice Kirby and Mr. Roger Clarke reflect concerns about how FIPs have not necessarily kept pace with modern information technology. The lag between technology on the one hand and law and policy on the other is, of course, not unique to privacy or to data processing technology. Kirby also mentioned developments with genetics and offered them as another example of a development with important privacy implications that postdated the Guidelines. He suggested that there might be a need for an ongoing review of the Guidelines to consider advances of technology and their implications for privacy. He asserted "it would certainly be remarkable if the words written in 1980 were to be the last expression of the international principles for personal privacy and data protection."[83] Still, he concluded that the OECD "framework of privacy principles . . . has been extraordinarily successful and remarkably enduring."[84]

---

[82] Available at http://www.pco.org.hk/english/infocentre/conference.html.
[83] *Id.*
[84] *Id.* See also Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada, *A Report to the 22nd International Conference of Data Protection Commissioners: Should the OECD Guidelines Apply to Personal Data Online?, (2000), at http://www.ipc.on.ca/english/pubpres/papers/oecd.htm.*

2.4.2 Critics Who Believe Fair Information Practices are too Strong

Criticism of FIPs can be inferred from policy statements of other participants. For example, restatements of FIPs without all traditional elements can be viewed as a rejection of the breadth of the principles. An example comes from the Federal Trade Commission.[85] In 2000, the Commission recommended that consumer-oriented commercial websites that collect personal identifying information from or about consumers online should be required to comply with "the four widely-accepted fair information practices." The FTC's version of FIPs includes notice, choice, access and correction, and security. The *choice* principle is not a core element of traditional FIPs. *Choice* means that consumers would have to be offered some ability to say how their personal data may be used for secondary purposes. It appears that the FTC modeled its *choice* principle on privacy policies prompted by elements of the American business community. Some in the business community quickly jumped on the FTC's restatement of FIPs to claim that the FTC's version is now "well-established."[86]

The FTC statement of FIPs does not address the *collection limitation* or *data quality* principle. The *accountability* principle is not expressly mentioned, but it is clearly part of the FTC's proposal since the Commission would enforce the legislation that it proposed and that enforcement would provide accountability. The other missing principle is that of *purpose specification*. The Commission's *choice* principle appears to be a partial substitute. What is absent is any requirement that a record-keeper specify the purposes for data collection and that subsequent use or disclosure be limited to those purposes and other closely related purposes.

Interestingly, the Children's Online Privacy Protection Act, which the FTC enforces, addresses all traditional elements of FIPs in some manner. However, the Commission did not recommend that all elements be included in proposed legislation applying to a broader set of website operators and data subjects. Nor did the Commission explain why it did not recommend enactment of all FIPs. The Commission's formulation of FIPs was compatible with some similar formulations from parts of the American business community. Other parts of the business community would probably view the FTC's version of FIPs as still too strong. Privacy advocates, of course, have other perspectives. With the membership changes at the Commission at the beginning of the Bush Administration in 2001, it now appears that a majority of FTC members do not support privacy legislation of any sort.

Trade association restatements of FIPs also follow the pattern of leaving out elements of FIPs without explanation. The Online Privacy Alliance, a cross-industry coalition of more than 80 global companies and associations committed to promoting the privacy of individuals online, has one of the more complete statements of FIPs.[87] The Alliance's *Guidelines for Online Privacy Policies* include

---

[85] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace,* (May 2000), at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[86] See, e.g., *Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Information Location Practices,* (Nov. 22, 2000) (Proceeding 01-72), at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6512158796.

[87] Available at http://www.privacyalliance.org/resources/ppguidelines.shtml.

five elements: 1) Adoption and Implementation of a Privacy Policy; 2) Notice and Disclosure; 3) Choice/Consent; 4) Data Security; and 5) Data Quality and Access. Accountability measures are mentioned as part of the *notice and disclosure* element. The *data quality and access* element is deliberately unclear about the scope of access and correction rights. The *choice/consent* element is similar to that adopted by the FTC.

A less complete set of privacy elements can be found in the "four traditional privacy protection practices"[88] of the Direct Marketing Association (DMA). The DMA is the largest trade association for users and suppliers in the direct, database, and interactive marketing fields. The four DMA elements are:

1. Provide customers with notice of their ability to opt-out of information exchanges;
2. Honor customer opt-out requests not to have their contact information transferred to others for marketing purposes;
3. Accept and maintain consumer requests to be on an in-house suppress file to stop receiving solicitations from your company; and
4. Use the DMA Preference Service suppression files.

Essentially, these four elements are simply notice and choice (i.e., opt-out). The second, third, and fourth elements of the DMA privacy practices are variations on the notion of opting out. Separately, the DMA provides some accountability measures through an internal ethical practices committee. The DMA privacy policy does not address any of the other FIPs elements.

Professor Fred H. Cate, an academic critic of privacy, proposed that the United States enact an omnibus privacy law limited to three basic elements: 1) Notice; 2) Consent; and 3) Accountability. He rejects other elements of FIPs as unworkable, undesirable, and, perhaps, unconstitutional. A high-level of EU-style privacy protections would, in his view, result in a high degree of intrusion into the activities and expression of individuals and institutions.[89] Cate and other scholars and analysts believe that privacy protections face significant obstacles under the free speech policy of the First Amendment to the U.S. Constitution.

[88] Available at http://www.the-dma.org/library/privacy/privacypromise.shtml.
[89] Fred H. Cate, *Privacy in the Information Age,* 111-112 (1997).

2.5 Other Approaches to Privacy

2.5.1 Privacy Protection Study Commission Approach to Privacy

The law that enacted the Privacy Act of 1974 also created a temporary privacy study commission.[90] The creation of the Privacy Protection Study Commission (PPSC) was a compromise between the Senate, which wanted a permanent privacy agency, and the House, which opposed a permanent agency.[91] The PPSC had a broad mandate to consider privacy issues in the federal government, state governments, and private sector.

The PPSC issued its final report in 1977.[92] The Commission offered dozens of specific recommendations for legislation and other actions. Few of those recommendations received serious consideration by the Congress. The PPSC based its recommendations on three broad objectives for an effective privacy protection policy:

- To create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return (*to minimize intrusiveness*);
- To open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it (*to maximize fairness*); and
- To create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual (*to create legitimate, enforceable expectations of confidentiality*).[93]

Arguably, these three objectives could be seen as alternative privacy organizing principles to FIPs. The PPSC itself noted that its objectives "subsume and conceptually augment" the fair information practice principles from the 1973 HEW advisory committee.[94] Many of the Commission's specific recommendations could be fairly characterized as implementations of FIPs principles as well as of the Commission's stated objectives.

Whether and how the PPSC objectives differ in any significant way from FIPs may not be worth discussing. The PPSC framework for privacy disappeared quickly from public view and has not substantially contributed to domestic or international debate over privacy in the last two decades.[95]

---

[90] Public Law 93-579, §5, 88 Stat. 1907 (1974).
[91] Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions,* VI Software Law Journal 199, 216-17 (1993).
[92] Privacy Protection Study Commission, *Personal Privacy in an Information Society,* (1977).
[93] *Id.* at 14-15.
[94] *Id.* at 15.
[95] In 1979, the Carter Administration responded to the report of the PPSC by offering broad legislative proposals for privacy. Even the Carter Administration did not adopt the PPSC privacy framework, relying instead on fair information practices and limits on the government as the two main organizing themes for its proposals. I.J. Carter, *President's Message to Congress on Proposals Protect the Privacy of Individuals*, Public Papers of the Presidents 582 (1979).

While the HEW Advisory Committee's report[96] continues to be used and cited, the PPSC's statement of objectives for an effective privacy policy work has been forgotten. The PPSC's report is worthy of mention principally because it was the only comprehensive study of privacy in the United States in several decades.

2.5.2 Privacy Standards

Canada took a different approach to privacy beginning in the early 1990s when it started a process to establish a *privacy standard*. A standard is a set of characteristics or quantities that describes features of a product, process, service, interface, or material.[97] Many international standards are technical specifications for products. However, the Canadian privacy standard was similar to the *generic management system standards* promulgated by the International Organization for Standardization (ISO) for quality management standards and for environmental standards.[98] These ISO standards establish requirements for what an organization must do to manage processes influencing quality (ISO 9000) or the processes influencing the effect of its activities on the environment (ISO 14000).[99]

The Canadian Standards Association (CSA) led the Canadian privacy effort. Representatives of all stakeholders, including government, business, and consumer interests participated in the development of the standard. The starting point was the OECD Privacy Guidelines.[100] Despite the broad representation of different interests in the drafting committee, the standard was eventually adopted without dissent. CSA published the Model Code as a National Standard of Canada in 1996.[101]

Not surprisingly, the CSA standard follows the international consensus on FIPs. The CSA standard has ten interrelated principles that can be readily mapped to the OECD Guidelines. The CSA standard is set out as a sidebar to illustrate the similarities. Like the Guidelines, the CSA privacy standard includes a commentary designed to explain how the principles should be interpreted and applied. An important difference between a standard and a sectoral code of practice is that the standard can be subject to certification, registration, and audit procedures used for management standards.[102]

---

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

[97] National Research Council, *Standards, Conformity Assessment, and Trade,* 9 (1995).

[98] Colin J. Bennett, *Adequate Data Protection by the Year 2000: The Prospects for Privacy in Canada,* in 11 International Review of Law Computers & Technology 79, 81 (1997).

[99] International Organization for Standardization, *ISO 9000 and ISO 14000 in Plain Language*, at http://iso.org/iso/en/iso9000-14000/tour/plain.html.

[100] Canadian Standards Association, at http://www.qmi.com/registration/privacy/default.asp?load=content&language=English.

[101] Canadian Standards Association, *Model Code for the Protection of Personal Information,* (CAN/CSA Q830-96), at http://www.qmi.com/registration/privacy/default.asp?load=content&language=English. For some history and background on the CSA Privacy Standard and Canadian legislation, see generally Stephanie Perrin et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide,* (2001).

[102] Colin J. Bennett, *Adequate Data Protection by the Year 2000: The Prospects for Privacy in Canada,* in 11 International Review of Law Computers & Technology 79, 80-1 (1997). See also Jos Dumortier & Caroline Goemans, *Data Privacy and*

The more recent history of the CSA standard is even more remarkable than the unanimous adoption of the standard itself. The Government of Canada adopted the standard as the basis for its private sector privacy legislation and enacted the standard directly into law in 2000.[103] In a few places, the Canadian law specified exceptions and alterations to the published standard. For the most part, however, the Canadian Parliament accepted the CSA Model Code without change. This concept of incorporating a management standard directly into law is unique[104] among national privacy laws.

The use of standards for privacy continues to percolate internationally, although the notion is much more controversial worldwide than it proved to be in Canada. In 1997, the European Committee for Standardization (known as *CEN*) established the Information Society Standardization System (ISSS) with the goal of bridging the gap between formal and informal standardization for information and communications technologies. CEN/ISSS sponsors the Initiative for Privacy Standardization in Europe, which is currently considering the idea of a privacy standard. The argument for a European standard is that because privacy issues rise above national law, global corporations need auditable codes of practice or standards to satisfy customers, partners, and national authorities.[105] However, there appears to be "tremendous aversion" among large corporations to a privacy standard similar to the ISO 9000 management standard.[106]

ISO has also struggled with the idea of a privacy standard. The ISO Committee on Consumer Policy (COPOLCO) passed several unanimous resolutions asking the ISO Council to develop an international standard for the protection of privacy. The Canadian privacy standard provided the inspiration for the COPOLCO initiative. The latest COPOLCO recommendation calls for work on an international standard for consumer protection in electronic commerce, including protection of personal data. Past recommendations generated considerable industry opposition. Discussions about international privacy standards continue today in several international forums, including ISO,[107] with a high level of controversy.

Whether standards will play a role in the future of international privacy efforts remains to be seen. The coordination of international standards efforts to address privacy has been limited, and multiple efforts proceed fitfully under the auspices of different organizations. It will take more time to see if the privacy standards movement will become important.

Standardization: Discussion Paper Prepared for the CEN/ISSS Open Seminar on Data Protection, (March 2000), at http://www.law.kuleuven.ac.be/icri/papers/doctrine/cen-paper.pdf (benefits of standards include streamlined methods and procedures for creation, maintenance, distribution of rules; balanced representation of all interests, including consumers; standards have a specific toolkit of enforcement mechanisms, including auditing, certification, and reporting).

[103] Personal Information Protection and Electronic Documents Act, R.S.C., ch. 5 (2000) at Schedule 1, at http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

[104] Stephanie Perrin et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide,* xv (2001).

[105] Initiative on Privacy Standardization in Europe, *Working Draft* at 5.6 (June 2001) (CEN/ISSS), at http://www.cenorm.be/isss/Projects/dataprotection/ipse/ipsefinalversion-29june2001.pdf.

[106] *Id.* at 5.9.

[107] *Id.* at 4.3 & 4.4.

Sidebar 2.5: Principles Set Out in the National Standard of Canada Model Code for the Protection of Personal Information[108]

Principle 1 – Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Principle 2 – Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 – Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 – Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 – Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Principle 6 – Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 – Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 – Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9 – Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 – Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

[108] Personal Information Protection and Electronic Documents Act, R.S.C., ch. 5 (2000) at Schedule 1, at http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

2.5.3 Information Infrastructure Task Force

During its first term, the Clinton Administration established the Information Infrastructure Task Force (IITF), a cabinet level group chaired by the Secretary of Commerce with representatives from most cabinet departments. The Task Force had an Information Policy Committee and a Privacy Working Group.

The Privacy Working Group developed a set of privacy principles that were designed to be consistent with "the spirit of current international guidelines, such as the OECD Guidelines."[109] The principles identified three fundamental values: information privacy, information integrity, and information quality. Once again, a privacy policy review produced a set of principles that roughly mirrored some standard FIPs.

The Privacy Working Group added three new thoughts. First, individuals should be able to safeguard their own privacy by having the opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions. Second, individuals should have the opportunity to remain anonymous "when appropriate." Third, information users should educate themselves and the public about how information privacy can be maintained. The use of encryption and anonymity has been controversial for many years, raising conflicts over law enforcement, national security, and control of technology. Recent terrorist activities in the United States have rekindled these debates. The suggestion for education about privacy did not include a plan or resources for implementation. Asking users to educate themselves assigns responsibility to no identifiable institution.

It is not clear that the report of the Privacy Working Group had much influence on activities inside or outside the Clinton Administration. The Group was chaired by a succession of civil servants and not by political appointees from the Administration. Nevertheless, its report shows a continued reliance on core FIPs principles for the development of privacy policy in the United States, with recommendations for limited expansion of core principles.

2.5.4 Others

FIPs are not necessarily the only source for substantive rules regarding information privacy. Different approaches have been suggested. Some are being implemented but others remain mostly theoretical. The nature of some approaches, however, the establishment of substantive privacy rules. Instead, they propose more procedural ways to allow record subjects and record-keepers to address privacy.

---

[109] Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information,* at Introduction (June 1995), at http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html.

2.5.4.1 Property Rights

Professor James Rule and computer scientist Lawrence Hunter observe that while we have more legislation and policy aimed at protecting privacy, we also have more unchecked appropriation of personal data.[110] They propose a different privacy protection mechanism: a property right over commercial exploitation of personal information. No information could be sold or traded from any personal data file for commercial purpose without the express consent of the data subject. Rule and Hunter envision the establishment of *data rights agencies* to represent individuals in the commercial marketplace. Individuals who want to allow the use of their information in exchange for royalty payments could do so using a data rights agency as a personal representative. Consumers willing to accept the consequences could even prevent the disclosure of their information to credit bureaus, a type of disclosure that occurs today without consumer notice or consent. Rule and Hunter see the need for legal safeguards that would, for example, prevent the denial of health care to an individual who declines data transfers for commercial purposes.

The Rule/Hunter proposal raises some practical, legal, and constitutional questions. The authors themselves recognize that there are practical issues but believe that they can all be adequately addressed. Even accepting the proposal as presented, it does not address privacy concerns that extend beyond the sale of data for commercial purposes or that relate to non-commercial and governmental activities. The scope of privacy protections – limited to commercial data sales and data subject choice – is narrow.

Others have also explored the extent to which property or intellectual property rights might provide protections for privacy interests. The property and intellectual property regimes have different purposes and different objectives, and each would have different consequences for privacy. Not all analysts agree that the rationale for granting individuals property rights in personal data is fundamentally compatible with the traditional rationale for granting property protection to an information resource.[111] Pamela Samuelson, a leading copyright expert, suggests that contracting (licensing) might do a better but not complete job in addressing the different and multiple interests that individuals have in their personal information.[112] The private resolution of economic interests through contracting[113] offers another regime for determining privacy interests.

---

[110] James Rule & Lawrence Hunter, *Toward Property Rights,* Personal Data, Visions of Privacy: Policy Choices for the Digital Age (Colin J. Bennett & Rebecca Grant eds., 1999). Others have made similar proposals. See, e.g., John Hagel III & Jeffrey F. Rayport, *The Coming Battle for Customer Information*, Harvard Business Review 53 (Jan.-Feb. 1997).

[111] See, e.g., Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection In Intellectual Property Lore*, Stanford Technology Law Review VS 8, 1999, at http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_8/; Pamela Samuelson, *Privacy as Intellectual Property*, Stanford Law Review 1125, 52 (2000).

[112] Pamela Samuelson, *Privacy as Intellectual Property*, Stanford Law Review 1125, 52 (2000). ("Work must continue on evolving norms about appropriate and inappropriate uses of personal data, on persuading firms that the trust necessary for electronic commerce to flourish requires the interests of individuals in information privacy to be given appropriate deference, and on adapting the technological infrastructure of cyberspace so that information privacy becomes easier to achieve.").

[113] Joel R. Reidenberg, *Setting Standards for Fair Information Practices in the U.S. Private Sector*, Iowa Law Review 497, 80 (1995) (discussing limits of contractual approaches).

Regardless of the merits of property rights (or contracting) for privacy, substantive privacy policies would not be directly established by law or by policy. For the most part, the choices about protecting privacy would be made on a case-by-case basis by the data subject who is the owner of the "property" (or the grantor of the license). The range of choices may be shaped, at least in part, by the statutory or other framework that established the property right or contracting process. If, for example, the law required that transactions include (or not include) security standards, then some substantive standards would be established. The enforcement scheme for the law would also be important. Contracting might bring with it concepts like unconscionability that could impose outer bounds on contract terms and that might protect against unreasonable exploitation of data subjects.

However, to the extent that the privacy protection framework depended on the individual choices of data subjects and the willingness of record-keepers, substantive policies have the potential to be variable. In theory, each individual could establish and seek to negotiate terms with each record-keeper. It is likely, though, that the high cost of negotiation under any regime relying on individual choices might lead to standardization of privacy terms. If, as Rule and Hunter suggest, data rights agencies would arise, they might become vehicles for establishing broader privacy policies. Another possibility is the establishment of default rules through legislation that could then be varied as agreed by the parties to any transaction or activity.

Property rights for privacy interests remain almost entirely a theoretical notion. The closest implementation (and a partial one at best) today comes when record-keepers offer *choice* to consumers. Some in industry present *notice and choice* as a "complete" privacy policy. Choice may be a source of privacy policies, but only to the extent that data subjects can make a choice. When the choice offered by a record-keeper to data subjects only covers limits on some secondary uses and disclosures of personal data, it is difficult to characterize the activity as a full privacy policy. Principles of access/correction, collection limitation, security, and others are rarely included when choice is available.

The desire of record-keepers for standardization narrows the options presented to data subjects to those that the record-keepers are willing to offer. Another factor limiting the range of choices is the willingness of data subjects to make decisions. It is unlikely that many individuals would be willing or pleased if asked to make numerous record keeping choices for each third party record-keeper that maintains personal information about them. The number of third party record-keepers with information about the average individual could easily be measured in the dozens.

One area where statutory rules are likely to remain essential is with the collection, maintenance, use, and disclosure of personal information by government. The number, size, and scope of responsibilities for federal agencies make it unlikely that the full range of privacy policies will be practical for routine negotiation between agency and data subject. The same is true for most state and local agencies. It may be possible, however, to give data subjects the ability to decide if government can disclose personal information for non-essential secondary purposes. Technology may support the exercise of individual choice in some governmental privacy matters. One federal

statute already mandates the exercise of individual choice about disclosure of state government records.[114]

2.5.4.2 Privacy Enhancing Technologies

Another approach to establishing substantive rules about privacy is to use technology to help define and mediate privacy interests. Privacy enhancing technologies (PETs) refer to technical and organizational concepts that aim at protecting personal identity.[115] For present purposes, PETs must be distinguished from data security, which is aimed at protecting the processing of data against loss and against unauthorized destruction, modification, use, access, and disclosure. PETs may be relevant to security, but the interest here is in how they support other privacy protections.

PETs may seek to eliminate the use of personal data or to give the data subject greater control over his or her own data.[116] Encryption is one type of PET, but many other types are in use or are conceivable. For example, subway fare cards and telephone calling cards that store value and are sold without identification of the purchaser are a form of PET. The automated destruction of a transaction record at a fixed time after completion is another PET. These types of PETs avoid defining the substance of privacy because no identifiable records exist.

PETs can also enhance other privacy principles, such as those found in FIPs.[117] For example, the principle of openness may be furthered by creating a way for data users to learn about the privacy practices of websites. A leading example is the Platform for Privacy Preferences Project (P3P), sponsored by the World Wide Web Consortium (W3C).[118] W3C created P3P to serve as an industry standard that will allow users to gain more control over the use of personal information on websites. P3P-enabled websites describe their privacy policies in a standardized, machine-readable format. P3P-enabled browsers can read a website's privacy policy and compare it to a user's own established set of privacy preferences. The user can be alerted to any differences and can make choices about how or whether to proceed when informed that a website's privacy policies are not consistent with the user's preferences. It is not certain, however, that P3P offers enough flexibility and precision to describe the nuances of a website's privacy policy. In some instances, a written privacy policy must

---

[114] The Driver's Privacy Protection Act, 18 U.S.C. §2721 et seq., gives data subjects a choice about whether their records can be disclosed for marketing and other purposes. As originally enacted, the Act gave data subjects a negative choice (or opt-out). Congress amended the Act in 1999 to require an affirmative choice (or opt-in).

[115] Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, Technology and Privacy: The New Landscape 125 (Philip E. Agre & Marc Rotenberg eds., 1997). PETs are sometimes contrasted against PITs, or privacy-*invasive* technologies. See, e.g., Remarks of Ann Cavoukian, Ontario (Canada) Information and Privacy Commissioner, MBS Access & Privacy Conference (Oct. 1, 1999), at http://www.ipc.on.ca/english/pubpres/speeches/mbs-99.htm, ("Privacy-Invasive Technologies . . .are technologies that can be used to undermine privacy by tracking, profiling, or facilitating surveillance of individuals.").

[116] For additional views on the role of PETs, reference Information and Privacy Commissioner, Ontario Canada & Registratiekamer (Dutch Data Protection Authority), The Netherlands, *Privacy-Enhancing Technologies: The Path to Anonymity,* (1995) (Volume I), at http://www.ipc.on.ca/english/pubpres/papers/anon-e.htm.

[117] John J Borking & Charles D Raab, *Laws, PETs and Other Technologies for Privacy Protection,* (2001), at http://elj.warwick.ac.uk/jilt/01-1/borking.html, (mentioning transparency, data quality, respect for the rights of parties involved, and security).

[118] Available at http://www.w3.org/P3P/.

be lengthy in order to describe fairly the details of how personal information may be collected, maintained, used and disclosed. P3P may not have the vocabulary necessary to convey all the information.

The earlier discussion about property rights as a privacy protection scheme noted the high cost of negotiations over privacy between record-keepers and record subjects. One advantage of P3P is that it *automates* the exchange of information about preferences and policies. P3P may also automate discussions between parties and reduce the cost.[119] This addresses one of the consequences that arise when each user individually establishes personally acceptable privacy rules. An individual who is unhappy with the policies at a website could then make a knowing choice about whether to do business at that website or, perhaps, a decision about the conditions under which the individual will agree to do business. Whether P3P will extend beyond take-it-or-leave-it offers by websites and allow for accommodations of individual privacy requirements is uncertain. P3P is just beginning to be implemented on some Internet sites.

Some critics see P3P as failing to establish privacy policies because it fails to ensure the observance of FIPs. For example, the Article 29 Working Party of supervisory authorities established under the EU Directive offered its opinion on P3P in a 1998 document.[120] The Working Party questioned the adequacy of a technical solution that did not meet minimum levels of data protection and that placed responsibility for privacy in the wrong place.

> A technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web. It must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. Use of P3P and OPS in the absence of such a framework risks shifting the onus primarily onto the individual user to protect himself, a development which would undermine the internationally established principle that it is the 'data controller' who is responsible for complying with data protection principles (OECD Guidelines 1980, Council of Europe Convention No. 108 1981, UN Guidelines 1990, EU Directives 95/46/EC and 97/66/EC). Such an inversion of responsibility also assumes a level of knowledge about the risks posed by data processing to individual privacy that cannot realistically be expected of most citizens.[121]

Others also question the lack of complete privacy policies. The *notice and choice* approach at the core of P3P is a "weak model for privacy" and not consistent with the approach taken in the United

---

[119] Lawrence Lessig, *Code and Other Laws of Cyberspace,* 160 (1999).

[120] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Platform for Privacy Preferences (P3P)* and the *Open Profiling Standard, (OPS)* (1998) (WP 11), at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp11en.pdf.

[121] *Id.* Discussions between P3P developers and EU data protection officials have been ongoing. For a summary of developments, see Lorrie Faith Cranor, *The Role of Data Protection Authorities in the Design and Deployment of the Platform for Privacy Preferences,* paper prepared for presentation at the 23rd International Conference of Data Protection Commissioners, (Sept. 25, 2001), at http://www.paris-conference-2001.org/eng/contribution/cranor_contrib.html.

States to ensure privacy protections in other sectors with rapidly changing technology.[122] Another limitation of P3P is that it works only on the Internet and only for websites that agree to participate. It has no applicability in other online contexts or in the offline world. With the introduction of new P3P-compatible browsers in the fall of 2001, P3P will be tested in the marketplace to see if users and website operators find it useful. However, even if a website uses P3P, users cannot be sure that the website is actually complying with its stated privacy policy.

It is not clear whether P3P will work for government websites. Federal websites must comply with established legal requirements in the Privacy Act of 1974 and other laws. The statutory requirements are both different from and more stringent than the P3P requirements. In any event, at least some users of federal agency websites will be obliged to use the websites and will have no choice about the privacy policies under which the sites operate. Even if P3P does not fully support user-website negotiations over privacy for federal websites, the notion of automated privacy disclosures for government websites may still be feasible, if only as a way of notifying interested users about privacy policies.

Depending on the nature, location, and operation of PETs, technology can mandate substantive policies in a manner similar to that of law. Technological standards, whether at the Internet, network, or program level, can restrict processing of personal data in ways that protect privacy. Enforcement of technical rules can be automated and self-executing. The technology can make it impossible to violate established privacy or other standards.[123] Thus, technology can provide both substantive rules and enforcement through the same device. P3P is a voluntary standard for both websites and users so it does not mandate compliance with any specific privacy policies by anyone. It is possible to envision other technologies that could mandate privacy protections or that could prohibit use of some privacy protective techniques.

Finally, a PET may appear to be useful in helping websites and users address privacy concerns. It is possible, however that the same PET could be counterproductive in other ways. Some lawyers worry that P3P could increase a company's liability over privacy. One prominent Internet lawyer developed an alternative that will allow a website to disclaim its own P3P statement for purposes of liability.[124] Whether this approach will be successful is unknown. Now, a website faces the possibility that it could be held responsible at law or by the FTC for complying with a declared privacy policy. If a website can deny responsibility and liability for its own policy, consumers may

---

[122] Electronic Privacy Information Center & Junkbusters, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy,* (June 2000), at http://www.epic.org/reports/prettypoorprivacy.html. For another negative view on technological solutions, reference Beth Givens, Director, Privacy Rights Clearinghouse, *Eight Reasons to be Skeptical of a "Technology Fix" for Protecting Privacy,* (2000), at http://www.privacyrights.org/ar/8skeptical.htm.

[123] For one of the early discussions of this subject, reference Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology,* 76 Texas Law Review 553 (1998). See also Lawrence Lessig, *Code and Other Laws of Cyberspace*, 160 (1999).

[124] Benjamin Wright, *The Law of Electronic Commerce,* quoted in Bureau of National Affairs, *Privacy P3P's Arrival Raises Concerns That Tool May Create Liability, Drive Away Site Traffic,* 6, Electronic Commerce & Law Report, (Oct. 3, 2001), at http://ipcenter.bna.com/ipcenter/1,1103,1_968,00.html.

not have either assurance or recourse about privacy. If P3P becomes a RDT (responsibility denying technology), it may no longer really qualify as a PET.

2.5.4.3 Openness

Advocates of more openness in government and elsewhere in society are not likely sources for substantive privacy protections. Openness advocates tend to oppose privacy restrictions, but their views should nevertheless receive some representation here.

David Brin is an advocate of more openness in modern life, although it would be unfair to call him an opponent of privacy. Brin's thesis is that the value of transparency is underrepresented in discussions about privacy.[125] He believes that more openness will lead to more accountability at all levels, and the result will be more freedom. For example, he discusses the growing use of cameras in public places and their effect on behavior. He proposes *more* cameras, and he wants to make the pictures widely available. Cameras broadcasting routine activities over the Internet can make police and other government officials more accountable for their actions. Brin sees criticism as the key to improving society and to remedying errors and self-deception. He also suggests a rule of reciprocal transparency that would require corporate executives collecting personal information about consumers to post their own personal information on the Internet.

The press is also a strong proponent of openness, especially with respect to government records. In recent comments on medical privacy rules, the Reporters Committee for Freedom of the Press said that privacy restrictions could prevent journalists from performing their vital role of keeping the public informed about important patient matters and medical issues of concern to the public.[126] In arguing for access to electronic court records, the Reporters Committee suggested that readily available court records would enable greater press and public oversight of foster care by allowing searching for foster parents with a record of abusive behavior.[127] This sample does not exhaust the arguments presented by representatives of the media or other openness advocates.

In some contexts, especially with respect to government records and government restrictions on the public availability of records maintained by private sector record-keepers, openness values often conflict with privacy interests. Struggles over the availability of public records[128] maintained by government agencies can be heated. First Amendment values are a significant part of the openness portfolio. Privacy and openness are not always in conflict. Many elements of FIPs, for example, do not create any conflict. The privacy principles of openness (transparency), individual participation, security, and others do not appear to create any concerns for openness advocates. The conflicts that

---

[125] David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom,* (1998).

[126] Available at http://rcfp.org/news/documents/medprivacy.html.

[127] Available at http://rcfp.org/news/documents/electronic.html.

[128] A public record can be defined as: 1) a register, list, roll, or compendium of personal data under the control or direction of a public body; 2) maintained pursuant to statute, regulation, rule, or administrative practice; and 3) open (in whole or in part) to public inspection, copying, distribution, or search under a specific law or policy. See generally Robert Gellman, *Public Registers and Privacy: Conflicts with Other Values and Interests,* Blair Stewart, *Five Strategies for Addressing Public Register Privacy Problems.* Proceedings of the 21st International Conference on Privacy and Personal Data Protection (Hong Kong, 1999), at http://www.pco.org.hk/english/infocentre/conference.html.

arise over use and disclosure limitations, however, are quite sharp. The extent to which government limitations on the use and disclosure of personal information by private sector record-keepers can be consistent with the First Amendment to the U.S. Constitution remains the subject of intense debate. Even exemptions from privacy rules for the news media create definitional problems.[129] The difficulties of defining who is a qualified journalist have been exacerbated in recent years by the ability of individuals to publish their own materials directly on the Internet.

2.5.4.4 Marketplace Solutions

Those who want to let the marketplace address privacy concerns have different and sometimes overlapping motivations. Some worry about effects on the First Amendment right of free speech. They oppose privacy legislation as unconstitutional. Some support privacy self-regulation as an alternative to legislation. Some draw a distinction between privacy laws for the government, which they support, and privacy laws for the private sector, which they oppose. The political arguments for and against these positions are not relevant here. The question is whether any of the proponents of marketplace solutions have any substantive privacy standards to contribute to the debate.

House Majority Leader Dick Armey (R-Texas) has articulated the view that government is the biggest privacy offender and should be the subject of more intense review.[130] He sees the government as the natural test subject for developing a deeper understanding of the effects of privacy regulation, and he wants the government to set an example for the private sector on privacy. Privacy standard setting for private sector activities would be a lower priority. An important point is that the privacy law and policy responses for the government and the private sector may differ in scope, substance, priority, and in other ways. Among other reasons, the government is subject to constitutional constraints whereas the restrictions on government action in the Bill of Rights do not apply to the private sector.

Some supporters of self-regulation endorse voluntary policies for the nature and process of self-regulation activities. For example, the Online Privacy Alliance, a cross-industry coalition of more than 80 global companies and associations committed to promoting the privacy of individuals online, published standards for effective enforcement of self-regulation. Separately, the Online Privacy Alliance also published its own version of FIPs for online privacy.[131] This effort represents one of the more complete and substantive attempts to prescribe the content of privacy self-regulation.

Others only see self-regulation driven by market forces as useful, and they see no need for substantive rules. The Cato Institute writes "in most cases no third party standards or oversight at

---

[129] See generally, Jane E. Kirtley, *Is Implementing the EU Data Protection Directive in the United States Irreconcilable with the First Amendment?,* 16, Government Information Quarterly 87 (1999).
[130] Dick Armey, *The Conservative's Case for Privacy*, Speech Delivered to the Federalist Society, (June 27, 2001), at http://freedom.house.gov/library/technology/federalist.asp.
[131] Available at http://www.privacyalliance.org/resources/ppguidelines.shtml.

all are necessary for 'self-regulation.'"[132] With true market-based self-regulation, each company will regulate itself according to internal standards and market pressures. Under this approach, even government-driven self-regulation is not desirable because it mimics official regulation without any of the safeguards for regulatory activities. In another publication, the Cato Institute suggests that the government's role is not to dictate the terms of privacy contracts – that is, to establish substantive privacy rules – but to enforce privacy contracts entered into by businesses and individuals.[133]

The Pacific Research Institute for Public Policy is another opponent of privacy legislation and a supporter of self-regulation and marketplace solutions.[134] The Institute's recent report on privacy does not propose substantive privacy rules, but it does support self-regulation. It promotes technologies available to protect individual privacy as better than legislation. It opposes the FTC's FIPs as unnecessary and costly, and because they may give consumers less privacy by reducing marketplace pressures for new technology. As evidence of successful self-regulation, the report notes the growth of privacy policies, chief privacy officers, and privacy audits. This view is suggestive of rules for privacy, although the report is not prescriptive. It supports letting consumers determine the right level of privacy through contracts and legislation ensuring that contracts made online can be enforced.

Several privacy seal programs exist that require participating organizations to meet substantive privacy criteria for websites. Two of the leading privacy seal programs are Better Business Bureau Online (BBBOnline)[135] and TrustE.[136] Each program maintains its own set of privacy rules. These programs are voluntary and privately funded by members. The programs allow members to display a privacy seal on their websites to serve as a notice to consumers that the website meets the criteria of the seal program.

Both TrustE and BBBOnline require participants to meet criteria for notice, choice, access, security, and redress. The substantive requirements of the two programs are similar as evidenced by some organizations that participate in both seal programs. The privacy rules are abbreviated versions of FIPs, similar to the version proposed as a legislative standard by the FTC for online activities. The redress procedures are discussed separately under the enforcement chapter.

The merits and effectiveness of privacy self-regulation have been contested over the last several years. The evolution of views at the FTC over several years offers an interesting commentary on the subject. The Commission's initial approach was to encourage online privacy self-regulation and to

---

[132] Solveig Singleton, *Regulatory Obstacles to Innovation: Is Self-Regulation The Answer?,* (1999) (Cato Institute), at http://www.cato.org/pubs/wtpapers/990913catoself.html.
[133] Wayne Crews, *Policymakers Should "Opt-Out" of Privacy Legislation,* (March 13, 2001) (Cato Institute), at http://www.cato.org/dailys/03-13-01.html.
[134] Sonia Arrison, *Consumer Privacy: A Free-Choice Approach,* (Sep. 2001) (Pacific Research Institute for Public Policy), at http://www.pacificresearch.org/.
[135] Available at http://bbbonline.org/.
[136] Available at http://www.truste.org/.

encourage industry and consumers to work together toward that goal. In 1998, the Commission reported to the Congress that it was hopeful that self-regulation would achieve adequate privacy protections for consumers. The Commission did not recommend the passage of privacy legislation.[137]

By 2000, the Commission changed its mind. In a new report on online privacy, the Commission concluded that self-regulation had failed:

> Because self-regulatory initiatives to date fall far short of broad-based implementation of self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders.[138]

The Commission then recommended that Congress pass online privacy legislation.[139] However, support for the report was not unanimous, and two Commissioners dissented, one in whole and one in part. Whether the report's recommendations still represent the views of the Commission is doubtful. The Commission's membership changed when President Bush appointed a new chairman in 2001. In a speech on October 4, 2001, the new chairman, Timothy Muris, announced that "it is too soon to conclude that we can fashion workable legislation" for online privacy. He announced instead a series of other measures, including increased enforcement of current privacy laws.[140]

Debates over self-regulation, like other aspects of privacy, sometimes become contests between two diametrically opposed positions. The alternatives presented are either legislation or self-regulation. Each entrenched viewpoint has variants, and middle grounds do exist. For example, one advocacy group that promotes democratic values and constitutional liberties in the digital age supports a mixture of self-regulation technology, and legislation. In testimony before the Senate, Jerry Berman, Executive Director of the Center for Democracy and Technology, supported baseline rules and fair information practices "to augment the self-regulatory efforts of leading Internet companies, and to address the problems of bad actors and uninformed companies."[141]

Other countries have married legislation and various forms of self-regulation. The EU Data Protection Directive encourages the drafting of industry codes of conduct.[142] The Netherlands

---

[137] Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress,* (1999), at http://www.ftc.gov/os/1999/9907/privacy99.pdf.

[138] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace,* 35 (May 2000), at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[139] *Id.* at 36-38.

[140] Available at http://www.ftc.gov/speeches/muris/privisp1002.htm.

[141] Testimony before the Senate Committee on Commerce, Science, and Transportation (May 25, 2000), at http://www.cdt.org/testimony/000525berman.shtml.

[142] *EU Data Protection Directive,* at Article 27(1) ("The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors."). The Working Party of national data protection authorities established under Article 29 of the Directive issued several documents on codes of conduct. European Commission Working Party on the Protection of Individuals with Regard to the Processing

offers a good example of the implementation of a middle ground. Upon application by an organization, the College Bescherming Persoonsgegevens (Netherlands Data Protection Authority) can declare that a sectoral code of conduct properly reflects the legal requirements for the processing of personal data. The Netherlands approach requires that requests for approval must come from a representative organization, that the sector be precisely defined, and that any dispute procedures be independent.[143] The Netherlands law illustrates that self-regulation can play a role in a legislative framework for privacy and can serve as intermediate construct between official regulation and informal self-regulation.[144]

2.5.4.5 Human Rights

The right to privacy is sometimes described as a fundamental human right. Europeans are more likely to define privacy in terms of human rights. For example, the title of the 2001 annual conference of the Data Protection Commissioners hosted in Paris by the National Commission on Data Processing and Liberties (Commission Nationale de l'information et des Libertés) was "Privacy – Human Right."[145]

Numerous international human rights documents treaties include privacy as a basic right. The "modern privacy benchmark at an international level"[146] is the United National Universal Declaration of Human Rights adopted in 1948. Article 12 states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.[147]

In 1950, the Council of Europe adopted a Convention for the Protection of Human Rights and Fundamental Freedoms. Article 8 provides:

> Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the

---

of Personal Data, *Judging Industry Self-Regulation: When Does It Make a Meaningful Contribution to the Level of Data Protection in a Third Country?,* (1998) (WP 7), at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp7en.pdf, and *Future Work on Codes of Conduct: Working Document on the Procedure for the Consideration by the Working Party of Community Codes of Conduct,* (1998) (WP 13), at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp13en.pdf.

[143] Personal Data Protection Act (Netherlands) at Article 25 (Session 1999-2000 Nr. 92), at http://www.registratiekamer.nl/bis/top-1-11.html.

[144] Charles D. Raab, *Sectoral Data Protection in Europe,* 17 (presentation at the Conference on Personal Data Protection in Europe and in Hungary, January 1998).

[145] Available at http://www.paris-conference-2001.org/.

[146] David Banisar, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments,* 6 (2000).

[147] Available at http://www.un.org/Overview/rights.html.

> protection of health or morals, or for the protection of the rights and freedoms of others.[148]

A more recent European document, the Charter of Fundamental Rights of the European Union adopted in 2000, contains another statement about privacy. Article 8 on the protection of personal data provides:

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.[149]

Unlike the previous two human rights documents, the EU Charter of Fundamental Rights provides a degree of specificity about the content of the privacy right. An accompanying explanation makes it clear that the Article is based on the EU Data Protection Directive and other EU documents.[150] Thus, it is not surprising that the EU Charter reflects elements of FIPs.

The idea of privacy as a fundamental human right is not limited to international treaties. National and provincial instruments may also define privacy as a basic right. For example, Chapter 1 of the Quebec Charter of Human Rights and Freedoms includes as fundamental freedoms and rights:

> Every person has a right to respect for his private life. Every person has a right to non-disclosure of confidential information.[151]

Another fundamental characterization of privacy popularly used in Germany is that of the *right to informational self-determination*. The concept comes from a 1983 decision of the Federal Republic of Germany's Federal Constitutional Court. A challenge to a national population census addressed privacy rights under the German constitution. In its decision postponing the census on the grounds of potential invasion of privacy, the Federal Constitutional Court first used the term *right to informational self-determination* as a constitutional right. However, as one commentator observed, the decision "does not make clear what claims the individual can make."[152]

This discussion does not exhaust the statements about privacy that can be found in human rights documents.[153] However, the sample provided here is sufficiently representative for present purposes. While international recognition of privacy as a fundamental human right is an important

---

[148] Available at http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.
[149] Available at http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf.
[150] Available at http://www.europarl.eu.int/charter/pdf/04473_en.pdf.
[151] Available at http://www.cdpdj.qc.ca/htmen/htm/4_4.htm.
[152] *Flaherty* at 47. For more about the right of informational self-determination, see Virtual Privacy Office, Independent Centre for Privacy Protection, Schleswig-Holstein, Germany, at http://www.datenschutz.de/recht/grundlagen/ris.xml.
[153] David Banisar, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments,* (2000).

development, the international and other statements offer limited direction about the content and elements of the privacy right. It is clear, particularly in the case of the EU Charter of Fundamental Rights, which other instruments (like the EU Data Protection Directive) must be read to provide the substantive details. Understanding the human rights aspects of privacy is important to any international discussion, but human rights language offers limited direction about the substantive meaning of privacy. For substance about privacy, it is necessary to look to other international instruments, national laws, and other documents.

2.6 The Challenges of Implementing Fair Information Practices

FIPs are recognized worldwide as a framework for information privacy. However, even if FIPs are readily accepted as a starting place, any detailed inquiry into privacy policy using FIPs will quickly become more complex and more judgmental. Translating FIPs into privacy laws or policies – or using FIPs to evaluate the degree of privacy found in an existing law or set of practices – is hard because the FIPs principles are not self-implementing. The manner of their implementation will depend on multiple factors, including the type of data involved, the type of the record-keeper, the purpose of processing, the way in which the data will be used and disclosed, the technology employed, costs, and the traditions of the jurisdiction, industry, or record-keeper. The multidimensional nature of privacy means that there can be a diversity of implementation strategies for the same principle. The purpose of this section is to describe some of the challenges of translating FIPs into real world practices and of evaluating personal information processing activities against FIPs standards.

2.6.1 Introduction

Differences in the application of data protection principles can readily allow for alternative approaches, with the possibility of conflicts in regulatory approaches in different jurisdictions. A common reliance on FIPs does not avoid all problems or conflicts. What FIPs provide is a common menu of information privacy issues for consideration by policy makers. FIPs do not guarantee complete compatibility or commonality of response.

Versions of FIPs rarely exceed a few pages. However, the versions often come with much lengthier explanatory documents that begin to suggest the complexities of implementing FIPs. The OECD Guidelines are accompanied by an *Explanatory Memorandum* consisting of 77 paragraphs (roughly 22 pages) that address in greater depth the background, implementation, and interpretation of the Guidelines. For example, the explanation of the principle of individual participation considers, among other things, how long a data controller has to respond to requests for access to records by a data subject, and the possibility of an exemption for a data controller who otherwise regularly provides information to data subjects. The memorandum also states that the extent to which a data subject should be able to obtain copies is a matter of implementation left to the decision of each nation.[154] This last point suggests, for example, that a nation could implement data subject access properly without allowing the data subject to obtain a copy of his or her record. These are all

[154] *OECD Privacy Guidelines,* paragraph 59.

implementation details that are not addressed in a short statement of basic principles and that could be decided in different ways without necessarily being inconsistent with the basic policy.

Similarly, the basic Safe Harbor principles agreed to by the U.S. Department of Commerce and the European Commission are short. They are accompanied, however, by a set of Frequently Asked Questions (FAQ) that are eight times as long. FAQ 8 on Access consists of eleven subquestions addressing subjects such as exceptions to the right to access, the effort required to retrieve information, and the time limits for responses.[155] These questions and answers reflect some of the implementation problems raised by potential Safe Harbor participants during the negotiations that produced the agreement.

The EU Data Protection Directive includes 72 prefatory recitals that address, among other things, details of interpretation of the Directive. For example, recital 41 states that the right of data subject access must not adversely affect the trade secrets or intellectual property of the controller. This is a point not directly addressed in Article 12 on Right of Access, but the recital recognizes a potential limitation on the ability of a data subject to obtain access. Several other recitals address other definitive or potential limitations on the right of access in other contexts.

The length of explanatory documents is not the only measure of the potential diversity of implementation of common principles. Some specific examples will shine light on the divergent ways that data protection principles can be implemented and on threshold definitional issues. A study of online privacy regulations conducted for the European Commission by two American law professors looked at aspects of the law in four EU Member States.[156] The study examined definitions of what constitutes identifiable data, rules for registration and supervision, transparency (e.g., openness/notice), profiling and sensitive data, and security for online services. The study found similarities and differences in how each Member State applied EU data protection principles to online data. For example, Britain and France take different approaches to defining personal information subject to regulation. In deciding whether information is identifiable, Britain looks at the context to determine if identity can be determined from the data and other information in the possession of the data user. France takes a broader approach, asking whether it is at all possible to trace the information back to an identifiable user.[157] These are distinct inquiries, and significantly different results will emerge at times. In some instances, France will regulate a particular type of processing for privacy while Britain would decline to regulate the same activity.

The study concluded that the differences had some significance for the structure and development of online services.[158] In other words, countries found different ways to apply common principles in the online environment, and the differences have the potential to create conflicts. Divergences in

---

[155] Department of Commerce, *Safe Harbor Privacy Principles,* FAQ 8 on Access, at http://www.export.gov/safeharbor/sh_documents.html.

[156] Joel R. Reidenberg & Paul M. Schwartz, *On-line Services and Data Protection and Privacy,* (1988) (Volume II Regulatory Responses), at http://europa.eu.int/comm/dg15/en/media/dataprot/studies/regul.htm.

[157] *Id.* at 124.

[158] *Id.* at 123.

the application of the Directive to online activities are, at least in part, a consequence of the drafting of the directive before the scope of online activities became manifest. However, the basic point about multiple implementation strategies and disparate policy choices while still operating under common principles remains independent of the technological currency of the Directive.

Protecting privacy is nearly always a balancing act. In the words of one data protection scholar, "[p]rivacy protection in law and practice involves a balance between competing values in order to achieve a result that safeguards individual privacy while also accommodating other important social, political, or economic ends."[159] These other goals include national security, law enforcement, economy and efficiency, and public health. When balancing privacy interests against other socially recognized values, FIPs provide a framework for making sure that the balancing includes the elements of privacy. However, it is important to recognize that FIPs do not dictate a specific outcome. When evaluating broadly defined policy objectives against one another, it is easy to understand how different evaluators can achieve different outcomes.

The tradeoffs between privacy and other values are usually context-driven. For example, policy may require that personal data maintained by private record-keepers be shared with government authorities at times. For health care providers, the obligation may be an affirmative one. Health care providers are often affirmatively required to disclose records of communicable diseases with public health agencies. Banks may be asked to share some customer records with financial regulatory agencies only upon request. Any record-keeper may be required to disclose records in response to subpoenas. However, the procedures for responding may differ depending on the nature of the records and whether the subpoena is for use by a grand jury, by a regulatory agency, or in routine litigation.

A general summary of some implementation issues raised by FIPs principles follows.[160] The goal is to provide a flavor of the difficulties of implementing FIPs. The analysis is not comprehensive. A complete discussion of the principles, especially in the context of specific categories of records (e.g., health, education, marketing, employment), would identify additional questions and conflicts, and that discussion could continue for hundreds of pages. The security principle is not discussed here because its technical aspects are beyond the scope of this report. The accountability principle is addressed in the next chapter through a discussion of enforcement methods.

---

[159] Charles D. Raab, *From Balancing to Steering: New Directions for Data Protection* 68 in *Visions of Privacy: Policy Choices for the Digital Age,* (Colin J. Bennett & Rebecca Grant eds., 1999) (footnote omitted).

[160] For a discussion of the complexities of implementing the EU Data Protection Directive for international companies (i.e., U.S. companies), Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive,* (1998).

2.6.2 Collection Limitation

The *collection limitation* principle calls for the collection of personal information "where appropriate, with the knowledge or consent of the data subject." The language of the principle itself makes it clearly apparent that a diversity of applications is possible and is expected. The use of the word *fair* demonstrates the point. What is or is not appropriate or fair will depend on context, circumstances, and values. No one is likely to argue, for example, that it would be appropriate for all criminal investigations to require the knowledge or consent of the subject of the investigation.

The principle can be satisfied with either knowledge or consent of the data subject. These alternative approaches have significantly different implementation strategies. Consent can be obtained in a variety of ways. The law of the Czech Republic required *written* consent for processing, with only some relatively narrow exceptions to the requirement.[161] This may be one of the strictest implementations of the *collection limitation* principle in any national data protection law. By contrast, the EU Directive requires *unambiguous consent*[162] for processing, but the exceptions are much broader and include when processing is necessary for the purposes of the legitimate interests of the controller.[163] This exception allows much commercial data processing to continue without the need for consent from the data subject.

The U.S. Privacy Act of 1974 has somewhat comparable language. The Act requires an agency to collect information *to the greatest extent practicable* directly from the subject individual if the information may be used to make an adverse determination about the individual.[164] This interpretation of the *collection limitation* principle is stronger in some ways than the EU or Czech Republic implementation because it seeks to foreclose collection of information from third parties. However, the restriction only applies when the purpose of the collection may be used to make an adverse determination about the data subject. The U.S. provision, then, is stronger in some ways and weaker in other ways than the EU or Czech Republic implementation. It is easy to argue that the U.S. provision meets the essential fairness goals of the *collection limitation* principle, but the conclusion that the language truly satisfies the principle remains open to debate.

---

[161] Act No. 101 of April 4, 2000 on the *Protection of Personal Data,* as amended at Article 5(2), 5(5), at http://www.uoou.cz/eng/101_2000.php3.

[162] The EU Data Protection Directive discusses, but does not define, three flavors of consent: consent, explicit consent, and unambiguous consent. Unambiguous consent appears to mean that the consent must be freely given, specific, and informed. In the case of data exports to countries with inadequate protection, the data subject must be properly told of the risk that data will be transferred.

[163] *EU Data Protection Directive,* at Article 7. An exception to the *legitimate interest of the controller* standard allows the controller's interest to be outweighed by "the interests or fundamental rights and freedoms of the data subject." *Id.* at 7(f).

[164] 5 U.S.C. §552a(b).

2.6.3 Data Quality

The *data quality principle* introduces the concept of *purpose*. Important issues with any FIPs purpose requirement are who defines the *purpose* and whether there are any controls on the definition. If a commercial record-keeper can define *purpose* to mean anything that might produce revenues or profits, then the goal of imposing limits will be defeated. Where statements of purpose are submitted to and overseen by data protection authorities, overly broad statements may attract negative comments or even be rejected. In some EU Member States and in other countries as well, data controllers are sometimes required to file a purpose statement with the data protection supervisory authority. Oversight of a purpose statement by a data protection authority illustrates the potential interplay between FIPs principles and an administrative structure for privacy. The structure can impose tension on the implementation of the principles by a record-keeper by establishing contextual boundaries.

Another important word in the principle is *relevant*. Relevance is a concept that is clearly context driven. Its presence in the principle illustrates why implementation of FIPs requires the application of judgment. The later use of the term *incompatible* is further evidence on this point.

Another element of data quality that is only sometimes expressly stated is retention. When the retention of personal information is not longer required, the information should be destroyed. Data retention policies vary with the type of record-keeper, nature of the data, applicable laws, and other factors. A wide range of data retention practices can be compatible with the principle.

2.6.4 Use Limitation/Purpose Specification

The *use limitation* and *purpose specification* principles require that the purposes for which personal information is collected be identified not later than the time of collection and that any incompatible[165] uses require consent or legal authority.

The restrictions on data use imposed by these principles have not been embraced by the American business community. Substitute statements of privacy principles tend to ignore purpose specification and propose a *choice* standard. For example, the restatement of FIPs by the Federal Trade Commission avoids the word *consent* and instead relies on the notion of *choice*.[166] The FTC restatement represents a change that weakens the protections intended by the OECD Guidelines, but it still serves to illustrate the complexity of implementation. Whether consent or choice is the standard, implementing the policy presents hard questions.

---

[165] The *routine use* provision of the Privacy Act of 1974 allows an agency to define addition disclosures that are "compatible with" with purpose for which a record was collected. 5 U.S.C. §552a(a)(7). The standard used to describe secondary uses (e.g., *compatible with* versus *not incompatible with*) can produce significantly different results in some instances.

[166] Federal Trade Commission, P*rivacy Online: Fair Information Practices in the Electronic Marketplace,* at iii (May 2000), at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf ("Choice: Websites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided *(e.g.*, to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).").

Much of the debate in the United States has turned solely on the narrowly defined distinction between opt-in and opt-out. *Opt-in* means affirmative choice. An individual's information may be processed in an opt-in regime only if the individual has affirmatively agreed to the processing. *Opt-out* means negative choice. An individual's information may be processed under an opt-out regime unless the individual has objected to the processing.[167]

The manner in which options are presented is widely believed to make a significant difference to the outcome. In many circumstances, people will accept the default option that requires no action on their part. Thus, when opt-in is the method, people are not likely to act to opt-in. When opt-out is the method, people are not likely to act to opt-out. For those who want to use personal information for secondary purposes, the nature of the option presented to individuals can be crucial. As the discussion below suggests, however, other elements beyond the mere type of option are relevant.

While some believe that *consent* implies opt-in and *choice* implies opt-out, neither conclusion is certain. The terminology alone is not clear enough to allow for a definitive determination, and the context for any policy may well turn on the circumstances and method for the exercise of a decision by a data subject. U.S. law provides a few examples.

The Driver's Privacy Protection Act (DPPA) as originally passed in 1994[168] provided that state motor vehicle departments could only disclose personal information for marketing uses if the data subject had a clear and conspicuous opportunity to prohibit the disclosure. The law described an opt-out requirement. In 1999, Congress amended this language to require that disclosures for marketing were permissible only with the express consent of the data subject.[169] The amendment changed the opt-out to an opt-in. Neither version of the DPPA included many details about the nature of the decision to be presented to the data subject. However, it was clearly understood by the Congress that drivers must renew their licenses routinely and that drivers would have regular opportunities to indicate their preferences. Format and procedural issues under both approaches were left largely to the states to decide. When the opt-in requirement became law, many states no longer asked drivers to express a choice. Because few drivers could be expected to opt-in, any resulting list would not have significant value.

Under Gramm-Leach-Bliley (Financial Institutions Modernization Act), banks must give customers the opportunity to opt-out of disclosures of some personal information to non-affiliated third

---

[167] Whether the terms are clearly distinguishable may be questioned. One commercial website asks users for approval when the privacy policy changes. The website sends a notice and tells users that if they do not respond, the company will assume that the users have *opted-in* to the new policy. Failing to respond would normally be treated as an opt-out and not an opt-in. See DNA Sciences, at http://dna.com/privacyPage/privacyPage.jsp?site=dna&link=PrivacyStatement.htm#5. Whether the DNA Sciences characterization of opt-in is an aberration or a trend is unclear. It illustrates how language can be applied in unexpected ways in the absence of an explicit definition.

[168] Public Law 103-322, §300002, 108 Stat. 2099 (1994).

[169] 18 U.S.C. §2721(b)(12). Congress made the same change for another category of disclosures. *Id.* at §2721(b)(11).

parties.[170] The Federal Trade Commission regulations offer details on the form and nature of the opt-out. An annual notice to customers is required.[171] The rules state that the opt-out notice given to customers must be *clear and conspicuous* and that a reasonable means of exercising the opt-out must be provided.[172] A reasonable means of opting out includes either 1) a check-off box in a prominent position on the relevant form; 2) a reply form with the address to which the form should be sent; 3) an electronic means to opt-out; or 4) a toll free number.[173] In addition to defining the reasonable means for opting out, the FTC rules also specified what would be unreasonable means. These include 1) requiring a customer to write a letter; and 2) not including a check-off box in a subsequent notice when that is the only means of opting out.[174] An opt-out may be exercised at any time,[175] and it remains in effect until revoked by the customer.[176]

The privacy rule issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA) includes an opt-out for marketing uses of personally identifiable health information.[177] Protected health records may be used or disclosed by an entity covered by the HIPAA rules for marketing under prescribed conditions. A patient record can be used for marketing without the patient's affirmative consent and without giving the patient the right to opt-out in advance. However, the marketing communication must contain instructions describing how the patient can opt-out of receiving future marketing communications. Unlike the FTC's Gramm-Leach-Bliley opt-out rule, the HIPAA privacy rule does not define what constitutes a reasonable or unreasonable means for opting out. This means that a data subject under HIPAA could be required to write a letter to opt-out of a marketing activity, but the Gramm-Leach-Bliley rule provides that making a data subject write a letter is unreasonable. The difference between the two rules on opt-out process is particularly notable, and it illustrates how implementation of the same policy by two agencies can have significantly different consequences for data subjects. All opt-outs are not necessarily the same.

The EU Directive requires that Member States grant data subjects the right to object "on request and free of charge" to the processing of personal data by a controller for the purposes of direct marketing. An alternative option is to require that a controller who wants to transfer personal information to a third party for direct marketing must inform data subjects before the first transfer and must expressly offer the right to object.[178] However, in the case of sensitive data (such as health data), processing data for marketing purposes requires explicit consent of the data subject.[179]

---

[170] 15 U.S.C. §6802(b).
[171] 16 C.F.R. §313.5.
[172] *Id.* at §313.7(a)(1).
[173] *Id.* at §313.7(a)(2)(ii).
[174] *Id.* at §313.7(a)(2)(iii).
[175] *Id.* at §313.7(f).
[176] *Id.* at §313.7(f).
[177] 45 C.F.R. §164.514(e).
[178] *EU Data Protection Directive,* at Article 14(b).
[179] *Id.* at Article 8.

These examples show that a diversity of consent or choice procedures can be employed. It is difficult based only on a short statement of principle to determine which procedure is sufficiently protective of privacy in all contexts. The HIPAA rule that allows any protected health data to be used for marketing by a qualified third party without affirmative consent would likely draw sharp objections under the policies of the EU Directive. For personal data of lesser sensitivity, there may be more to debate about the adequacy of the procedures for exercising consent/choice.

Analyzing consent/choice issues solely on an opt-in or opt-out standard may be too limiting to permit a proper evaluation of the privacy consequences. The nature of any option offered to the data subject is only one relevant factor. Other factors include:

- What does the option cover? A use or disclosure affirmatively consented to by a data subject is by definition acceptable. Is any use or disclosure permissible as long as an opt-out is provided? Is there some independent constraint on the scope of use and disclosure, such as a statement of purpose specified for the processing at the time of collection?
- What is the form and timing of the notice to the data subject? Must a notice be written? Clear and conspicuous? Understandable to the average individual? Must a notice be given before first use of the data? Must a notice be repeated annually or at another interval? Is a notice posted obscurely on a website sufficient? If an option box on a website is pre-checked, does that constitute opt-in or opt-out? If no box is checked and the website requires the user to make a selection before moving to the next screen, is that something other than opt-in or opt-out? Does the type of information (e.g., medical/financial as opposed to name and address) or the proposed use/disclosure (e.g., publication of a list of welfare recipients) affect form and timing of the notice?
- What form of response by the data subject is required? Must a data subject write a letter? Is there a check-off box? Postpaid envelope? Toll-free telephone number? Must the data subject fill out an option form or does the form arrive pre-populated with relevant data so that it may be more easily returned? Must an option selected on a website be verified by a subsequent confirmation from the data subject? Is the option presented separately from other elections available to data subjects? For example, is a consent for medical treatment and a consent for use of medical information for marketing presented as a single election or can one be selected and not the other?
- Can a user be required pay to opt-out[180] or must the right to object be exercisable free of charge?
- How long is an opt-out effective? Does it expire after a fixed period?[181] Does it matter if the controller sends a notice of expiration to the data subject?

[180] The Direct Marketing Association charges a "processing fee" of five dollars for those who want to use the online opt-out for telemarketing calls, at http://www.the-dma.org/cgi/offtelephonedave.

[181] The Direct Marketing Association (DMA) opt-out for email is effective for only one year and then must be renewed, at http://www.e-mps.org/en/ind_static.html. The DMA's opt-out for telemarketing is effective for five years, at http://www.the-dma.org/cgi/offtelephonedave.

These questions show that applying a privacy principle can involve many alternative approaches. Simply describing a consent/choice approach as either opt-in or opt-out is not sufficient to permit a complete assessment of the privacy consequences.

2.6.5 Use Limitation

Under the *use limitation* principle, personal data should not be used for unspecified purposes except with data subject consent or by authority of law. The form and content of consent offers several elements that may vary from one context to another. Sensitive information or information used to make significant determinations about data subjects may call for more rigorous consent procedures. For example, consent for some uses or disclosures might require particular notices to appear on the consent form so that individuals will be aware of the consequences of the consent. Consent might be time-limited, subject to revocation under specified conditions, or even implied.

Uses required by law will naturally vary considerably with the type of record or record-keeper. Any jurisdiction could, by passing a law, make any particular use or disclosure compatible with the principle. Consider whether it is appropriate to allow health researchers to obtain access to identifiable health records for use in epidemiological research designed to evaluate the best course of treatment for a disease. One country could decide that data might be disclosed to qualified health researchers without the consent of the data subject. Another might require affirmative consent from each patient for each proposed research use or, in the alternative, a general one-time consent covering all possible research uses. Another could require independent review of the research by an ethics committee as a condition of access,[182] with the procedural requirements and substantive standards for the committee's review varying considerably.

Each of these policies, although significantly different from each other, may nevertheless be compatible with FIPs. The judgments needed to make choices are not necessarily limited to those suggested by FIPs. Other values, unrelated directly to privacy, must be considered and may well produce different outcomes for some jurisdictions. On the particular point of researcher access to health records, health institutions and advocates sometimes have significantly different perspectives on the proper rules for researcher access. Respect for health privacy is universal, but researchers place greater weight on the benefits of their research as a justification for reasonable intrusions on patient privacy.

[182] This is the policy governing research access to health records regulated by the Health Insurance Portability and Accountability Act. A researcher seeking access to *protected health information* needs approval from an Institutional Review Board before a record-keeper covered by the law can disclose the records. See 45 C.F.R. §164.510(i). The HIPAA rule only slightly modifies the procedure in common use before HIPAA for federally funded research.

2.6.6 Openness

The FIPs principle of *openness* suggests that individuals should receive notice when a third party collects personal information about them. The implementation of the principle is often tailored to the record-keeper and type of record. Under the Privacy Act of 1974, federal agencies provide notice by publishing descriptions of systems of records in the Federal Register.[183] This is a notice option only available to federal agencies because only agencies can publish notices in the Federal Register. Individual notice also comes through required disclosures on forms used by agencies when collecting personal information for inclusion in Privacy Act systems of records.[184]

Laws defining notice obligations for the private sector implement those obligations in other ways. A credit bureau ("consumer reporting agency") regulated under the Fair Credit Reporting Act does not have any direct obligation to send a notice of information practices to a data subject. This may be because credit bureaus do not collect personal information directly from consumers or have any other routine contact. However, the law requires that a consumer receive a notice of rights from anyone who obtains a credit report for employment,[185] who obtains an investigative credit report,[186] or who takes adverse action against a consumer based on information in a credit report.[187] The law requires notice when a consumer is at greater risk or has actually been denied credit. Otherwise, the intensive and continual collection, maintenance, disclosure, and use of personal information by the credit reporting industry continues without any direct notice to consumers. Whether the notices required by the Act, taken as a whole, offer sufficient openness to satisfy the principle is a matter of judgment. The law demonstrates that Congress made some precise choices about openness requires that appear based on the costs and benefits of providing notice at different stages of the credit reporting process.

In contrast, a cable television provider has contacts with a subscriber when initiating service and routinely for billing. The Cable Communications Policy Act requires notice when the subscriber initiates service and annually thereafter.[188] This approach to notice seems unquestionably consistent with the openness principle. Whether the content of cable notices is sufficient is a separate question.

The Video Privacy Protection Act takes a different approach. The law requires that consumers receive notice and the opportunity to opt-out only if the video service provider plans to disclose information for marketing purposes.[189] If the provider does not plan to make marketing disclosures, then the law does not require any notice of other information practices. Whether the video law's limited notice requirement satisfies the principle of openness is a matter of interpretation. Some

[183] 5 U.S.C. §552a(e)(4).
[184] *Id.* at §552a(e)(3).
[185] 15 U.S.C. §1681b(b).
[186] *Id.* at §1681d(a).
[187] *Id.* at §1681m.
[188] 47 U.S.C. §551(a)(1).
[189] 18 U.S.C.§2710(b)(2)(D).

would argue that a record-keeper still has a notice obligation even in the absence of any intention to use or disclose consumer information for marketing. Business activities necessarily require other uses and disclosures that consumers may be entitled to know about.

Foreign data protection laws often require notice to data subjects of information practices of those collecting information directly from the data subjects.[190] A broader type of public notice may come through requirements to register with or notify the data protection authority.[191] Data protection authorities sometime maintain public registers with information about those who have notified or registered their data processing activities.[192] Notification or registration requirements often have significant exceptions so it is far from clear that a public register of data processing activities might provide a complete alternative to other forms of notice. Notification or registration may also serve the principle of *purpose specification* as well as the principle of *openness*.

How does the principle of openness apply when personal information is collected not directly from the data subject but from a third party? This type of detail is rarely addressed in broad principles and is often not addressed anywhere in policy documents. Many alternative implementation strategies are possible. Under New Zealand's privacy law, notice to the data subject is not required when personal data is collected from a third party. It is an exception to the general principle of notice in New Zealand. Under Canada's privacy law, notice may be required, but not if the information is directory information about employees of an organization. The Canadian law excludes that information from the definition of *personal information* so the collection is unregulated. In Britain, notice is required, but not when it would require *disproportionate effort*.[193] Clear guidance on what constitutes *disproportionate effort* is hard to find. None of these alternative policy choices is facially incompatible with FIPs because the broad principles do not prescribe how the policy should be applied in every situation. Whether any of these three approaches is sufficiently protective of privacy requires a judgment that may be more subjective than objective. The different results in national laws may reflect legal, cultural, or political differences.

2.6.7 Individual Participation

The OECD Guidelines provide that individuals should have a right of access to records pertaining to them and a right to seek corrections. In implementing this policy, the types of problems, questions, and controversies that have arisen in the past include:

1. ***Scope.*** Should the policy of access and correction apply to all record-keepers? Will broad exceptions be necessary for national security and law enforcement records? Application of an access-and-correction rule to records maintained by journalists will certainly raise strong objections on First Amendment grounds. Defining who is a qualified journalist presents a

[190] See, e.g., *EU Data Protection Directive,* at Article 10.
[191] *Id.* at Article 18.
[192] See, e.g., the United Kingdom Office of the Information Commissioner, where a searchable Register of Data Controllers is available on the office website, at http://www.dpr.gov.uk/.
[193] Article 11 of the EU Directive says that in cases of third party collection, notice may not be required if it involves disproportionate effort. The British law mirrors the Directive on this point.

host of challenges, especially in the Internet environment. Should a data subject be able to learn if a record-keeper maintains a record about him or her even if access to the record can be denied?

2. ***Procedures.*** Must a request for access identify specific records or can a data subject simply ask for all records maintained by a record-keeper? How often can a data subject exercise access and correction rights? Once a year? Every 30 days? How long will record-keepers have to retrieve records? Should the time for retrieval vary with the age of, or storage technology used for, the records? How much can record-keepers charge for retrieving records, for permitting access, and for making copies? Must charges be based on actual cost, average cost, or some other standard? If someone cannot afford to pay the charge for access, must the record be provided anyhow? How much of a search must a record-keeper make in response to a request? Will record-keepers be required to find records from decades ago? How much identifying information can record-keepers demand from requesters before allowing access/correction? Can that identifying information be stored or used in other ways? Will record-keepers be liable absolutely for disclosing records to the wrong individual?
3. ***Format of Records.*** What obligation do record-keepers have to present information in an intelligible manner? Must technical information and abbreviations be decoded and explained? Does the right of access extend to the logic of automated data processing activities? When can a record-keeper withhold a record because it might disclose a trade secret? How much effort must a record-keeper undertake to retrieve information from a data system not inherently designed to locate individual data items? Will record-keepers be required to create a retrieval capability for record systems that do not otherwise retrieve records by individual identifier?
4. ***Conflicts.*** Do records that include information about other individuals (e.g., group therapy records) have to be disclosed as well? What rule applies when parents seek to exercise the right of access to records of medical treatment obtained independently by their children?
5. ***Exceptions.*** Are there some records that can be denied, e.g., records that would be expensive or burdensome to find, medical records when disclosure could lead to harm, records whose disclosure might interfere with litigation, records relating to employment testing, information that would identify confidential sources, records that contain trade secrets or privileged information, or records that would prematurely reveal information about law enforcement investigations? Will access/correction rules differ when record-keepers use records to make current decisions about individuals? Should statistical or research records be exempt totally or for a limited time? How should statistical and research records be defined? Should personal notes maintained by psychiatrists, supervisors, and others are exempt from access? When is a record sufficiently non-identifiable to be exempt from access and correction requests?
6. ***Enforcement.*** How will access/correction rights be enforced? Must record-keepers establish an appeal process for request denials? Can record-keepers be sued? Can a data

subject collect damages for economic loss, psychological harm, punitive damages, and attorney fees?

7. ***Correction.*** Must a record-keeper correct information obtained from another source? Does it matter if the record-keeper uses the record to make a decision? Must all incorrect information be removed or can it be marked as incorrect and retained? If incorrect records were previously disclosed to others, must the correction be sent to them, should the data subject have a choice about disseminating corrections, or should the data subject be left with the responsibility? Can fees be charged for exercise of correction rights or for sending notice to previous recipients?

Additional questions arise when applying the principle in a networked environment. How will the policy of access and correction apply to network records? How will record-keepers identify online requesters? Will online identification standards differ from offline standards? Does a right of access and correction mean that backup records and deleted records must also be searched, retrieved, disclosed, and corrected? Where multiple record-keepers maintain a common database for personal records, which has the obligation to accept requests? How will changes be managed for shared records, and how will liability be allocated in case of errors?

2.6.8 Additional Factors

Despite the importance of FIPs to EU privacy laws, another fundamental principle of EU law is relevant to the interpretation of the EU Data Protection Directive as well as instructive for the purposes of this discussion of FIPs implementation. In interpreting and applying the EU Directive, the Principle of Proportionality[194] is an important concept and one regularly cited in data protection discussions. Proportionality is a fundamental principle of European law requiring that any action should not be more burdensome than is necessary to achieve the objectives.

The principle of proportionality, which is similar to the more familiar American notion of reasonableness, is routinely mentioned as a basis for ameliorating or avoiding inappropriate, unfair, or overly expensive outcomes that might result from the strict application of a fundamental rule. For example, in the Safe Harbor framework negotiated by the Department of Commerce and the European Commission[195], the obligation to provide an individual with access to his or her own record is expressly "subject to the principle of proportionality or reasonableness and has to be tempered in certain instances." The need for EU laws to be proportionate to the objectives of data protection is a strength as well as a source of disparate interpretation and implementation. The same general constraint has broad applicability in the United States as well, and it will be invoked to avoid harsh, burdensome, or excessive outcomes in the implementation of privacy policies.

---

[194] Treaty of Amsterdam, Oct. 2, 1997, O.J. (C 340) 1 (1997), *Protocol on the Application of the Principles of Subsidiarity and Proportionality,* para. 1, at http://europa.eu.int/eur-lex/en/treaties/livre345.html.

[195] Department of Commerce, *Safe Harbor Privacy Principles,* FAQ 8 on Access, at http://www.export.gov/safeharbor/sh_documents.html.

2.6.9 Making Broad Data Protection Assessments

Applying FIPs in any context can require as much art as science. It is difficult to find any formulaic methodology for determining when a specific principle has been applied in a manner that is sufficiently protective of privacy and that is reasonable as well. What is true for one principle is also true for the multiple principles that form the basis for data protection activities. Each principle is subject to multiple interpretations and implementations so that overall judgments about privacy protections are particularly difficult. However, the difficulty of the judgments does not mean that they are impossible to make. Indeed, broad judgments about the sufficiency of privacy practices are becoming more routine and more essential to international data transfers.

The EU Directive prohibits exports of personal data to third countries that do not ensure an adequate level of protection.[196] However, the assessment of national or sectoral adequacy is not easy because of the lack of clear guidance.[197] To some extent, the lack of clarity in the Directive may well be intentional. It is not always possible to identify every element relevant to these determinations or to state how each element should be weighted. Privacy standards, especially when assessed in an international context, may be affected by political and other considerations. The EU-U.S. Safe Harbor agreement is the result of political negotiations and reflects compromises from all participants. The lack of detailed standards no doubt made it easier to reach an agreement.

Other countries use similar concepts to regulate exports to other jurisdictions, but not every law uses the same standard or measures the standard against the same circumstances in the third country. The EU judges adequacy in light of all the circumstances surrounding a data transfer.[198] The Czech Republic says that national legislation must correspond to requirements in its law.[199] The Canadian law directs an organization exporting data to use contractual or other means to provide for a comparable level of protection.[200]

At the highest level of generality, these three national policies are the same. However, application of the policies in practice may differ considerably, and some differences in results are inevitable. Nevertheless, the international community is slowly gaining experience as nations begin the process of evaluating the privacy laws, regulations, and practices of other nations. The European Union has already undertaken assessments of the privacy laws of several other nations.[201] Eventually, we may

---

[196] *EU Data Protection Directive,* at Article 25(1).

[197] This is not to suggest that there is no guidance. See, e.g., Working Party on the Protection of Individuals with Regard to the Processing of Personal Data,) *First Orientations on Transfers of Personal Data to Third Countries –Possible Ways Forward in Assessing Adequacy,* (1997) (WP 4), at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp4en.pdf. See also Charles Raab et al., *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data,* (1998) (Report prepared for the European Commission).

[198] *EU Data Protection Directive,* at Article 25(2)

[199] Act No. 101 of April 4, 2000 on the Protection of Personal Data at Article 27, at http://www.uoou.cz/eng/101_2000.php3.

[200] Personal Information Protection and Electronic Documents Act, R.S.C., ch. 5 at Schedule 1, Clause 4.1.3 (2000), at http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

[201] Available at http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/index.htm for assessments for Hungary and Switzerland.

find that many nations find it necessary to assess the privacy laws and practices of many other nations.

International experience may provide some assistance to others engaged in broad privacy assessments. Domestic assessments of privacy laws, policies, self-regulatory codes, and the like may benefit from the ongoing international privacy activities, which may eventually lead to demands for more privacy standardization. Using FIPs as a framework for assessment offers an assurance that all major information privacy elements will be considered and for doing the hard work of evaluating those elements in a fair and objective way.

2.7 Conclusion

The international consensus on privacy is based largely on the principles reflected in FIPs. That consensus is at the highest policy level, and the implementation of the principles through national laws is significantly variable. The policy consensus, however, is strong and deep, and it has lasted for more than two decades.

In the United States, the federal government has operated for more than 25 years under the Privacy Act of 1974, a statutory implementation of FIPs. Other U.S. privacy laws also implement FIPs to differing degrees. These other laws typically apply to a carefully defined set of records maintained by private sector record-keepers or, in a few cases, by state governments or schools.

It would be hard to say that there is a clear consensus in the United States around FIPs, although privacy debaters increasingly acknowledge the importance of FIPs. In recent years, some new formulations of FIPs in the United States have deviated in significant ways from the international consensus by omitting some elements and watering down others.

Other approaches to defining the substance of privacy are the subject of continuing debate. Proposals for privacy protection that rely on property rights or contract tend to offer more individual choices and fewer independent or general rules. Proponents of openness as a response to privacy are rarely concerned with the establishing of privacy rules. Technological responses to privacy protection have yet to be fully explored or implemented, but they range from wholly procedural responses to partial implementation of FIPs to individual choices without any minimum substantive rules. Statements about privacy as a fundamental human right lack specificity.

It cannot be surprising that few substantive privacy rules are to be found among marketplace proponents. It is possible to find procedural and political advice to help determine when it is appropriate to consider legislation as an alternative to other options, but marketplace proponents leave substance to the marketplace. Self-regulation may be characterized either as a standardless response to market pressures or as a recognition of the need for the creation of some common rules or policies without the direction of the government.

The protection of privacy, like other complex goals such as the protection of security, the promotion of economic growth, or the use of safe and effective drugs, requires complex judgments that cannot always be reduced to a formula. Despite the complexity of the goals and the diversity of opinions on their value and on the ways to achieve them, it is still possible to find useful and objective ways to proceed with the task. For privacy, even critics concede that one of the "great strengths" of the EU Directive is the establishment of across-the-board privacy protections.[202] The differences and difficulties in implementation of privacy should not obscure the advantages of starting from common principles.

[202] Fred H. Cate, *Privacy in the Information Age,* 110 (1997).

Section 3: Enforcement Mechanisms

3.1 Enforcement of Privacy Laws

Once policy makers decide on substantive privacy rules, they can choose from a wealth of enforcement tools. Options include familiar devices such as civil lawsuits, criminal penalties, and administrative enforcement. The purpose of this chapter is to describe the range of available enforcement methods used in the United States.

Enforcement of privacy laws or standards does not necessarily occur via a private lawsuit or formal government action. Government oversight mechanisms can play a role in encouraging privacy compliance, and these mechanisms can work even in the absence of a substantive law. Oversight alone can serve as an alternative to a statute, as a supplement to lawsuits, to encourage self-regulation, to promote the adoption of privacy enhancing technology, or to accomplish other comparable purposes. Models for government and other types of privacy institutions will be considered in a later chapter.

Private sector oversight and enforcement mechanisms can also serve as alternatives to legislation, with varying degrees of official recognition and acceptance by the courts and by other interested parties, including foreign nations. Privacy seal programs are the leading examples of private enforcement methods.

3.2 Privacy Torts

Following the suggestions of Brandeis and Warren for a privacy tort,[203] the common law developed new remedies for invasions of privacy in the last hundred years. Over forty years ago, Dean William Prosser classified a welter of common law decisions about privacy into four basic privacy torts.[204] Prosser's work was highly influential. American law now generally recognizes those four privacy torts described by Prosser. They are: 1) intrusion upon an individual's seclusion or solitude; 2) public disclosure of private facts; 3) placing an individual in a false light highly offensive to a reasonable person; and 4) an unpermitted use for private commercial gain of a person's identity. In addition, a related right often recognized is the right of publicity, or the right to control commercial use of an individual's identity. The Restatement of Torts[205] (see Sidebar 3.1) embraced Prosser's

[203] Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy,* 4 Harvard Law Review 193 (1890).
[204] William Prosser, *Privacy,* 48 California Law Review 383 (1960).
[205] 3 Restatement (Second) of Torts §652A et seq. (1977).

formulation, and most states adopted some or all of these torts through statutes or common law. These remedies are largely but not exclusively aimed at private rather than governmental actions.

Some doubt the value of privacy torts as meaningful protections for privacy, especially in the modern information age. The concerns about newspaper intrusions into private lives using new forms of technology (i.e., photography) that prompted Brandeis and Warren to write their article have been supplemented by concerns about new types of information technology and expansive databanks that the classic privacy torts may not reach. Conflicts with First Amendment values have always existed and have never been clearly resolved. In 1983, a law professor concluded that the privacy tort was a "phantom tort" that may have impeded the development of more effective remedies:

> After ninety years of evolution, the common law private-facts tort has failed to become a usable and effective means of redress for plaintiffs. Nevertheless, it continues to spawn an ever-increasing amount of costly, time-consuming litigation and rare, unpredictable awards of damages. In addition, this "phantom tort" and the false hopes that it has generated may well have obscured analysis and impeded efforts to develop a more effective and carefully tailored body of privacy-protecting laws.[206]

Doubts about the value and applicability of privacy torts increased as the information age advanced.[207] Tort remedies respond to some privacy concerns, but they do not necessarily match up with the realities of current computer and network technologies and of corporate data collection and processing activities. Because of the often-hidden nature of the commercial exchange, compilation, and use of personal information, most data subjects are unaware of the extent to which their personal information was obtained, is stored, or is being shared.[208] Sometimes, data subjects are aware of the use of their information (e.g., by receiving marketing communications), but they are not always aware of the source of the data or the extent of data sharing. The lack of transparency makes remedies difficult for consumers to consider. A law professor describes the situation in these terms:

> A market for privacy can only function effectively if there is transparency. Yet, the privacy marketplace illustrates a classic problem of market failure. The actual information practices of businesses are largely hidden from public view. . . . The barriers for individuals to discover how business[es] use their personal information are frequently insurmountable. At the same time, businesses profit enormously from a trade in personal information hidden from public view. Victims have no means of

---

[206] Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort,* 68 Cornell Law Review 291, 334 (1983).

[207] See, e.g., Fred H. Cate, *Privacy in the Information Age,* 90 (privacy torts "offer little protection for information privacy.").

[208] See, e.g., Robert Gellman, *Public Record Usage in the United States,* at 9, Paper presented at the 23rd International Conference of Data Protection Commissioners (Sept. 25, 2001), at http://www.paris-conference-2001.org/eng/contribution/gellman_contrib.html. ("The existence of cooperative databases is almost completely hidden from American consumers.").

> recourse, and no independent mechanism exists to determine whether fair information practices are followed.[209]

Analyzing current commercial data practices under the four classic privacy torts confirms the general uncertainty about a lack of recourse. It is difficult to argue that commercial data activities using personal information obtained from public and private sources result in a physical intrusion or public disclosure. It is equally difficult to argue that false light is shed. Whether there is an actionable appropriation of a name or likeness for an unpermitted use may be more of an open question.[210] Data subjects may also find that any necessity to demonstrate harm from information processing creates a substantial barrier to a lawsuit. Many in the information industry would argue that a lack of clearly demonstrable harm is evidence that the underlying data processing activities are not objectionable and should not be actionable in a court of law.

It remains unclear if privacy tort law can (or, some would say, should) provide a response to increasing commercial processing of personal information. While these processing activities remain controversial, the lack of consensus about their value and propriety may be one factor contributing to the lack of development of a direct remedy. Privacy litigation has increased in the last few years, but successful verdicts by plaintiffs in tort actions over commercial trafficking in personal information are rare. Some cases have produced settlements favorable to plaintiffs, however.[211] Many privacy cases, relying on tort, fraud, and other consumer causes of action, are currently before the courts.

Tort actions have some inherent limits. The scope of relief available through lawsuits will often be narrow (i.e., monetary damages) and may not meet or establish substantive privacy standards. For example, most FIPs elements are not directly attainable through tort litigation. A jury verdict may provide damages, but the classic privacy torts are not likely to induce or force a record-keeper to publish descriptions of record systems, limit collection practices, meet data quality standards, allow individual access and correction, or restrict internal uses of data.[212] Some of these results have been achieved through settlements. Restrictions on the disclosure of personal data may be a possible remedy for the tort of appropriation of name or likeness. Even here, basic privacy tort law provides

---

[209] Joel R. Reidenberg, *Privacy Protection and the Interdependence of Law, Technology and Self-Regulation,* 5, Paper presented at the 23rd International Conference of Data Protection Commissioners (Sept. 25, 2001), at http://www.paris-conference-2001.org/eng/contribution/reidenberg_contrib.pdf.

[210] Robert Gellman, *Does Privacy Law Work?,* Technology and Privacy: The New Landscape 193, 209-12 (Philip E. Agre & Marc Rotenberg eds., 1997).

[211] For example, in *Dennis vs. Metromail Corp.,* (No. 96-04451, 200th Judicial District, TX), a case involving the use of prisoners to process consumer surveys, a comprehensive settlement was reached. The settlement included a fund to pay actual damages, a *cy pres* fund, and remedial measures changing Metromail's business practices. The changes included no future use of prison labor, better disclosure to consumers about how data will be used, better confidentiality protections, and prompt honoring of opt-out requests).

[212] James Maxeiner, *Business Information and "Personal Data": Some Common-Law Observations About the EU Draft Data Protection Directive,* 80 Iowa Law Review 619, 622 (1995) ("Common-law privacy rights are not intended to be a response to privacy issues raised by commercial information processing activities generally. They hardly could be. They mandate no affirmative obligations, such as obligations of notification, data quality, information subject access, or security.").

that there can be no liability for use of public record information.[213] Commercial data companies routinely retrieve considerable amounts of personal information from government agencies.[214]

A second potential shortcoming with current tort remedies relates to their occasional reliance on expectations and reasonableness. Professor Paul Schwartz writes about the "silent ability of technology to erode our expectations of privacy."[215] The widespread use of computers to collect, combine, and manipulate personal information may redefine expectations and reasonableness standards long before any litigation commences. Once data use and manipulation have become commonplace and profitable, plaintiffs may find it much more difficult to argue successfully that the activities are unreasonable. This may be especially true on the Internet because "computer technology can lock-in a poor level of privacy, which will then diminish beliefs about a 'reasonable' level of privacy."[216]

[213] William Prosser, *Privacy* 48 California Law Review 383, 394 (1960).

[214] See, e.g., Federal Trade Commission, Public Workshop on the Information Marketplace: Merging and Exchanging Consumer Data (March 13, 2001) (statement of Paula Bruening, Staff Counsel, Center for Democracy and Technology), at http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm (public records reveal "a vast array of detail about an individual's life, activities and personal characteristics."); *Emerging Financial Privacy Issues, Hearing before the Subcommittee on Financial Institutions & Consumer Credit of the House Committee on Banking and Financial Services,* (1999) (testimony of Dr. Mary J. Culnan, Professor, McDonough School of Business, Georgetown University), at http://www.house.gov/financialservices/72099cul.htm ("Technology has redefined the public record. Public records formerly existed as 'puddles of data,' manual record systems or small files or databases contained on standalone computer systems. Privacy was often protected by the effort required to access to these records. Today, advances in technology and the growth of the Internet have promoted the merging of puddles into readily accessible lakes or even oceans of personal information.").

[215] Paul Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States,* 80 Iowa Law Review 553, 573 (1995).

[216] Paul Schwartz, *Privacy and Democracy in Cyberspace,* 52 Vanderbilt Law Review 1606, 1670 (1999).

Sidebar 3.1: Invasion of Privacy Torts

From the Restatement of the Law of Torts (Second):

652A. General Principle

1. One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.

2. The right of privacy is invaded by:

   a. Unreasonable intrusion upon the seclusion of another, as stated in 652B; or
   b. Appropriation of the other's name or likeness, as stated in 652C; or
   c. Unreasonable publicity given to the other's private life, as stated in 652D; or (d) publicity that unreasonably places the other in a false light before the public, as stated in 652E.

652B. Intrusion upon Seclusion

One, who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

652C. Appropriation of Name or Likeness

One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.

652D. Publicity Given to Private Life

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

1. Would be highly offensive to a reasonable person, and
2. Is not of legitimate concern to the public.

652E. Publicity Placing Person in False Light

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if

1. The false light in which the other was placed would be highly offensive to a reasonable person, and
2. The actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

3.3 Constitutional Litigation

The U.S. Constitution – particularly the Bill of Rights – provides direct and indirect protections for a surprising variety of privacy rights and interests. In a famous statement from a 1965 privacy decision involving state law restricting contraceptives, Mr. Justice William O. Douglas described the zones of privacy rights and interests addressed directly or indirectly in the Constitution by citing five different amendments in the Bill of Rights:

> The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. . . . Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[217]

Constitutional litigation over privacy rights is common.[218] For example, the Fourth Amendment's protection against unreasonable searches and seizures is tested in court every day across the country. The Federal Constitution gives individuals rights only against the government and not against other individuals or legal persons. Individuals harmed by private parties must rely on tort, contract, or other remedies.[219]

Constitutional litigation over information privacy matters appears to be growing, but the scope of the constitutional protection remains uncertain. In 1977, the Supreme Court addressed informational privacy issues in *Whalen v. Roe*,[220] a case involving a clash between the privacy of medical records and the ability of the state to mandate reporting of patient information. The decision, however, left considerable confusion about the status of a constitutional right to information privacy.[221]

---

[217] *Griswold v. Connecticut,* 381 U.S. 479, 484 (1965) (citation omitted).

[218] 42 U.S.C. §1983 provides a civil cause of action in federal court for violations of the Constitution.

[219] By contrast, the California Constitution expressly identifies privacy as an inalienable right. One purpose of the constitutional provision on privacy, which was adopted by referendum in 1974, was to address personal control over the circulation of personal information. The California Supreme Court held in 1994 that the constitutional protection applied to both the public and private sectors. *Hill v. NCAA,* 865 P.2d 633 (S. Ct. Cal. 1994). See also Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law,* 132-137 (1996). California has "the strongest constitutional scheme of data protection in the United States." *Id.* at 135.

[220] 429 U.S. 589 (1977).

[221] Compare, e.g., *Slayton v. Willingham,* 726 F.2d 631 (10th Cir. 1984) (finding that the Supreme Court has explicitly recognized that the constitutional right to privacy encompasses an individual interest in avoiding disclosure of personal matters) with *J.P. v. DeSanti,* 653 F.2d 1080 (6th Cir. 1981) (failing to interpret *Whalen* as creating a constitutional right to

Several recent lower court cases have found, in some instances, that a right of information privacy does exist. For example, in 1998, the Sixth Circuit held that undercover police officers have a privacy interest of a constitutional dimension in certain personal information contained in their personnel files.[222] In 1999, the Tenth Circuit held that the constitutionally protected privacy interest in avoiding disclosure of personal matters clearly encompasses medical information and its confidentiality, including both collection and dissemination of the information.[223]

In 1980, the Third Circuit decided a case involving a subpoena to an employer for its employees' medical records for use in an investigation of a possible health hazard in the workplace.[224] The most notable part of the decision listed factors to be considered in deciding whether an intrusion into an individual's privacy is justified. The seven factors identified by the court were: (1) the type of record requested; (2) the information it does or might contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosure; (6) the degree of need for access; and (7) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest favoring access.[225] The importance of this decision is the identification of specific elements to be considered in weighing a privacy interest. Given the narrow context of the case, it is hard to characterize this list as a complete statement of the constitutional interest in information privacy. Nevertheless, the decision takes a clear step toward identifying those factors, at least when assessing the needs of government against the privacy interests of data subjects.

Some read existing case law and already see a constitutional right of information privacy.[226] While it will likely take additional litigation to clarify the law in this area, a constitutional right of information privacy has the potential to impose some broad constraints on *government* activities. However, the scope of any constitutional right to information privacy and the extent to which the right may meet international privacy standards remain uncertain and difficult to predict.[227] Additional constitutional litigation may eventually provide a clearer definition of the duties of government with respect to personal information. Even if it does, however, the courts are not likely to provide clear, direct, or comprehensive guidance any time soon. It can take years or decades before the right case comes along that can result in better guidance from the courts.

---

have all government action weighed against the resulting breach of confidentiality) with *Borucki v. Ryan,* 827 F.2d 836 (1st Cir. 1987) (*Whalen* appears to have specifically reserved decision whether there is a constitutionally rooted duty of nondisclosure regarding personal information collected by the state under assurances of confidentiality).

[222] *Kallstrom v. City of Columbus,* 136 F.3rd 1055 (6th Cir. 1998).

[223] *Norman-Bloodsaw v. Lawrence Berkeley Laboratory,* 135 F.3rd 1260 (10th Cir. 1998).

[224] *United States v. Westinghouse Electric Corp.,* 638 F.2d 570 (3d Cir. 1980).

[225] *Id.* at 578.

[226] Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Information Privacy,* 10 Southern Illinois University Law Review 479 (1990).

[227] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law,* 89-90 (1996) (constitutional right of information privacy provides some of the required elements of European fair information practices).

3.4 Statutory Rights of Action

One traditional remedy for private violations of individual interests is a statutory cause of action. In theory, the model is simple and direct. An aggrieved individual sues the person who violated the statute and the individual's rights. As the Sidebar 3.2 on enforcement options in federal privacy laws shows, private rights of action are commonplace in privacy legislation. It is noteworthy, however, that neither privacy law passed since 1998 (Children's Online Privacy Protection Act and Gramm-Leach-Bliley) provides for any individual enforcement.

Sidebar 3.2: Enforcement Options in Federal Privacy Laws

Privacy Laws (1)	Criminal Penalties	Civil Remedies	Administrative Enforcement	State Enforcement Authorized
Privacy Act of 1974	X	X	X	
Fair Credit Reporting Act		X	X	X
Family Educational Rights and Privacy Act		(2)	X	
Cable Communications Policy Act		X	X	
Video Privacy Protection Act		X		
Driver's Privacy Protection Act	X	X		
Tele-communications Act		X	X	
Children's Online Privacy Protection Act			X	X
Gramm-Leach-Bliley			X	
Health Insurance Portability and Accountability Act	X		X	

(1) For citations to these laws, see the previous chart.
(2) For a discussion of the status of civil remedies under the Family Educational Rights and Privacy Act, see the discussion below under Administrative Enforcement.

Chart Notes

Other laws addressing personal privacy matters not included in the chart have enforcement provisions. The Right to Financial Privacy Act (29 U.S.C. §3401 et seq.) provides civil remedies. The Electronic Communications Privacy Act of 1986 includes criminal penalties and civil remedies. The Telephone Consumer Protection Act (47 U.S.C. §227) includes civil remedies, administrative enforcement, and enforcement by state governments.

3.5 Individual Rights of Action

3.5.1 Privacy Act of 1974

The Privacy Act of 1974 establishes privacy standards for federal agencies. The Act addresses all elements of FIPs, and it includes several different types of enforcement. While the focus here is on statutory rights of action, this section will review all enforcement methods for the Act to put the civil remedies in a broader perspective.

The Privacy Act of 1974[228] allows an individual to sue a federal agency if the agency –

- has not complied with a request for access;
- has not amended a record in accordance with a request;
- has made an adverse determination based on a record that was not maintained with enough accuracy, relevance, timeliness, and completeness as necessary to assure fairness in making determinations about the individual; or
- has failed to comply with any other provision of the Act in a way that resulted in an adverse effect on an individual.

A successful plaintiff under the Act is entitled to injunctive relief only if an agency improperly withheld records or improperly denied a request for amendment. A court cannot enjoin an agency that failed to comply with other provisions of the Act, but a court can award damages.[229] A plaintiff can receive actual damages resulting from intentional or willful agency non-compliance, with a minimum award of $1,000. A successful plaintiff can also receive costs and attorney fees.

It is not easy, however, to win damages under the Act. The Act's high standard (*intentional or willful*) is a "formidable barrier for a plaintiff seeking damages."[230] Further, case law is split over whether a plaintiff must show actual out-of-pocket expenses before receiving the minimum amount. Courts are also split over whether no pecuniary damages for physical and mental injury – such as emotional trauma or fear – can be recovered.[231] These restrictions on damages, while not universally adopted, show how a statutory scheme can be affected by judicial interpretation. Whether the judicial interpretations constitute a narrowing of the Congressional intent is, of course, a matter of dispute.

The 1977 review by the Privacy Protection Study Commission (PPSC) criticized the civil remedy section of the Act as "ineffective from the individual's point of view."[232] The PPSC noted that the

---

[228] 5 U.S.C. §552a(g). The Act allows the Central Intelligence Agency and some law enforcement agencies to exempt themselves from the civil remedy provision. *Id.* at 552a(j).
[229] Department of Justice, *Privacy Act Overview,* at Civil Remedies E. (May 2000), at http://www.usdoj.gov/04foia/04_7_1.html
[230] *Id.*
[231] *Id.*
[232] Privacy Protection Study Commission, *Personal Privacy in an Information Society,* 529 (1977).

cost and time involved in bringing a lawsuit often makes individual enforcement impractical. Statistics provided by the Transactional Records Access Clearinghouse at Syracuse University show that from 1992 through 1999, plaintiffs filed 505 civil cases under the Privacy Act of 1974.[233] The substantial number of filed and reported decisions under the Privacy Act suggests that individuals have sought enforcement of at least some provisions of the Act. The PPSC's judgment on this point may have been premature. However, it is impossible here to assess whether plaintiffs deserved or were able to achieve adequate remedies.

The PPSC also concluded that it is too difficult to meet the Privacy Act's requirements for damages. This assessment appears to be closer to the mark. The PPSC recommended that Congress amend the law to make it more likely for an aggrieved plaintiff to recover damages.[234] Congress never seriously considered the recommendation.

The civil remedies in the Privacy Act should be assessed in light of other enforcement and oversight provisions of the law. The Act includes several other types of enforcement. Violations of the Act can result in criminal penalties. A government employee who improperly discloses personal information or who maintains a system of records without required public notice is guilty of a misdemeanor and may be fined up to $5,000. Any person who obtains a record about an individual under false pretenses is also guilty of a misdemeanor and may be fined the same amount.[235] Statistics provided by the Transactional Records Access Clearinghouse at Syracuse University found that from 1992 through 1999, federal agencies referred 34 Privacy Act cases for prosecution. Six of these cases resulted in convictions, one prosecuted defendant was found not guilty, and the rest were not prosecuted.[236] Even though only a small number of referred cases were prosecuted, even a referral is a notable event that is likely to send a signal to federal employees that an agency is aware of and actively pursuing criminal enforcement of the Act.

The Act assigns an oversight role to the Office of Management of Budget. The law directs OMB to provide continuing assistance to agencies and to develop guidelines and regulations for the use of agencies in implementing the Act.[237] Agencies must inform OMB and the Congress in advance of the establishment of or significant change in a system of records or computer matching program.[238] The purpose of the report is "to permit an evaluation of the probable or potential effect" on privacy or other rights of individuals.[239]

---

[233] Available at http://trac.syr.edu/. The information came from TRAC's Fedprobe facility.
[234] *Id.* at 528-32.
[235] 5 U.S.C. §552a(i).
[236] Available at http://trac.syr.edu/. Of the six convictions, five were obtained in 1995 in the northern district of Iowa against employees of the Agriculture Department.
[237] *Id.* at 552a(v).
[238] *Id.* at 552a(r), added by the Computer Matching and Privacy Protection Amendments of 1988, Public Law 100-503 (1988).
[239] *Id.*

When the Act was new, OMB did a good job in issuing guidelines and providing support to agencies. However, a 1983 Congressional report found that OMB's interest in the Privacy Act of 1974 "diminished steadily" since 1975.[240] For example, when computer matching arose as a privacy issue starting in the late 1970s, OMB eventually issued guidance to agencies. However, a Congressional study found that OMB made no effort to monitor agency compliance with its 1982 guidelines.[241] A 1985 GAO report on computer matching noted, "existing Federal guidance appears to lack an effective compliance enforcement mechanism."[242] A 2000 GAO report on Internet privacy discusses more recent OMB privacy initiatives and indicates some more interest and activity on the part of OMB.[243] The appointment in 1999 of a Chief Counselor for Privacy located in OMB sparked increased activity on the Privacy Act and on other privacy issues during the last 18 months of the Clinton Administration. The Bush Administration did not continue the position of Chief Counselor for Privacy, and it appears that privacy activity in OMB may have returned to previous levels.

Another opportunity for OMB oversight came through the annual reporting requirement. As originally enacted, the Privacy Act required the President to submit an annual report to the Congress listing each system of records that agencies exempted from the law. In addition, the report was supposed to include other information about administration of the Act.[244] The first annual reports were lengthy documents, some in two volumes, with considerable amounts of information. Beginning with the report covering calendar year 1980, OMB began to submit shorter, less complete reports. Some annual reports failed to include all required statutory elements.[245] In 1982, OMB recommended elimination of the annual reporting requirement, but Congress rejected the recommendation and expanded the required contents of the reports.[246]

---

[240] *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress,* House Report 98-455, at 35 (1983). Some Members of Congress offered separate views about the role of OMB. One Member who participated in the drafting of the Privacy Act of 1974 thought that OMB's performance should be evaluated against the Congressional expectation at the time of passage. His view was that Congress expected little from OMB. *Id.* at 56-57 (Separate views of John N. Erlenborn). Other Republicans noted that Congressional expectations increased as a result of the passage of the Paperwork Reduction Act of 1980 and that they expected regular and systematic oversight of privacy. *Id.* at 58 (Separate views of Thomas N. Kindness, Frank Horton, Lyle Williams, Dan Burton, Tom Lewis, Alfred A. McCandless, Larry E. Craig, and Dan Schaffer).
The 1983 Congressional report discussed the role of Congress in overseeing the Privacy Act. The report documented a fair amount of Congressional oversight from the time of the Act's passage through 1983. *Id.* at 37-55. The limited evidence available for subsequent years suggests a diminishing Congressional interest in the Act until the last few years when interest in privacy revived.

[241] *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress*, House Report 98-455, at 36 (1983).

[242] General Accounting Office, *Eligibility Verification and Privacy in Federal Benefit Programs: A Delicate Balance,* 12 (1985) (GAO/HRD-85-22).

[243] General Accounting Office, *Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy*, (2000) (GAO/GGD-00-191).

[244] Public Law 93-579, 5 U.S.C. §552a(p).

[245] In a 1983 investigative report, The House Committee on Government Operations found that the 1980 and 1981 reports failed, among other things, to include information on the Act's administration. *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress,* House Report 98-455, at 24-27 (1983).

[246] Congressional Reports Elimination Act, Public Law 97-375, §201 (1982), amending 5 U.S.C. §552a(p).

When passing the Computer Matching and Privacy Protection Amendments of 1988, Congress changed the reporting from annual to biennial.[247] The 1988 amendments also changed the substantive reporting requirements for system reports with the goal of obtaining more useful information for oversight purposes.[248] Congress also added a requirement for an OMB report on computer matching. The law mandated an annual report for the first three years and a biennial report thereafter.[249] The 1988 amendments show a continuing Congressional interest in reports on privacy from OMB.

In 1995, Congress repealed the annual Privacy Act reporting requirement as part of a broader change in regular Congressional reporting.[250] However, the 1995 changes did not alter the requirement for the computer matching report. It is unclear why Congress continued only the matching report, but it is possible that failure to eliminate it was an oversight.

The variety of enforcement mechanisms for the Privacy Act of 1974 suggests a serious Congressional concern that agencies be held accountable for compliance. No other U.S. privacy law ever included so many accountability mechanisms. However, the evidence suggests that the accountability mechanisms have not worked well.

3.5.2 Cable Communications Policy Act

[247] Computer Matching and Privacy Protection Amendments of 1988, Public Law 100-503, §8 (1988).
[248] See House Committee on Government Operations, *Computer Matching and Privacy Protection Act of 1988,* House Report 100-802, at 37 (1988) (report to accompany H.R. 4699).
[249] 5 U.S.C. §552a(u)(6).
[250] 5 U.S.C. §552a(s) repealed by The Federal Reports Elimination and Sunset Act of 1995, Public Law 104-66, § 3003, (1995), amended by Public Law 106-113, § 236 (1999) (changing the effective date to May 15, 2000).

The Cable Communications Policy Act[251] offers another example of a privacy law that includes a statutory private right of action, this one for cable television subscribers against cable operators. The Privacy Act of 1974, discussed in the previous section, allows a data subject to sue the federal government. The cable law allows a data subject to sue a *private sector* record-keeper. The private right of action is the only enforcement mechanism specified in the privacy section of the cable law.

The cable law, which addresses all but one of the FIPs, allows civil litigation in U.S. district court for any violation of its privacy provisions.[252] Because the Act establishes standards for openness, data quality, purpose specification, use limitation, and individual participation (access and correction), a cable operator's failure to comply with any of these FIPs could form the basis for a lawsuit. The cable law provides that its remedies are in addition to any other lawful remedy available to a cable subscriber.[253] This means that the federal cable law does not preempt any state or local cable privacy laws that are consistent with the federal requirements.[254] Enforcement activity by the Federal Communications Commission, which has general regulatory responsibilities under the cable law, is a possibility.

Possible recoveries include actual damages, punitive damages, attorney fees, and costs. As a floor for actual damages, the Act establishes liquidated damages to be computed at the rate of $100 per day for each day of violation or $1,000, whichever is higher.[255] The damages for a violation could be significant. A cable operator that sent a defective notice and did not correct the deficiency for a year could theoretically have to pay $36,500 in liquidated damages to *each* subscriber. A court could, however, award smaller amounts.

In practice, the ability of cable subscribers to enforce the cable law has been limited by judicial decision. In one of the few reported cases under the law, a district court refused to certify a class action in a case involving an alleged violation of the privacy provisions.[256] Without the ability to file class actions, much of the incentive that plaintiffs and their attorneys have to bring lawsuits to enforce privacy statutes is reduced or eliminated. The decision to restrict class actions under the cable law illustrate that litigation procedures can have a significant impact on private enforcement techniques.

3.6 Criminal Penalties

Some privacy laws include criminal penalties for violations. The criminal penalties of the Privacy Act of 1974 have already been discussed. In some instances, criminal penalties may be a consequence of the politics of Congressional committee jurisdictions. In the example discussed below, the Driver's Privacy Protection Act originated in the House and Senate Committees on the

[251] 47 U.S.C. §551.
[252] *Id.* at (f)(1).
[253] *Id.* at (f)(3).
[254] *Id.* at (g).
[255] *Id.* at (f)(2)(A).
[256] *Wilson v. American Cablevision of Kansas City*, 133 F.R.D. 573 (W.D. Mo. 1990).

Judiciary. In the absence of criminal penalties for violations, the bill that ultimately passed might not have been referred to the committees that had the strongest interested in passing legislation on the subject.

Congressional committees other than the Committees on the Judiciary can propose legislation with criminal penalties. However, criminal penalties are only occasionally used. The Driver's Privacy Protection Act, the Privacy Act of 1974, and the Electronic Communications Privacy Act are the only privacy laws that use criminal penalties for enforcement.

The Driver's Privacy Protection Act[257] (DPPA) is a federal privacy law regulating how states may process motor vehicle records, including driver's licenses and motor vehicle registrations. The DPPA is unusual in that it establishes *federal* privacy rules for records maintained by the states.[258]

The DPPA calls for a criminal fine for anyone who violates its standards by obtaining or disclosing personal information. Making false misrepresentation to obtain personal information is also unlawful.[259] State motor vehicle departments that have a policy or practice of substantial noncompliance with the DPPA can be subject to a civil penalty of not more than $5,000 per day. The U.S. Attorney General can impose the civil penalty.

In addition to the criminal penalties, the DPPA created a civil cause of action for a data subject against any person who obtains, discloses, or uses personal information from a motor vehicle record for an impermissible purpose. The remedies allowed by the statute include: 1) actual damages, but not less than $2,500 in liquidated damages; 2) punitive damages in cases of willful or reckless disregard of the law; and 3) attorneys fees and costs.

3.7 Administrative Enforcement

For some statutes administered by a regulatory agency, the possibility of administrative enforcement may be part of the basic statutory authority of the agency. For example, Sidebar 3.2 on enforcement options shows that both the Cable Communications Policy Act and the Telecommunications Act include the possibility of administrative action in addition to civil remedies expressly provided in the laws. The express inclusion of civil remedies suggests that Congress saw private lawsuits as the primary method of enforcement. These laws can be distinguished from other laws where Congress provided that administrative enforcement was the only enforcement option and private rights of action were deliberately excluded. Three of these laws, including two of the most recent privacy laws, will be described here.

---

[257] 18 U.S.C. §2721-25.

[258] The U.S. Supreme Court decided a dispute over the constitutionality of the Driver's Privacy Protection Act by finding that the law did not violate federalism principles. The decision upheld the constitutionality of the law, which had been challenged by several states as a violation of the Tenth and Eleventh Amendments of the U.S. Constitution, but the Court did not address privacy issues in its opinion. *Reno v. Condon,* 528 U.S. 141 (2000).

[259] The Transactional Records Access Clearinghouse at Syracuse University could not find any record of criminal prosecutions under the DPPA. Available at http://trac.syr.edu/.

1. Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)[260] establishes privacy rules for schools and universities that receive federal funds through the Department of Education. The law covers *education records* that contain information directly related to a student, and it establishes rules governing collection, use, disclosure, access, and correction. FERPA charges the Secretary of Education with enforcement responsibilities.

The major enforcement weapon in the statute is the termination of federal funding. FERPA regulations identify three enforcement methods: 1) withholding payments under any applicable program; 2) complaints to compel compliance through a cease-and-desist order; and 3) termination of eligibility to receive funding under any applicable program. The statute makes it clear that ending funding is a last resort.

FERPA itself provides no express private right of action against educational institutions for privacy violations.[261] However, some courts decided that FERPA violations may be challenged under 42 U.S.C. §1983, a civil rights statute that allows a civil action against government officials for deprivation of rights secured by the Constitution and laws. The details of §1983 jurisdiction are complex and not relevant here, but enforcement of privacy laws against government officials through this means is a realistic possibility.[262] It is possible, however, for Congress to pass a law and expressly foreclose enforcement through §1983 so the civil right statute need not become a more universal remedy for public sector privacy statutes that only have administrative enforcement.

2. Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act of 1998 (COPPA)[263] establishes rules governing the collection, maintenance, use, and disclosure of individually identifiable personal information obtained online from children under the age of 13. Congress assigned the Federal Trade Commission to promulgate rules and to be the principal enforcement agency.[264] The statute did not provide for a private right of action or for any other method of individual enforcement.

The FTC's rules[265] provide that a violation of the COPPA rules will be treated as a violation of the FTC's long-standing rule defining an unfair or deceptive act or practice under general FTC law.[266]

---

[260] 20 U.S.C. §1232g. FERPA is sometimes called the *Buckley Amendment*.
[261] See, e.g., *Tarka v. Franklin,* 891 F.2d 102 (5th Cir. 1989), *cert. denied*, 494 U.S. 1080, *reh. denied*, 496 U.S. 913 (1990).
[262] See *Falvo v. Owasso Independent School District,* 33 F.3d 1203 (10th Cir. 2000), *cert. granted* (U.S. June 25, 2001) (No. 00-1073), at http://www.supremecourtus.gov/orders/courtorders/062501pzor.pdf.
[263] 15 U.S.C. §6501 et seq.
[264] Because of limitations in FTC jurisdiction, other agencies are responsible for enforcement of COPPA for some sectors. 15 U.S.C. §6506. For purposes of the analysis in this report, the shared jurisdiction is not important. In any event, the FTC is clearly the lead agency for COPPA.
[265] 15 C.F.R. §312.9.
[266] 15 U.S.C. §57a(a)(1)(B).

The FTC's complaint process invites the submission of complaints through the FTC's website. However, the FTC expressly tells complainants that it "does not resolve individual consumer problems."[267] Complaints may "lead to law enforcement action."[268] A website operator who violates the FTC's COPPA rules can be liable for civil penalties of up to $11,000 per violation.[269]

The COPPA statute provides two other methods of enforcement. First, the attorney general of a State is authorized to bring an enforcement action on behalf of the residents of the State. Available relief includes injunctions and damages or other compensation.[270] States must notify the FTC before filing an action.

COPPA also authorizes the FTC to approve self-regulatory (or *Safe Harbor*) guidelines that may be developed by representatives of the marketing or online industries.[271] Under the FTC's regulations, incentives for compliance with self-regulatory guidelines may include: 1) mandatory and public reporting of disciplinary actions taken against violators of the guidelines; 2) consumer redress; 3) voluntary payments to the U.S. Treasury for violators; and 4) referral to the FTC of operators who engage in a pattern or practice of violations.[272]

3. Health Insurance Portability and Accountability Act

In 1996, Congress authorized the development of uniform standards for the electronic transmission of health information. The Administrative Simplification Subtitle of the Health Insurance Portability and Accountability Act (HIPAA)[273] authorized the Secretary of Health and Human Services (HHS) to promulgate regulations on health privacy if Congress did not pass legislation by 1999.[274] When the Congressional deadline expired without action, the Secretary began the regulatory process and issued final regulations in December 2000.[275] The regulation is final, but it does not take effect until 2003.

The Administrative Simplification Subtitle of HIPAA included several enforcement mechanisms. First, the Secretary is authorized to impose civil penalties for any violation of the standards authorized under the subtitle.[276] The civil penalties apply to privacy and to other HIPAA standards. Second, the statute includes a criminal penalty for wrongful disclosure of individually identifiable

---

[267] Available at https://rn.ftc.gov/dod/wsolcq$.startup?Z_ORG_CODE=PU01.
[268] *Id.*
[269] Federal Trade Commission, *Frequently Asked Questions about the Children's Online Privacy Protection Rule,* (Volume 1) (COPPA Enforcement), at http://www.ftc.gov/privacy/coppafaqs.htm#enforce.
[270] 15 U.S.C. §6505.
[271] *Id.* at §5604. Other persons may also seek approval for self-regulatory guidelines.
[272] 15 C.F.R. §312.10(b)(3).
[273] Title II, Subtitle F of Public Law 104-191.
[274] 42 U.S.C. §1320d-2 note.
[275] 45 C.F.R. Parts 160 & 164.
[276] 42 U.S.C. §1320d-5.

health information. The criminal penalty can be as high as $250,000 and imprisonment for ten years. Not all breaches of the privacy standard are subject to the criminal penalties.

The privacy rules issued by the Secretary do not provide for any civil lawsuits by aggrieved data subjects. The Secretary did not believe that the statute authorized establishing private rights of action through regulations.[277] The Secretary designated the HHS Office for Civil Rights as the departmental component responsible for implementing and enforcing the privacy regulation.[278] HHS will accept complaints about noncompliance with HIPAA privacy rules, and the Department "may" investigate the complaints.[279] The rules do not provide a mechanism that would allow an individual to recover damages for violations of the rules. The Department expects to issue additional regulations about HIPAA enforcement.

3.8 Self-regulation/Free Market/Privacy Seals

Self-regulation[280] for privacy can be accomplished in a variety of ways, including but not limited to individual company acceptance of complaints from individuals, independent resolution of complaints through private or government mechanisms, audits, privacy seal programs, and government supervision/certification of self-regulatory programs. Self-regulation can also extend to the establishment of private rights through contracts or other devices, with the possibility of judicial enforcement in contract, tort, or other forms of litigation.

A significant issue with self-regulation is defining its scope. Drawing sectoral boundaries can present the same problems for self-regulators as for statute writers. The Gramm-Leach-Bliley[281] law on privacy of consumer financial information made the scope problem more apparent. While the law principally regulated banks and comparable financial institutions, the regulations also covered real estate appraisers, automobile dealerships, career counselors, check printers, accountants, travel agencies, and others who might not be otherwise considered the equivalent of banks.[282] In addition, privacy rules for health care institutions and financial institutions overlap because financial institutions conduct some health care financial arrangements and vice versa. The Gramm-Leach-Bliley regulations include a rule explaining how the financial privacy rules interface with the health care privacy rules under HIPAA.[283]

Consider, for example, the rules (statutory or self-regulatory) that might apply to a transaction that includes a consumer authorizing over the Internet an electronic payment to a health care provider

---

[277] 65 Fed. Reg. 82605 (Dec. 28, 2000).
[278] See the HIPAA privacy website of the Office of Civil Rights, at http://www.hhs.gov/ocr/hipaa/.
[279] 42 C.F.R. §160.306.
[280] Self-regulation comes in a variety of forms and flavors. For a taxonomy of self-regulatory approaches, see Douglas C. Michael, *Federal Agency Use of Audited Self-Regulation as a Regulatory Technique,* 47 Administrative Law Review 171 (1995).
[281] 15 U.S.C. §6801-6809.
[282] See Federal Trade Commission, *Privacy of Consumer Financial Information*, 15 C.F.R. §313.3(k). Other agencies with regulatory authority for Gramm-Leach-Bliley issued comparable regulations. See 15 U.S.C. §6805 (identifying other agencies with shared regulatory authority for financial privacy matters).
[283] 15 C.F.R. §313.1(b).

for a co-payment required by a health insurer. Is the record of the transaction an Internet record, bank record, health record, insurance record, or something else? What happens when one institution plays more than one role in the transaction? For example, the bank could also be the Internet service provider. The problem of defining sectoral boundaries has not received much attention.[284]

FIPs are widely recognized substantive standards for information privacy. However, there are no generally accepted standards for identifying or assessing the core elements for enforcement in privacy self-regulation programs.

The FTC's work on privacy and self-regulation includes the Commission's own limited set of FIPs as substantive privacy criteria.[285] However, the Commission did not offer any clear criteria for assessing self-regulatory programs, other than to comment on whether the evidence from its administrative record demonstrated "meaningful broad-based privacy protections."[286] In other words, the Commission looked at the breadth of self-regulatory programs, but it made no attempt to measure the depth of the programs.

The Article 29 Working Party, established under the EU Directive, has some useful guidance on measuring self-regulation. The Working Party acknowledged the difficulty of assessing the effectiveness of a self-regulatory code,"[287] but it proceeded to suggest three functional criteria for measuring effectiveness: 1) a good level of compliance; 2) support and help to individual data subjects; and 3) appropriate redress.[288] These criteria identify elements that are useful in judging self-regulatory enforcement activities, although they have not been widely cited outside the EU. The use of these criteria within the EU, however, is not without importance, as the discussion of Safe Harbor will show later.

The Online Privacy Alliance (OPA), a cross-industry coalition of more than 80 global companies and associations committed to promoting the privacy of individuals online, identifies five elements of a self-regulatory program. They are: 1) third-party enforcement programs; 2) privacy seal programs; 3) verification and monitoring; 4) consumer complaint resolution; and 5) education and outreach.[289] The OPA elements are broadly similar to the criteria from the Article 29 Working Party.

---

[284] For more on definitional problems and conflicts that can arise with sectoral privacy self-regulation, Robert Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules,* 41 Villanova Law Review 129, 143-145 (1996).

[285] Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress,* (1999), at http://www.ftc.gov/os/1999/9907/privacy99.pdf. *Privacy Online: Fair Information Practices in the Electronic Marketplace,* at 35 (May 2000), at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[286] *Id.* at 35.

[287] European Commission Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Judging Industry Self-Regulation: When Does It Make a Meaningful Contribution to the Level of Data Protection in a Third Country?*, 3 (1998) (WP 7), at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp7en.pdf.

[288] *Id.* at 3-5.

[289] Available at http://www.privacyalliance.org/resources/enforcement.shtml.

3.8.1 Federal Trade Commission Enforcement through Unfair or Deceptive Trade Practices

The FTC has some authority over the collection and dissemination of personal data based on Section 5 of the Federal Trade Commission Act.[290] The FTC Act prohibits unfair and deceptive practices in and affecting commerce. It authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations. The Act provides a basis for government enforcement of the privacy policies of companies subject to its jurisdiction. For instance, failure to comply with stated information practices may constitute a deceptive practice, and the Commission has authority to pursue the remedies available under the Act for such violations. The Commission has brought several enforcement actions.[291]

However, the Commission's authority covers only those instances in which a company subject to its jurisdiction actually adopted a privacy policy. The Commission can hold a company to compliance with a stated privacy policy. However, the Commission never issued rules requiring companies either to adopt information practice policies or to abide by fair information practice principles on their websites.[292] The one exception is for websites that collect information from children under the age of 13, where COPPA establishes privacy requirements that the websites must meet.[293]

The Commission's authority over unfair and deceptive practices provides an enforcement backstop for some privacy self-regulatory programs. This authority may be in addition to other self-regulatory enforcement methods described here. However, the Commission does not resolve individual consumer problems and may not offer any meaningful help to individual consumers who have been harmed by a company's failure to comply with a stated privacy policy.

3.8.2 Compliance Audits

The privacy principles of one trade association illustrate the use of compliance audits. The Individual Reference Services Group (IRSG) is an association of commercial services that provide data to help identify, verify, or locate individuals. The substantive provisions of its privacy principles are not of interest here.[294]

IRSG Principle XI requires member companies to hire a reasonably qualified independent professional service at least once a year to conduct an assurance review. A summary of the review must be made publicly available.[295] The review is the only enforcement mechanism in the IRSG rules. The principles do not require member companies to entertain complaints from individuals or

---

[290] 15 U.S.C. §45.

[291] See Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace,* at n.21 (May 2000), at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf and http://www.ftc.gov/privacy/coppafaqs.htm#enforce.

[292] Whether the Commission could or would issue substantive privacy rules for websites or others engaged in interstate commerce is an open and controversial question.

[293] 15 U.S.C. § 6501 et seq.

[294] The Federal Trade Commission reviewed the IRSG principles in 1997. Federal Trade Commission, *Individual Reference Services: A Report to Congress,* (1997), at http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

[295] Available at http://irsg.org/html/industry_principles_principles.html.

even to allow individuals to obtain access to all records about themselves.[296] Individuals do have limited ability to seek corrections of IRSG records,.

IRSG published reasonably detailed assurance criteria for the assessments.[297] It is not clear how those criteria are used in the reviews. The public disclosure of the results of the reviews offers only a one-line statement that the companies are in compliance with the principles.[298] Regardless of how the IRSG companies actually conduct and report on the compliance audits, the framework is noteworthy for its published criteria, annual review, and commitment to publish the results.[299]

3.8.3 Privacy Seals

Privacy seals are privately operated, voluntary programs that allow qualifying online merchants to display a trademarked logo intended to let web users identify companies that that meet the program requirements. Two of the leading privacy seal programs are BBBOnline[300] and TrustE.[301] These two programs are roughly comparable, and only the BBBOnline program, operated by the Better Business Bureau, will be described here. The substantive privacy requirements of the BBBOnline program were discussed in the previous chapter.

The BBBOnline Program has three basic enforcement elements. First, an applicant must complete a Compliance Assessment Questionnaire that is used to determine if an organization is eligible for the program. BBBOnline reviews the questionnaire and the organization's website before accepting the application.[302] Second, the organization must annually certify that its practices are unchanged or must submit a new application and compliance assessment.[303] Third, the organization must agree to participate in BBBOnLine's Privacy Program Dispute Resolution Process and to abide by its decisions.[304]

The dispute resolution process accepts complaints about the use of "personally identifiable information" and "prospect information" in an online or electronic commerce environment. BBBOnline will also accept complaints about organizations that are not participants in its seal

---

[296] See Federal Trade Commission, *Individual Reference Services: A Report to Congress,* (1997), at http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.html ("The IRSG principles do not give consumers access to the public information maintained about them and disseminated by the look-up services. Accordingly, consumers will not be able to check for inaccuracies resulting from transcription or other errors occurring in the process of obtaining or compiling the public information by the look-up services.").

[297] *The Individual Reference Services Group Privacy Principles Assurance Criteria,* at http://irsg.org/html/criteria.htm.

[298] Available at http://irsg.org/html/3rd_party_assessments.html.

[299] At the end of 2001, the Individual Reference Services Group announced that it would disband. See the announcement, at http://irsg.org/html/termination.html. Although the organization no longer exists, its policy still serves as one of the few examples of a self-regulatory compliance review program.

[300] Available at http://bbbonline.org/.

[301] Available at http://www.truste.org/.

[302] Available at http://bbbonline.org/privacy/apply.asp.

[303] BBBOnLine Privacy Program Participation Agreement at 4.B. (Renewal Terms), at http://bbbonline.org/privacy/license.pdf.

[304] Available at http://bbbonline.org/privacy/dr.asp.

program,[305] although it is not clear how effective the dispute program will be with companies that did not agree to participate in advance of a complaint.

The dispute resolution program operates under published rules.[306] If the subject of a complaint does not comply with the program's decision, BBBOnline may undertake a seal compliance review and may refer the case to "the appropriate government agency."[307] The most likely agency is the FTC, which agreed to review referrals from privacy self-regulatory organizations. FTC jurisdiction over unfair or deceptive act or practices in commerce gives the Commission the ability to challenge the failure of a company to comply with its stated privacy policy. The Commission did just that in one case.[308] If a company agreed to comply with a dispute resolution service offered by a privacy seal program and then failed to live up to the agreement, the FTC could presumably take action for that failure as well. There are no reported cases of FTC action in privacy dispute matters.

3.9 Export Restrictions and the Safe Harbor

Privacy laws in European Union Member States and in an increasing number of other countries prohibit the export of personal data to another country that does not provide adequate privacy protections. The Safe Harbor framework negotiated between the European Union and the United States allows participating companies to continue to import personal data into the United States from Europe in the absence of a generally adequate level of privacy protection in the United States. The Safe Harbor framework and its substantive privacy requirements are discussed in an earlier chapter. The Safe Harbor Principles include rigorous enforcement requirements.[309]

The broad enforcement standards for Safe Harbor participants require mechanisms to assure compliance with the Safe Harbor Principles and to provide recourse for individuals whose data is affected by non-compliance. Privacy seal programs play an important part in meeting these requirements. Complaint mechanisms for individuals must be readily available, affordable, and independent.[310] BBBOnline, for example, offers its members a dispute mechanism sufficient to

---

[305] Available at http://bbbonline.org/privacy/dr.asp.

[306] *Id.*

[307] *Id.* at Part 4.9.2.

[308] See *Federal Trade Commission v. Toysmart.Com,* at http://www.ftc.gov/os/2000/07/toysmartcmp.htm.

[309] "Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations." Department of Commerce, *Safe Harbor Privacy Principles,* at http://www.export.gov/safeharbor/sh_documents.html.

[310] The Safe Harbor documents include a set of *frequently asked questions* about the Principles. FAQ 11 on Dispute Resolution and Enforcement provides additional details about dispute resolution requirements. Available at http://www.export.gov/safeharbor/sh_documents.html.

meet the Safe Harbor requirements.[311] Other possibilities for dispute resolution include compliance with regulatory supervisory authorities that handle complaints and a commitment to cooperate with data protection authorities in the EU.[312]

An additional enforcement method is follow-up procedures for verifying that businesses in the Safe Harbor are complying with their stated privacy practices. This means that a Safe Harbor participant should have internal procedures for periodically conducting compliance reviews for privacy requirements.[313] The procedures might include an audit. An annual statement from the participant verifying completion of a self-assessment should demonstrate compliance.

Remedies and sanctions constitute the third element of Safe Harbor enforcement. Sanctions may include publicity, deletion of data, suspension and removal of a privacy seal, and compensation for individuals. Notice of compliance failures by Safe Harbor participants to government agencies is a required element. The FTC is a central figure in responding to any notice of compliance failure. The FTC committed to reviewing on a priority basis referrals from privacy self-regulatory organizations, such as BBBOnline, and from EU Member States.[314] A referral that alleges non-compliance with the Safe Harbor Principles could lead to a finding that Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. The result could be administrative or judicial action.[315]

Another sanction could be denial of Safe Harbor status. It is not entirely clear, however, who makes the determination when a persistent failure to comply with the requirements means that Safe Harbor status must be withdrawn. The Commerce Department operates the website identifying Safe Harbor participants, and it is supposed to include notices about failure to comply.[316]

Enforcement under the Safe Harbor framework is, in theory, a strong non-statutory procedure. Indeed, sanctions could be more severe than some of the statutory penalties. Denial of Safe Harbor status would mean that a company could no longer import personal data from Europe and that it could lose significant amounts of business. However, the Safe Harbor enforcement methodology is new and untested. It remains to be seen if there will be complaints or whether the complaints will be promptly processed. The Federal Trade Commission rarely pursues individual complaints, and it is unclear what its promise for priority reviews for complaints from foreigners will mean in practice.

---

[311] Available at http://bbbonline.org/intl/index.asp.
[312] Department of Commerce, *Safe Harbor Privacy Principles*, FAQ 11 on Dispute Resolution and Enforcement, at http://www.export.gov/safeharbor/sh_documents.html.
[313] Department of Commerce, *Safe Harbor Privacy Principles,* FAQ 7 on Verification, at http://www.export.gov/safeharbor/sh_documents.html.
[314] Letter from Robert Pitofsky, Chairman, Federal Trade Commission, to John Mogg, Director, DG XV, European Commission (July 14, 2000), at http://www.export.gov/safeharbor/FTCLETTERFINAL.htm.
[315] Department of Commerce, *Safe Harbor Privacy Principles,* FAQ 11 on Dispute Resolution and Enforcement, at http://www.export.gov/safeharbor/sh_documents.html.
[316] *Id.*

3.10 Conclusions

This examination of privacy enforcement mechanisms shows positive and negative features for all options. Privacy torts are more widely available, but the remedy is of uncertain value and applicability to modern information privacy activities. Constitutional litigation is a developing area of the law, but at best it only can offer responses to government privacy invasions. Statutory remedies against the federal government in the Privacy Act of 1974 have been used with some regularity, but it remains uncertain whether the law effectively and appropriately allows aggrieved individuals to recover damages. The evidence suggests that other Privacy Act enforcement mechanisms have had limited effect. Criminal enforcement of privacy laws is rare. The extent to which any of these enforcement elements could or should be enhanced, improved, or more aggressively pursued is an open question. Models for statutory and litigation remedies abound.

Administrative enforcement is still largely unproved. The Department of Education has taken some enforcement actions under the Family Education Rights and Privacy Act (FERPA). The FTC has brought some cases under the COPPA and under its unfair and deceptive practices jurisdiction. It is too soon to offer any assessment of enforcement under Gramm-Leach-Bliley, and the privacy rules for the HIPAA do not take effect until 2003. The Safe Harbor process, which may qualify as a type of administrative enforcement, is also too new to assess. Evidence about private sector enforcement mechanisms, including seals and audits, is limited.

It is difficult to assess any enforcement mechanism without more facts. In order to estimate whether the mechanisms work, it is necessary to have a better sense of the number of problems or complaints that exist (the denominator) and the number of problems or complaints that achieved a fair resolution (the numerator). Even with more information, an evaluation of the results requires some value judgments, and agreements on those judgments may be difficult to achieve. An assessment of litigation needs to examine not only any available statutory or constitutional remedy but also the procedural elements (like certification of class actions) that have a major effect on the utility of the remedy.

Enforcement remains a central issue in privacy. The European Union's emphasis on enforcement makes that clear in an international context, but the issue is also important domestically. Despite the significant degree of uncertainty about privacy enforcement mechanisms, policy makers have a wealth of options from which to choose. The next chapter describes how administrative structures have been used in overseeing privacy policy, enforcement, and other activities.

~~Section 1:~~Section 4: Structures

Formatted: Bullets and Numbering

~~1.14.1~~ The Importance of Structural Responses to Privacy Law and Policy

This chapter describes federal, state, international, and corporate organizational and structural approaches to privacy. More specifically, the chapter addresses the project's statement of work requiring the contractor to "[a]nalyze the possible application of such leading strategies, principles, or models to the U.S. federal government. This shall include an analysis of the implications for (and needed changes to) current laws, policies, and organizational structure."[317] To accomplish these requirements, this chapter addresses "both public and private sector organizations," including organizations "(1) within the United States of America . . . and (2) outside the United States of America."[318]

For purposes of this report, the term *structure* is meant to describe the components or units within an organization and their relationship to other such components in an organization.[319] Factors that can be used to describe structure include:

- Location of a unit within the larger organization;
- Reporting responsibilities of a particular unit in terms of to whom or to what that unit is accountable;
- Number and skills/knowledge of individuals within the unit;
- Actual tasks and responsibilities of the unit and how those tasks and responsibilities relate to the larger organization and other units;
- The manner in which a person is directed to lead or manage a particular unit; and
- Specific guidelines or requirements for which the unit has responsibilities.

This is not a comprehensive list but it does suggest the factors describing organizational structure that the study team reviewed.

---

[317] Commerce Business Daily Solicitation No. OAM-2001-N-0018, *Privacy-Related Research and Analysis & Information Resources Management Services,* (April 23, 2001, Section II).
[318] *Id.*
[319] Fremont E. Kast and James E. Rosensweig, Organization and Management (4th ed. 1985).

Organizational structure is especially important within the present study as it offers significant clues about the way in which a government or other organization perceives the role, responsibilities, and usefulness of a privacy office. A 1989 study of data protection agencies concluded that "[t]he United States carries out data protection differently than other countries, and on the whole does it less well, because of the lack of an oversight agency."[320] Thus, it would be particularly instructive to examine other governments' approaches to structural and operational methods for administering privacy and data protection.

For example, a privacy office with no enforcement or investigational power, or a privacy office that has a small, poorly trained staff, reveals much about the jurisdiction's perception of the privacy function. Changes in society and technology may also provide evidence that previous structures for addressing privacy may be inadequate for new developments. Changes may suggest that privacy should be assigned a higher priority, that better coordination with other organizational or informational activities is needed, or that past substantive policies are insufficient coping with current technologies.

The purpose of this chapter is to identify and describe the manner in which privacy activities are organized and structured in a selection of federal, state, international and corporate agencies. The study team relied on a combination of techniques such as review of traditional academic literature, analysis of relevant legal documents, examination of websites, and interviews with selected experts knowledgeable about privacy in these contexts.

The facts and findings offered here represent a starting point in the study of privacy structure. In some instances, the study team was unable to obtain all relevant structural information, even after consultation of the official government websites, legal sources, and secondary academic materials. In those cases, as much information as was available is provided. Consequently, findings are tentative at best.

Comparisons across the examples provided in this chapter should be made with care, as the contexts in which these structures operate vary considerably. Also, the privacy structures of nations that operate under a parliamentary form of government are considerably different than the type of organization found in the federal government or state governments in the U.S.

The chapter is organized into a discussion of federal, state, international, and corporate structures. The specific federal agencies, states, and nations were selected in light of the study team's knowledge of situations where useful information about privacy structure would most likely be obtained. During interviews, the study team also asked interviewees for ideas and suggestions regarding other agencies, individuals, or contexts that would contribute to the understanding of these issues. These factors, as well as resource constraints, combined to determine the countries, agencies, and states investigated. The chapter concludes with summary comments about organizational structure as it pertains to privacy and data protection.

---

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

~~1.2~~4.2 Federal Structures

Formatted: Bullets and Numbering

The federal structure for privacy protection, regulation, and oversight is a composite approach to privacy issues. There is no central focal point for the coordination, communication, oversight, and enforcement of all federal privacy activities and initiatives. OMB has been given overall responsibility for federal privacy under the Privacy Act of 1974, however, it is up to each agency to implement and comply with federal mandates. OMB sometimes undertakes privacy policy-making as part of its general management activities, but other agencies sometimes have been involved in privacy policy too. Other privacy laws fall under the jurisdiction of other agencies, with the Federal Trade Commission (FTC) being the most important.

This subsection provides a description of the major components within the federal privacy structure, including the FTC's and OMB's roles in privacy, and two examples of privacy offices to provide insight into the variety of privacy functions these offices can serve and the differences between those offices.

~~1.2.1~~4.2.1 Federal Trade Commission

Formatted: Bullets and Numbering

The FTC is an independent U.S. government agency responsible for keeping American business competition free and fair. Its mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive practices and to increase consumer choice by promoting vigorous competition. In that role, the FTC performs several functions in the privacy arena, such as providing advice and recommendations, conducting investigations, and enforcing Federal statutes. The FTC's formal role in privacy dates back to 1970, when it was assigned enforcement responsibility for the first information privacy law, the Fair Credit Reporting Act.

With the growth of the Internet age and e-commerce in the 1990s, the FTC began to devote more resources to addressing the misuse of online personal information. The FTC's Bureau of Consumer Protection staff undertook a Consumer Privacy Initiative, which arose from the April 1995 public workshop on Consumer Protection and the Global Information Infrastructure. The purpose was to examine online consumer privacy and to promote consumer and business education about the use of personal information online.

Since then, the FTC has been studying online privacy issues with a goal to understand the marketplace and its practices, and to assess the impact to businesses and consumers. To further that goal, the Commission held several public workshops, examined Web site information collection and use practices, commented on developments in privacy, such as new technology and industry privacy efforts, and made recommendations to Congress and industry. Actual enforcement actions in privacy matters have been relatively few in number.

~~1.2.1.1~~4.2.1.1 Congressional Testimony and Reports

Formatted: Bullets and Numbering

Over the last six years, the FTC presented Congress with approximately sixteen statements regarding online privacy. This level of effort reflects the strong Congressional interest in privacy. The testimony included self-regulation, children's privacy, identity theft, Internet privacy and fraud, and electronic payment systems. From their workshops, testimony, and research, the FTC released the following reports to Congress on privacy.[321]

1997 – Individual Reference Services – A Report to Congress

This report discusses industry principles to limit the availability of certain types of personal information, summarizes how individual reference services work, provides an overview of the types and sources of personal identifying information, describes the self-regulatory principles including an annual compliance review, and provides recommendations to address other unresolved concerns.

1998 – Privacy Online: A Report to Congress

This report describes the FTC's subset of fair information practice principles, including enforcement as a critical component, presents the results of the online privacy survey of commercial websites, raises concerns about protecting children's privacy and recommends that Congress pass legislation to address those concerns. This report urges industry focus on developing and implementing effective self-regulatory programs.

1999 – Self-regulation and Privacy Online: A Federal Trade Commission Report to Congress

This report assesses the progress made in self-regulation to protect consumers' online privacy since the previous report to Congress, setting out an agenda of Commission actions to encourage industry's full implementation of online privacy protection. The Commission states in the report that legislation to address online privacy was not appropriate at the time.

2000 – Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress

This report presents the results of the FTC's online survey, considers recommendations of the Advisory Committee on Online Access and Security, sets forth the FTC's conclusion that legislation is necessary, and provides a framework for such legislation.

2000 – Online Profiling: A Report to Congress (Part 1 and 2)

---

[321] FTC Online Privacy Reports to Congress are available online, at http://www.ftc.gov/privacy/.

Part one of this report describes the nature of online profiling, consumer privacy concerns about these practices, and the Commission's efforts to address those concerns. Part two of this report provides specific recommendations to Congress, based on FTC's consideration of the industry's self-regulatory proposals and how they interrelate with the Commission's previous views and recommendations on online privacy.

~~1.2.1.2~~4.2.1.2 Advisory Committee on Online Access and Security

Formatted: Bullets and Numbering

In December 1999, the FTC formed the Advisory Committee on Online Access and Security to provide advice and recommendations on the costs and benefits of implementing some fair information practices. In particular, the Advisory Committee was asked to address two issues: 1) providing online consumers reasonable access to personal information collected from and about them on domestic commercial websites, and 2) maintaining adequate security for that information. The Charter directed the Advisory Committee to "consider the parameters of reasonable access to personal information and adequate security and present options for implementation of these information practices in a report to the Commission."[322]

The Committee was a diverse group, comprised of 40 e-commerce experts, security specialists, and consumer and privacy advocates, who met four times in public meetings at the FTC in Washington, DC. The Committee was not required to provide a consensus on definitions and options for legislation, mandatory regulation or self-regulation; nor was its report intended to replace more detailed and industry-specific initiatives in fields regulated by law, such as health care and financial services. Rather, the Advisory Committee was asked to present a range of definitions and options for implementing the Fair Information Practice principles of access and security. Except for security, where all members of the Committee agreed to a clear recommendation, no one definition or option represented a consensus of the members of the Advisory Committee. The Advisory Committee's inability to achieve a consensus on the heart of its agenda is symptomatic of the divergence of views on privacy issues. The Advisory Committee submitted its Final Report to the Commission and was dissolved in May 2000.[323]

~~1.2.1.3~~4.2.1.3 Federal Trade Commission Privacy Agenda

Formatted: Bullets and Numbering

In October 2001, FTC Chairman Muris presented a detailed FTC privacy agenda at the Privacy 2001 Conference. The agenda was developed over four months through meetings with agency, consumer, industry, and trade association officials. The agenda includes a "substantial" increase in the FTC's commitment to protecting consumer privacy, and increases resources devoted to

[322] Charter of the *Federal Trade Commission Advisory Committee on Online Access and Security*, available online, at http://www.ftc.gov/acoas/acoascharter.htm.
[323] Final Report of the *Federal Trade Commission Advisory Committee on Online Access and Security*, (May 15, 2000), at http://www.ftc.gov/acoas/papers/finalreport.htm.

protecting privacy by 50 percent.[324] The new Privacy Agenda contains the following major law enforcement and education initiatives[325]:

- Creating a national do-not-call list;
- Beefing up enforcement against deceptive spam;
- Helping victims of identity theft;
- Putting a stop to pretexting;
- Encouraging accuracy in credit reporting and compliance with the Fair Credit Reporting Act (FCRA);
- Enforcing privacy promises;
- Increasing enforcement and outreach on children's online privacy;
- Tracking consumers' privacy complaints;
- Enforcing the Telemarketing Sales Rule;
- Restricting the use of pre-acquired account information;
- Enforcing the Gramm-Leach-Bliley act (GLB); and
- Holding privacy-related commission workshops.

Regarding possible legislation concerning both Internet and off-line privacy, Chairman Muris said that while there are "clearly good arguments for such legislation," such as the establishment of a clear set of rules about how personal information is collected and used, "it is too soon to conclude that we can fashion workable legislation to accomplish these goals." Citing the recent GLB privacy notices, he said, "we should at least digest this experience," before moving forward.

Muris's statement represented a retreat from the Commission's previous position favoring privacy legislation for the online environment. The privacy agenda includes several items that have been long-standing agenda items for the Commission or express statutory requirements. The Commission's track record for addressing privacy complaints was criticized under the previous Chairman for its inadequacy.[326] The extent to which the new agenda represents a real change is uncertain.

Although the majority of industry representatives and commissioners at the conference praised the stronger enforcement initiative, privacy groups and two fellow commissioners did not agree with the reversal from the Commission's earlier legislative recommendation. Muris's critics believe that "his

---

[324] Remarks of FTC Chairman Timothy J. Muris at the Privacy 2001 Conference, *Protecting Consumers' Privacy: 2002 and Beyond,* Cleveland, Ohio (October 4, 2001).
[325] FTC Press Release, *FTC Chairman Announces Aggressive, Pro-Consumer Privacy Agenda: Privacy Protection Resources to Increase by 50 Percent; Enforcement to be Enhanced,* (October 4, 2001).
[326] See, e.g., *Electronic Privacy Information Center,* at http://www.epic.org/privacy/internet/FTC/default2.html.

refusal to recommend new online privacy laws will only penalize companies that have already embraced the fair privacy practices."[327]

~~1.2.1.4~~4.2.1.4 Federal Trade Commission Enforcement

Formatted: Bullets and Numbering

Under the Federal Trade Commission Act, the FTC has broad authority over entities engaged in or whose business affects commerce, and authority to collect information about those entities. The FTC does not have criminal law enforcement authority, and important industries are exempted from FTC domain, such as banks, savings and loan associations, and common carriers.[328] Additionally, approximately 40 statutes governing specific industries and practices, such as the Truth in Lending Act, the Fair Credit Billing Act, the Gramm-Leach-Bliley Financial Services Act, and the Children's Online Privacy Protection Act, assign a specific role to the FTC. The FTC conducts both public and non-public investigations, which can result from consumer or business letters, Congressional inquiries, or articles on consumer or economic subjects. The FTC has several means for enforcing the statues and laws, ranging from a voluntary consent order to industry-wide rule making.[329]

- A consent order is used to obtain voluntary compliance from a company. A consent order is for settlement purposes only and does not constitute an admission of a law violation. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of $11,000.
- An administrative complaint begins a formal proceeding, where evidence is submitted and testimony is heard. If a law violation is found, a cease and desist order may be issued. The initial decision of the administrative law judge can be appealed to the Commission. Commission decisions can be appealed to the U.S. Court of Appeals. A Commission decision can result in consumer redress, as well as civil penalties or an injunction for violating the order.
- Trade regulation rules can be issued if evidence of unfair or deceptive trade practices is found in an entire industry. When issued, the rules have the force of law. The discussion of enforcement in section 3 of this report addresses other aspects of FTC privacy enforcement activities.

---

[327] Brian Krebs, *FTC Chief's New Privacy Agenda Attacked,* Newsbytes (October 4, 2001), at http://www.newsbytes.com/news/01/170835.html.

[328] Prepared Statement of the Federal Trade Commission, *Self-Regulation and Privacy Online,* Before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, United States House of Representatives, Washington, D.C. (July 13, 1999).

[329] FTC enforcement actions, at http://www.ftc.gov/ftc/action.htm.

4.2.2 Office of Management and Budget Privacy Efforts

In the Privacy Act of 1974[330], Congress assigned OMB with the responsibility to prescribe guidelines and regulations for the use of federal agencies in implementing the Act, and to provide continuing assistance to and oversight of implementation of the Act by agencies. In 1975, OMB issued the Privacy Act Guidelines[331] to implement and aid in administration of the Privacy Act. Figure 4.1 depicts the timeline for all OMB privacy guidance and policy since the Privacy Act.

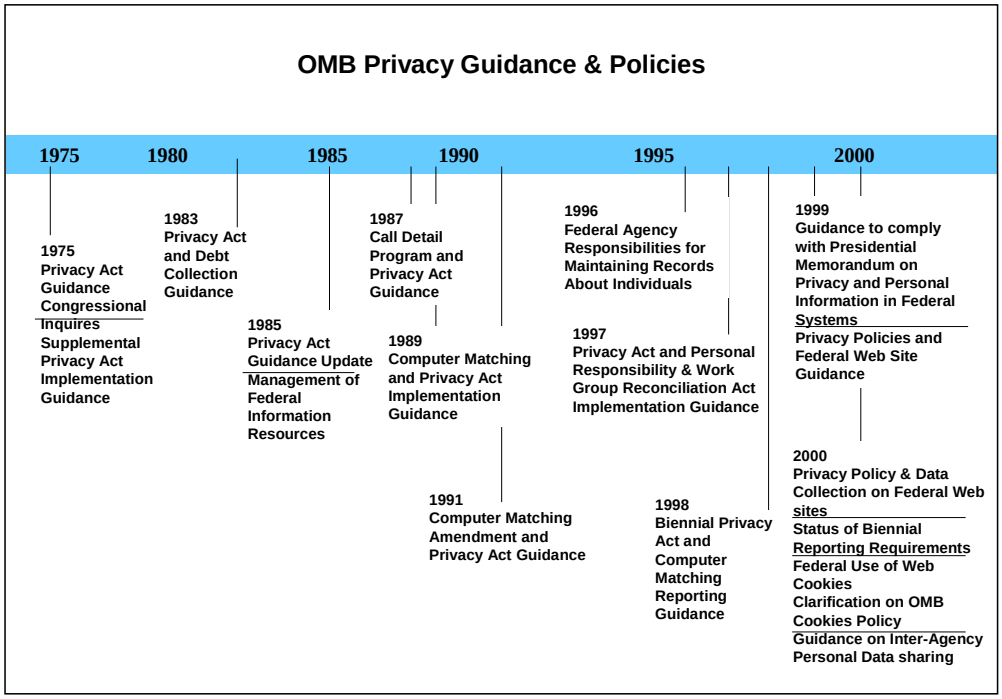


Figure 4.1 Timeline of OMB Privacy Guidance [332]

~~1.2.2.1~~4.2.2.1 Office of Management and Budget Privacy Initiatives

Formatted: Bullets and Numbering

Although OMB was given some overall responsibility under the Privacy Act of 1974, implementation of the policies was left to each agency. OMB was given additional privacy-related responsibilities under other laws, and Presidential Decision Directives and Memoranda, such as the Computer Security Act of 1988, the Paperwork Reduction Act of 1995, the Government Performance Results Act of 1993, and the Privacy and Personal Information in Federal Records Presidential Memorandum of 1998.

---

[330] 5 U.S.C. 552a Privacy Act.
[331] 40 Fed. Reg. 28, 948-78 (1975).
[332] Source of Office Management and Budget Privacy Guidance Listing, at http://www.whitehouse.gov/omb/inforeg/infopoltech.html.

In addition to the original 1975 Privacy Act guidelines, OMB provided supplemental privacy guidance and policy for particular subject areas, such as:

- System of records definition, routine use and intra-agency disclosures, consent and Congressional inquiries, accounting of disclosures, amendment appeals, rights of parents and legal guardians, and relationship to Freedom of Information Act (FOIA);[333]
- Relationship to Debt Collection Act;[334]
- Management of federal information resources;[335]
- Call detail programs;[336]
- Computer matching;[337] and
- Federal agency responsibilities for maintaining records about individuals.[338]

The Office of Information Regulatory Affairs (OIRA) in OMB also undertook other privacy initiatives from time to time, including:

- Coordinating policy across agencies;
- Coordinating with international privacy policies;
- Clearance government and private sector privacy activities; and
- Education visibility.

In the late-1990s, there was renewed emphasis on federal privacy initiatives as the government faced increased privacy concerns on many fronts. The Clinton Administration's desire to develop a National Information Infrastructure (NII) brought a series of politically sensitive issues to the forefront, including copyright protection, security, equal access to government information, and privacy.

The Administration's Information Infrastructure Task Force (IITF) Policy Committee, headed by Sally Katzen of OMB, established a Privacy Working Group to look at privacy issues related to networked computers. In 1995, the Working Group issued "Principles for Providing and Using Personal Information" as a statement on privacy. The Working Group's report was never formally adopted as policy, and it did not become a significant policy document. However, the President

[333] 40 Fed. Reg. 56, 741-43 (1975).
[334] 48 Fed. Reg. 15, 556-60 (1983).
[335] 50 Fed. Reg. 52730 (1985); OMB Circular A-130.
[336] 52 Fed. Reg. 12, 990-93 (1987).
[337] 54 Fed. Reg. 25818-29 (1989).
[338] 56 or 61 Fed. Reg. 6428, 6435-39 (1996).

cited the report on occasion in orders relating to privacy for a discussion of the IITF and the privacy working, see section 2.5.3.

In 1997, President Clinton issued the Critical Infrastructure Protection Presidential Decision Directive (PDD63), which identified thirteen tasks for agency heads. Under task eight, the Privacy Codes of Conduct,[339] the Administration directed OMB to:

- Encourage private industry and privacy advocacy groups to develop and adopt within the next 12 months effective codes of conduct, industry developed rules, and technological solutions to protect privacy on the Internet consistent with the Privacy Principles issued by the Information Infrastructure Task Force (IITF) Privacy Working Group;
- Develop recommendations on the appropriate role of government consistent with "A Framework for Global Electronic Commerce,"[340] and
- Ensure that means are developed to protect the privacy of children.

The Working Group's effort was also mentioned in a Presidential memorandum[341] that directed agencies to designate a senior privacy official and to conduct a review of Privacy Act compliance.

~~1.2.2.2~~4.2.2.2 Chief Counselor for Privacy

Formatted: Bullets and Numbering

In March 1999, as part of the government's effort to coordinate privacy policy across the federal government, the Clinton Administration appointed a Chief Counselor for Privacy in the Office of Management and Budget.[342] This was the first time that OMB ever had a highly visible official dedicated solely to privacy issues. The Chief Counselor for Privacy was to be the point person in privacy coordination efforts.[343] The Chief Counselor for Privacy worked on privacy initiatives[344] including:

- Privacy Awareness - Raising the awareness of privacy issues in general and working with the Administration for an "Electronic Bill of Rights" for individuals.
- Medical Privacy - Development of the Health Insurance Portability and Accountability Act (HIPAA) to ensure that individuals' personal medical information is not released without authorization.

---

339 *Towards Digital e-Quality,* The U.S. Government Working Group on Electronic Commerce, 2nd Annual Report, 1999, page 36.
340 *A Framework for Global Electronic Commerce,* (July 1, 1997), at http://www.iitf.nist.gov/eleccomm/ecomm.htm.
341 Presidential Memorandum for the Heads of Executive Departments and Agencies on Privacy and Personal Information in Federal Records, May 14, 1998.
342 *Id.* page 38.
343 Statement of John T. Spotila, Administrator of the Office of Information and Regulatory Affairs in the Office of Management and Budget, Submitted to the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform, United States House of Representatives. May 15, 2000.
344 Peter Swire, Interview with Peter Swire on October 12, 2001; *[Random-bits] Peter Swire on Clinton administration and privacy protection* (January 22, 2001), at http://lists.essential.org/pipermail/random-bits/2001-January/000497.html.

- Financial Privacy - Development of financial modernization legislation (Graham-Leech-Bliley) and additional proposed legislation to protect the private, personal financial information of consumers.
- Internet Privacy – Development of guidance and policies for federal agency personal data sharing,[345] Internet use,[346] use of cookies online,[347] and use of persistent cookies online.[348]
- Government Privacy
  - Work with the National Electronic Commerce Committee on e-commerce privacy issues at the state and local level.
  - Protection of identity theft and social security numbers.
  - Wiretap and government surveillance.
  - Genetic discrimination in federal hiring or promotion decisions.
  - Government databases and routine use issues.
  - Directions for federal websites to provide their privacy practices along with their budget requests and to make Privacy Impact Assessments (PIAs) part of the development of new government computer systems.
- International Privacy – Development of data protection standards and agreement on the Safe Harbor approach.

Although some thought that the Chief Counselor for Privacy "had done quite a good job in raising privacy as an issue within the White House and the Executive Branch,"[349] concerns remained about the role, resources, independence, and authority of the position. The office had a staff of three to deal with all federal privacy issues, had no enforcement mechanisms, and was part of the Administration and thereby obliged to support any of its privacy initiatives. Still, many viewed the office as useful, and some asked the incoming Bush Administration to continue to position.

Despite the concerns of advocacy organizations and academics expressed in a letter to OMB Director Daniels on April 16, 2001,[350] about the lack of leadership on the privacy issue, the Bush Administration confirmed on the same day that the Chief Counselor for Privacy position would not be filled. Instead, the responsibility for privacy policy and issues in the Bush Administration would be given to OMB and a yet-to-be appointed deputy director of management. That official would work with Bush and Daniels to determine how to staff the administration's privacy operations[351]

---

[345] M-01-05, *Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy* December 20, 2000, at http://www.whitehouse.gov/omb/memoranda/m01-05.html.

[346] M-00-13, *Privacy Policies and Data Collection on Federal Websites* (June 22, 2000) and M-99-18, *Privacy Policies on Federal Websites*, (June 2, 1999).

[347] Letter from Roger Baker to John Spotila on Federal agency use of Web cookies. July 28, 2000.

[348] Letter from John Spotila to Roger Baker, clarification of OMB Cookies Policy. September 5, 2000.

[349] Ari Schwartz, *Give privacy post some clout,* Federal Computer Week (August 21, 2000).

[350] Full copy of the letter , at http://www.cdt.org/privacy/010412omb.shtml.

[351] David McGuire, *Officials: Bush Administration Remains Focused on Privacy* Newsbytes (April 16, 2001), at http://www.fose.com/ind-news/010417075127.html.

and will "work closely with whoever fills the expected position of federal CIO."[352] The decision not to continue the Chief Counselor for Privacy represented a retreat to the more traditional and highly limited privacy role for OMB.

~~1.2.3~~4.2.3 An Example of Privacy Act Agency Office

Formatted: Bullets and Numbering

Some agencies have found it useful to have their own privacy offices. The Department of Defense is perhaps the best example of an office whose principal focus is on implementation of the Privacy Act of 1974. The Defense Privacy Office (DPO) and the Defense Privacy Board (DPB) originated in 1975 shortly after enactment of the Privacy Act. Their mission was to implement the Department of Defense Privacy Program. The DPB has oversight responsibility for implementation of the DoD Privacy Program, while the DPO carries out the day-to-day operations of implementing the DoD Privacy Program. Often, the DPO and DPB are used synonymously because they are so closely linked, although they have different goals and purposes. The DPO and DPB setup is perhaps the most formally structured Privacy Act compliance office anywhere in the federal government.

The DPB has oversight responsibility for implementation of the DoD Privacy Program. The Board has the following three areas of responsibility.[353]

- To ensure that the policies, practices, and procedures of the Program comply with the legal requirements (i.e., Privacy Act and OMB Circular A-130, as well as other pertinent authority), and that DoD components are compliant with the DoD Privacy Program.
- To serve as the primary policy forum for DoD Privacy Program matters, to address issues of common concern and to issue advisory opinions on the DoD Privacy Program so as to promote and ensure uniform and consistent policy among all DoD components, and the application of the corresponding regulations and laws.
- To perform other duties as identified by the Chair or the Board.

The DPO organization is under the direction of the Director of Administration and Management, Office of the Secretary of Defense, who serves as the Senior Privacy Official for DoD. The Director of DPO manages the organization and has four staff to perform the functions of DoD Privacy Program. Currently several of these positions are vacant.

Along with DPO, each individual DoD component (i.e., Army, Navy, and Air Force) administers the DoD privacy program for itself and is advised by DPO on privacy matters. DPO is responsible for providing guidance on how DoD will collect, maintain, use, or disseminate personal information on individuals. DPO is the primary agent for addressing issues of common concern to ensure that uniform and consistent policy is adopted and followed by DoD components. Specifically, DPO performs multiple functions to include:

---

[352] Patrick Thibodeau, *Bush makes key privacy decision: Administration won't appoint privacy czar*, Computerworld (April 16, 2001), at http://www.itworld.com/Man/2688/CWD010416STO59647/.

[353] Defense Privacy Board composition and responsibilities (Enclosure 4, E4.1, at http://www.fas.org/irp/doddir/d5400_11.htm

- Developing policy, providing program oversight, and serving as the focal point for Defense Privacy matters;
- Providing day-to day policy guidance and assistance to DoD components in the implementation and execution of their Privacy Programs;
- Reviewing new and existing DoD policies that impact on the personal privacy of the individual;
- Reviewing, coordinating, and submitting for publication in the Federal Register Privacy Act systems of records notices and Privacy Act rulemaking by DoD components;
- Developing and coordinating Privacy Act computer matching programs among DoD components and between DoD components and other federal and state agencies; and
- Providing administrative and operational support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee.

~~1.2.3.1~~4.2.3.1 Defense Privacy Office Major Policies and Practices

Formatted: Bullets and Numbering

The DPO policies center around the DoD Privacy Program, which is based on the Privacy Act of 1974, as implemented by Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and DoD Directives 5400.11 and DoD 5400.11-R "Department of Defense Privacy Program."[354]

The DPO prepares system notices and supplemental guidance based on OMB guidance to ensure proper implementation of the DoD Privacy Program. The DPO also determines whether a system of record is compliant with privacy issues and coordinates with DoD Chief Information Officer who has responsibility for privacy under the Paperwork Reduction Act.

The DPO is not confined to addressing Privacy Act matters. The Office addresses other related privacy issues to include financial privacy, medical privacy, email privacy, and the use or misuse of social security numbers. Furthermore, the DPO reviews proposed bills and writes opinions for the adoption of the Defense Privacy Board.

Other duties of the DPO Director include membership on the Defense Data Integrity Board and the Defense Privacy Board Legal Committee. The Defense Data Integrity Board is responsible for overseeing and coordinating all computer-matching programs involving personal records contained in systems of records maintained by DoD components. The Defense Privacy Board Legal Committee is responsible for addressing and resolving all legal issues arising out of or incident to the operation of DoD Privacy Program. Neither Board has formally met in years. Both primarily resolve issues via email.

---

[354] DoD Directive 5400.11, dated December 13, 1999, at http://www.dtic.mil/whs/directives/corres/html/540011.htm.

Privacy compliance audits and training are duties that could be handled by DPO. However, privacy compliance audits are undertaken by the Inspector General's office and privacy training is conducted by each DoD component.

The DPO Director believes that strategies to improve upon the implementation of privacy programs across the government could be adopted through updates to OMB guidelines, and that the Privacy Act of 1974 should be updated. Overall, there is a sense that the provisions in the Privacy Act and the guidelines set forth in the DoD Privacy program have managed to strike a balancing between the interests of the individual and the government. The Director stated, "the Privacy Act allows the government to conduct business while protecting individual privacy."

~~1.2.4~~4.2.4 An Example of Agency Office for Non-Privacy Act Privacy Issues

Formatted: Bullets and Numbering

Some agencies face privacy issues that extend beyond the limited confines of the Privacy Act of 1974. The IRS faces complex privacy and technology problems, and it responded with a unique privacy office that does not have responsibility for the Privacy Act of 1974.

In January 1993, the Commissioner of the Internal Revenue Service determined that taxpayers' right to privacy warranted the establishment of an executive position to oversee their privacy interests and to ensure that privacy protection strategies are integrated into all IRS modernization efforts.[355] Originally aligned within the CIO organization, the Office of the Privacy Advocate currently reports to the Chief, Communications and Liaison with the mission "to create, promote, and support privacy programs and privacy awareness Service-wide." While this new organizational alignment fosters the idea that privacy is not just an information technology issue, the optimum placement of this office may still be in question.

The purpose of the Office of the Privacy Advocate is not to manage the routine activities associated with the Privacy Act of 1974. This contrasts sharply with the role of the Defense Privacy Office, which concentrates on Privacy Act matters. At IRS, Privacy Act activities, which require a moderate amount of resources, are managed by Disclosure Offices within the District Offices throughout the country. The Office of Governmental Liaison and Disclosure has responsibility for disclosure oversight and Computer Matching Act compliance. IRS employees and officials have direct responsibilities under the Internal Revenue Manual for familiarity with the Act or for administration of the Act for their own functional areas. The National Director of the Office of Governmental Liaison and Disclosure is responsible for overall coordination of Service efforts to administer the Privacy Act, publication of required notices, preparation of general Internal Revenue Manual instructions, and administration of the access, amendment, and disclosure provisions of the Act. [356]

The IRS Privacy Advocate's role is much broader. The Advocate's goal is to ensure that the IRS integrates privacy strategies into all business processes. The separation of Privacy Act functions

[355] IRS, *Privacy: Working to Build Public Trust,* (Presentation Materials).
[356] Internal Revenue Manual, Part 1, 1.3 Disclosure of Official Information Handbook, Chapter 14 [1.3] 14.7, (08-19-1998).

from the privacy strategy operations allows the Office of the Privacy Advocate to concentrate on developing policy to ensure that IRS programs and projects collect only the taxpayer and employee data necessary to accomplish the Service's business objectives. Working closely with the business owners and system developers, the Office ensures that they build privacy features into all programs and IT systems, and ensures that IRS is at the forefront of preserving taxpayer privacy.

The Office of the Privacy Advocate provides Service-wide training and briefings to enhance privacy awareness at every level. Additionally, it partners with privacy professionals in other government agencies and external organizations to share knowledge, stay abreast of emerging privacy issues and technologies, and provide support and guidance.[357]

~~1.2.4.1~~4.2.4.1 Privacy Impact Assessments

Formatted: Bullets and Numbering

An element of the IRS Privacy Advocate's activities is the Privacy Impact Assessment (PIA). In the President's FY2001 budget, the PIA initiative was announced to make the assessments part of the development of new government computer systems.[358] The PIA is a plan to build privacy protection into new information systems, to work through questions on data needs and data protection prior to the system development. The IRS Privacy Advocate ~~appears to have~~ originated the structure for a PIA and IRS was the author of the PIA document. The CIO Council viewed the IRS's PIA as sufficiently valuable to adopt as a model for the rest of the federal government.[359] The Office of the Privacy Advocate published a technical manual instituting the PIA to ensure that IT systems the IRS develops protect individual privacy. As described in the manual, the PIA incorporates privacy into the development life cycle so that all information technology development initiatives can appropriately consider privacy issues from the earliest stages of design. The process consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by the Privacy Advocate.

A PIA begins in the early stages of the development of a system and is completed as part of the required System Life Cycle reviews. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in the Service.

Both the system owner and system developers must work together to complete the PIA. System owners must address what data is to be used, how the data is to be used, and who will use the data. The PIA forces system developers to address whether the implementation of the owner's requirements presents any threats to privacy.

A PIA is required for new systems, systems under development, and systems undergoing major modifications. The Privacy Advocate has the authority to request that a PIA be completed on any system that may have privacy risks. Legacy systems, as they exist today, do not have to complete a

[357] IRS, *Privacy: Working to Build Public Trust,* (Presentation Materials).
[358] M-01-05, *Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy,* December 20, 2000, at http://www.whitehouse.gov/omb/memoranda/m01-05.html.
[359] Available at http://www.cio.gov/Documents/pia_for_it_irs_model.pdf.

PIA. However, if the automation or upgrading of these systems puts the data at risk, the Privacy Advocate may request a PIA. Similarly, currently operational systems are not required to complete a PIA. However, if privacy is a concern for a system the Privacy Advocate can request that a PIA be completed. If a potential problem is identified concerning a currently operational system, the Service will use best, or all reasonable, efforts to remedy the problem.[360]

~~1.2.5~~4.2.5 Federal Structures Conclusion

Formatted: Bullets and Numbering

As the federal structures research indicates, the federal government has many players with limited privacy roles and no central point for coordination and management of governmental privacy. Congress passes privacy laws, FTC enforces some privacy laws in the commercial arena, OMB provides guidance and regulations to government agencies for the Privacy Act of 1974, and other agencies have defined and typically limited roles for other privacy laws. In addition, some agencies have jumped into and out of the privacy arena over the last two decades. Yet there is no one focal point for management of the various privacy efforts or for privacy policymaking. Additionally, the focus and emphasis on the federal privacy initiatives has fluctuated over the years depending on the particular interests of the Administration in power and the importance of privacy to the public. For many years, privacy received little attention from any federal agency, and it was only with the rise in public concern in the Internet era that government privacy activities increased in volume and importance. The Clinton Administration was the most active on privacy since the Carter Administration.

~~1.2.5.1~~4.2.5.1 *Federal Trade Commission has Limited Privacy Jurisdiction*

Formatted: Bullets and Numbering

Two points are most noteworthy about the FTC's role. First, it does not have jurisdiction over all privacy practices. It has the ability to enforce a few privacy statutes that affect some, but not all, commercial actors. For most commercial websites, the Commission only has the ability to enforce a privacy policy voluntarily adopted by the website. It has not sought to establish affirmative privacy requirements for websites generally or for other record-keepers that fall within the Commission's general jurisdiction but outside the scope of the privacy laws that it administers (i.e., Fair Credit Reporting Act, Children's Online Privacy Protection Act, Gramm-Leach-Bliley). If a website has no stated privacy policy, the FTC's current position is that the Commission cannot enforce any privacy rules or policies against the website unless a statute applies. The Commission's jurisdiction over noncommercial activities is highly limited and may not extend to many activities that affect privacy.

Second, the Commission has many functions with respect to consumer protection. Privacy is only one of those functions. The Commission is not a full time privacy agency and it does not serve the functions that national privacy agencies perform in other countries. Over the years, interest in privacy has waxed and waned at the Commission. The Commission devotes fewer resources to privacy than to some other consumer protection issues.

---

[360] Internal Revenue Service, *Privacy Impact Assessment,* Version 1.3, December 17, 1996 (Technical Manual).

~~1.2.5.2~~4.2.5.2 Office of Management and Budget's Privacy Emphasis Varies

Formatted: Bullets and Numbering

Since the issuance of the Privacy Act in 1974, OMB has provided occasional guidance on privacy related issues. At times, the focus has been on the storage and access to the data, and other times the focus has been on the collection practices and use of the data. OMB typically addresses privacy on a reactive basis to concerns brought to light by legislation, court decisions, agency confusion, or other pressures. However, there have been some brief periods when OMB has been proactive in regard to privacy, most notably through the initiatives of the Chief Counselor for Privacy.

Regardless of the direction of the privacy guidance and enforcement, it is apparent that there is no strategic plan in place for ensuring privacy remains in focus within the federal government. Both the FTC and OMB have alternated on the importance of privacy, at times supporting more federal intervention and other times supporting less federal intervention. The FTC's Congressional reports have oscillated between recommending industry self-regulation to federal legislation for privacy and most recently back to self-regulation. OMB changes its privacy emphasis, at times emphasizing coordination of internal government privacy policy, at other times reacting to legislation, and at other times doing nothing. Except for the early days of the Privacy Act of 1974 and the era of the Chief Counselor for Privacy, OMB's privacy activities have always been at a low level.

~~1.2.5.3~~4.2.5.3 Agency Privacy Offices Fit Their Situations

Formatted: Bullets and Numbering

As seen from the two agency privacy office examples, the mission and functions of these offices can vary greatly depending on whether the privacy focus is strategic to manage overall privacy concerns or operational to manage issues related to a specific privacy statute.

The longevity of DPO suggests that the office plays a useful role in Privacy Act implementation at DoD, although the DPB may no longer be an important component in DoD Privacy Act work. DOD established its privacy structure right after the Privacy Act of 1974 became law, and the formal structure has remained mostly unchanged over the years. In practice, the operations of the Office and the Board evolved as DoD completed the initial work of complying with the Act and the longer-term maintenance and oversight of the law continued. Given the size of DoD, a central office appears to make sense, and the DPO's expertise has been usefully applied in other privacy areas beyond the Privacy Act. However, the Privacy Act of 1974 continues to provide the main reason for DPO's existence. Whether it would be valuable to change or broaden the role of the DPO is an unexplored issue.

It is not clear, however, that DPO is a useful model for other federal agencies. Due to the sheer size of DoD and extent of personal data collected about their personnel, the scope of Privacy Act operations at DoD far exceeds that of any other agency, and other agencies may not need the same degree of oversight and internal coordination as DoD.

Given the size of the IRS and its intensive data processing responsibilities, the separation of Privacy Act functions from the Privacy Advocate's strategic privacy function also appears to make sense. Indeed, the need for separate offices for Privacy Act compliance and for privacy strategy functions

may be a commentary on the Privacy Act itself. Compliance with the Privacy Act only goes so far to protect the privacy of data subjects. IRS found that a higher-level review of business strategies is needed to address privacy effectively. The Privacy Act, drafted long before the era of distributed processing, addresses privacy at the relatively low level of systems of records. Whether that approach is still effective with changes in information technology is an open question. While there have been occasional discussions about how to reform the Privacy Act, no one has reconceptualized privacy at the federal level and offered a new approach that reflects current technology and the changing role of the federal government. Reform or replacement of the Privacy Act has not been on the agenda of the Congress, OMB, or anyone else. The shortcomings of the Act have been well known for decades, but as interest in privacy grew in the last decade, that interest focused, not surprisingly, on dynamic new private sector and Internet activities rather than the stodgy old Privacy Act. The adoption of the IRS's PIA by the CIO Council is another signal that agencies themselves see that additional responses are needed to address privacy at the federal level.

It is impossible to extrapolate from these two examples with any confidence. However, it may be that the federal government faces several different types of privacy problems. The first is the traditional management of personal information. A second relates to the strategic needs of incorporating privacy protections into large new systems, e-government activities, and agency data sharing activities. A third may relate to broader privacy policy-making and oversight for the country at large. The existing Privacy Act of 1974 really only addresses the first of these areas, and the Act may not accomplish its purpose very well any more. The other areas are either unaddressed or have been addressed locally (as at the IRS) or occasionally (as with the Privacy Counselor at OMB).

~~1.2.5.4~~4.2.5.4 Federal Privacy Agency Has Been Proposed

Formatted: Bullets and Numbering

It is difficult to draw conclusions with much breadth or firmness based on the findings about federal structure done for this report. It may be that the more traditional agency narrow focus on the Privacy Act's specific requirements means that larger privacy issues will remain unaddressed. In other words, managing the trees in the Privacy Act's forest is not the same thing as managing the privacy forests. Whether all federal agencies have a big enough privacy forest to warrant higher-level management is an open question. Clearly, some are too small or have too few personal records to be sources of much concern. On the other hand, the increasing emphasis on e-government may mean that privacy issues will arise in unexpected places.

The Privacy Act of 1974 is sometimes called a first-generation privacy law, enacted in response to planned or envisioned national data banks and concentrating more narrowly on the functions of data processing. Second-generation privacy laws in Europe began the establishment or enhancement of data-protection institutions with broader roles.[361] The Privacy Act, for the most part, has remained at the first-generation level throughout its entire 25-plus years. The Computer Matching and Privacy Protection Amendments of 1988 added a requirement for agency Data Integrity Boards (DIBs) to oversee computer-matching activities. This might be seen as a step

[361] Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe,* Technology and Privacy: The New Landscape, 218-241 (Philip E. Agre & Marc Rotenberg eds., 1997).

toward that second generation, but the evidence suggests that DIBs took a very narrow role and has had little influence.

The establishment of the IRS Privacy Advocate with its broader privacy role may be seen as recognition by the IRS of the need for a generational expansion of its privacy focus well beyond the confines of the Privacy Act. By contrast, the DoD office remains a first generation attempt to address privacy. While is not intended as a criticism of the DoD office, it is the IRS office that is most interesting and may provide a more current model for privacy activities at other agencies. The development of the IRS privacy office in response to perceive internal needs (as well as some external political pressure) appear, at least tentatively, as a significant development as information technologies extend throughout government.

Additionally, because privacy and its protection are subject to the inclinations of a political agenda, it is easy for the emphasis to grow or die. Thus the development of privacy protection can have a tendency to move "one step forward, two steps back." Privacy and the protection of personal information in the federal structure is an issue that will not go away, especially with the proliferation of e-government. National privacy concerns and privacy practices might be better served if given more emphasis, appropriate resources, and more integration into federal Internet activities.

Based on the research, it is difficult to draw firmer conclusions. A federal privacy structure has been a constant, if low level, idea for several decades. Sidebar 4.1 offers a brief history of proposals for a federal privacy agency. Politically, the notion of a federal privacy agency has never captured enough interest to receive serious consideration. Whether a federal agency would improve agency and private sector privacy activities is an open question not receiving much attention today. The establishment of national privacy agencies in nearly every other country that has addressed privacy suggests that most of the rest of the world sees such an office as valuable. Whether lessons learned abroad have relevance to the United States may warrant more debate.

Management of federal agency privacy programs has not attracted much public or political interest. While it is not surprising that internal agency management matters are of little general interest, it may be that there is much room for development and improvement at the agency level. IRS is not the only agency that has established an internal privacy structure in recent years, and more study of internally generated privacy structures at IRS and other agencies may be fruitful.

Sidebar 4.1: History of proposals for a federal privacy agency

No federal agency dedicated to privacy has ever existed in the United States. Proposals for a privacy agency have been offered from time to time over the past 25 years.[362] The proposals have never attracted a critical mass of support, but the idea of a privacy agency reemerges repeatedly. Because of the importance of privacy agencies to international data protection activities – all or nearly all countries with national data protection laws have dedicated privacy offices – a brief review of the history of the idea of a federal privacy agency is relevant.

On two different occasions, Congress voted on proposals to establish a permanent privacy agency. In the 93rd Congress when the bill that later became the Privacy Act of 1974 was under consideration, the Senate approved a proposal for the establishment of a Privacy Protection Commission as a permanent agency. The Commission's jurisdiction would have extended primarily to federal government records, with limited authority to consider state and private sector record keeping.[363] An amendment offered on the floor of the House to establish a privacy commission failed on a voice vote.[364] The two Houses compromised by establishing the Privacy Protection Study Commission as a temporary study commission.

In 1994, during debate over the Consumer Reporting Reform Act of 1994,[365] Senator Paul Simon offered an amendment to establish a permanent Privacy Protection Commission. The Commission would have had no regulatory powers. Its role was to provide leadership on federal, state, and private sector privacy matters. The Senate defeated the proposal on a procedural vote.[366]

Members of Congress introduced bills to create a privacy commission from time to time, however none saw any formal activity.[367] A bill to establish a temporary study commission received serious consideration in the House in 2000.[368] It received a majority vote, but failed passage for lack of a supermajority required under the procedure used to bring it to a vote.[369]

Administrative ideas for a privacy commission date back to Richard Nixon. In 1974, Nixon established a Domestic Council Committee on the Right of Privacy. The first chair was Vice President Gerald Ford, and Vice President Nelson Rockefeller took over as chair later. The Committee's report on *National Information Policy*[370] broadly addressed the policies that govern the way that information affects society. The report found that executive and legislative responses to

[362] Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions,* 6 Software Law Journal 199 (1993).
[363] S.3418, 93rd Congress, §522(a) (1974).
[364] 120 Congressional Record 36,956 (1974), see also House Committee on Government Operations, *Privacy Act of 1974*, H.R. Rep. No. 1416, 93rd Congress at 38-9 (1974) (additional views of ten members favoring an agency).
[365] S.783, 103rd Congress.
[366] 140 Congressional Record S5133 (May 4, 1994).
[367] See, e.g., H.R. 285, 95th Congress (1977); H.R. 3743, 98th Congress (1983); H.R. 3669, 101st Congress (1989).
[368] H.R. 4049, 106th Congress (2000).
[369] Available at http://thomas.loc.gov/cgi-bin/query/R?r106:FLD001:H58562.
[370] Domestic Council Committee on the Right of Privacy, *National Information Policy: Report to the President of the United States,* (1976).

information policy problems were ad hoc and piecemeal. The report recommended the establishment of a permanent policy organization within the Executive Office of the President to address national information policy, including privacy.

The Commission on federal paperwork was a temporary study commission that operated from 1975 to 1977. Its wide-ranging recommendations included creation of a new federal agency to centralize and coordinate information management functions within the executive branch, including privacy.[371] The proposal had some similarities to the recommendations of the Nixon Administration's Domestic Council Committee.

The Privacy Protection Study Commission, established under the Privacy Act of 1974, supported the creation of a permanent privacy agency. The Commission's first recommendation was to establish an independent Federal Privacy Board to function principally as an oversight, research, and advisory organization.[372]

From time to time, federal agencies have taken on and then abandoned significant privacy roles. Starting in the Carter Administration and continuing into the Reagan Administration, the National Telecommunications and Information Administration (NTIA) was a lead agency for some privacy functions. NTIA reemerged in the privacy arena for a time during the Clinton Administration as well. The Bureau of International Communications and Information Policy in the State Department engaged in some international privacy activities during the late 1970s and early 1980s. The U.S. Office of Consumer Affairs showed interest in privacy starting in 1989 that continued for a few years until the Office was abolished in 1998. The Office of Management and Budget and the Federal Trade Commission have had more continuing roles, but interest in privacy at both agencies has waxed and waned over the years. Recent legislation increased the FTC's privacy regulatory functions.

During the Clinton Administration, the Information Infrastructure Task Force, a cabinet level group chaired by the Secretary of Commerce, reexamined the idea of a privacy agency. A paper prepared by the Information Policy Committee of the IITF outlined options for promoting privacy. The purpose of the paper was to find the "best mechanism to implement fair information practices that balances the needs of government, commerce, and individuals, keeping in mind both our interest in the free flow of information and in the protection of information privacy."[373] The report set out three options for a privacy agency: 1) a government agency with regulatory powers; 2) a government agency without regulatory powers; and 3) a non-governmental or advisory organization.

---

[371] Commission on Federal Paperwork, *Confidentiality and Privacy,* (1977).
[372] Privacy Protection Study Commission, *Personal Privacy in an Information Society,* 37 (1997).
[373] National Information Infrastructure Task Force, Information Policy Committee, *Options for Promoting Privacy on the National Information Infrastructure,* (1997), at http://iitf.doc.gov/ipc/privacy.html.

In the summer of 1998, Vice President Al Gore recommended increasing the role of OMB in privacy coordination.[374] This led to the establishment of a Chief Privacy Counselor at OMB in early 1999. The office of the Chief Privacy Counselor continued until the end of the Clinton Administration, but the position was not continued by the new administration. A brief description of the Chief Privacy Counselor's functions can be found elsewhere in the report.

[374] Available at http://privacy2000.org/archives/VPOTUS_7-31-98_vp_announces_electronic_bill_of_rights.htm.

4.3 State Structures

The approaches to privacy protection, regulation, and oversight among the state governments are as varied as the states themselves. Some states have complex systems for protecting the personal and data privacy of the citizenry of the state, while others offer little or no protection in these areas. Some have tried different approaches to an information privacy office, while at least one has even abandoned its attempt completely after establishing an information privacy office.

These offices work in a wide range of related areas, including, though not limited to, open records, open meetings, freedom of information, protection of personal privacy, data protection, consumer protection, sunshine laws, and identity theft investigations. The states analyzed in this section were selected to provide insight into the variety of functions these offices can serve and the similarly wide range of activities in which the offices can engage. They display the wide array of state approaches to privacy offices, from the complex structure of Hawaii's Office of Information Practices to the entirely abandoned Office of the Privacy Advocate in Wisconsin. The roles of the agencies also vary greatly, ranging from acting as an ombudsman to acting as a referral service to issuing legally binding orders.

In conducting research into the variety of approaches that selected states have taken with privacy issues, the study team employed a number of methods to understand the relevant governmental structures. This included: analyzing the relevant statutory and constitutional provisions, with an emphasis on the offices' enabling laws; engaging in scripted interviews (Appendix C) with key individuals knowledgeable about the background and operations of a particular state office; and conducting a thorough review of the website of each state's privacy office (or related office, as appropriate). For the sake of gathering as much information as possible while minimizing the risk to any of the individuals consulted, personal identities have been kept confidential, and no insights or information gained and used is attributed to them. The following subsections provide a case-by-case review of selected states.

4.3.1 California

Section 1 of Article I (Declaration of Rights) of the California Constitution provides the following "inalienable rights" to the people of California: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursing and obtaining safety, happiness, and privacy."[375]

By creating the Office of Privacy Protection (the Office) in its 2000 session,[376] the California Legislature has begun to institutionalize certain privacy protections and assistance in both the public agency and the consumer arenas. That Office has recently become operational,[377] receiving funding in July 2001, and was staffed in September 2001.

---

[375] Cal. Const. at I, § 1.
[376] 2000 Cal. Stat. 984, § 1, codified as amended at Cal. Business and Prof. Code § 350 (Deering 2001).
[377] Available at http://www.privacyprotection.ca.gov.

Situated within the California Department of Consumer Affairs,[378] the Office is similar in many respects to any bureau within the state agency hierarchy of the executive branch. The Office is headed by a Chief (a "career executive" position) who reports to the Director of the Department of Consumer Affairs, who in turn reports to the Secretary of State and Consumer Services Agency, who reports to the Governor. The Office has a staff of 7.5 full-time equivalent positions and an annual budget of $1,300,000 for 2001. Beginning in January 2003, the Office will issue annual reports to the Legislature.[379] However, the first report to the Legislature will be in April 2002, when budget hearings begin.

The legislation creating the new Office of Privacy Protection also requires each state agency to "maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977 ... that includes, but is not limited to, the following principles":

a) Personally identifiable information is only obtained through lawful means;

b) The purposes for which personally identifiable data are collected are specified at or prior to the time of collection, and any subsequent use is limited to the fulfillment of purposes not inconsistent with those purposes previously specified;

c) Personal data shall not be disclosed, made available, or otherwise used for purposes other than those specified, except with the consent of the subject of the data, or as authorized by law or regulation;

d) Personal data collected must be relevant to the purpose for which it is collected;

e) The general means by which personal data is protected against loss, unauthorized access, use, modification or disclosure shall be posted, unless such disclosure of general means would compromise legitimate state department or state agency objectives or law enforcement purposes; and

f) Each state department or state agency shall designate a position within the department or agency, the duties of which shall include, but not be limited to, responsibility for the privacy policy within that department or agency.[380]

While the Information Practices Act contains California's original and more detailed codification of its FIPs, the foregoing privacy policy statute is an important updating of the state's concerns in this area, and is all the more significant because it arose in conjunction with the state's recent regulatory efforts to establish the Office of Privacy Protection. California law also requires each state agency that electronically processes personal data to display a comprehensive privacy notice on its website.[381]

---

[378] The Department of Consumer Affairs' website, at http://www.dca.ca.gov.
[379] Cal. Bus. and Prof. Code § 351 (Deering 2001).
[380] 2000 Cal. Stat. 984, § 2, codified at Cal. Gov. Code § 11019.9 (Deering 2001).
[381] Cal. Gov. Code § 11015.5 (Deering 2001).

By statute, the Office has been charged with: "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices in adherence with the Information Practices Act of 1977...."[382] In carrying out this charge, it focuses both internally on the information practices of government agencies, and externally on consumers' issues and complaints. Its activities, responsibilities, and powers include:

- Educating the public of their rights and options;[383]
- Making privacy recommendations to organizations to promote and protect the interests of consumers;[384]
- Promoting voluntary nonbinding arbitration and mediation of privacy-related disputes;[385]
- Receiving complaints and providing advice, information, and referral;[386]
- Assisting in the investigation and prosecution of crimes such as identity theft;[387] and
- Facilitating the training of state and local law enforcement agencies.[388]

A key element of the legislation creating the Office of Privacy Protection was the intent to create a governmental unit focused on protecting the rights granted under the Information Practices Act of 1977.[389] The Office does not yet have any operational experience to report, but its structural features and focus are clear: It is an office within a consumer protection agency, concerned primarily with consumer empowerment and assistance in all privacy-related matters, while also very much involved in privacy policy analysis, development and recommendations in the public and private sectors.

4.3.2 Connecticut

Unlike states such as California and Connecticut does not have an explicit constitutional provision regarding privacy. Instead, it has provisions protecting certain aspects of an individual's privacy, such as guaranteeing freedom from unwarranted arrests, detention, or punishment ("Right of personal liberty"),[390] similar to the approach taken in the U.S. Constitution.

The State of Connecticut does not have a unit that focuses on privacy per se; rather, the organization with partial operational relevance to privacy-related issues is the Freedom of

---

[382] Cal. Bus. and Prof. Code § 350(a) (Deering 2001).
[383] *Id.* § 350(b), (e)(2), (e)(3).
[384] *Id.* § 350(c).
[385] *Id.* § 350(d).
[386] *Id.* § 350(e)(1), (e)(2).
[387] *Id.* § 350(e)(4).
[388] *Id.* § 350(e)(5).
[389] 1977 Cal. Stat. 709, § 1, codified as amended at Cal. Civ. Code §§ 1798-1798.76 (2001).
[390] Conn. Const. at I, § 9.

Information Commission (the Commission or FOI Commission).[391] It was officially constituted under Connecticut's Freedom of Information Act[392] (FOI Act) on July 1, 1975, three months before the substantive rights conferred by that act (providing the public with rights of access to records and meetings of public agencies) became effective. The Commission's primary mission revolves around overseeing compliance with the FOI Act.[393] Among other provisions, the act requires the Commission to "conduct training sessions, at least annually, for members of public agencies for the purpose of educating such members as to the requirements of" relevant statutes.[394] An example of its educational mission is a 16-hour technical training program that includes privacy protection and is being pilot tested for all levels of government. This program was developed as a result of a recent survey conducted by the Commission.

The FOI Commission is an independent government oversight body. It has five members, all of whom are appointed by the Governor, with no more than three from the same political party.[395] The individual who serves as Executive Director and General Counsel administers the Commission. The Executive Director is appointed by the Commission but does not serve at its pleasure; rather, he or she can only be terminated for just cause. Presently, the FOI Commission office has sixteen employees and a published budget of $1,300,000 for 2001.

In the context of alleged violations of the FOI Act, the Commission can issue orders, hold hearings, conduct investigations, issue subpoenas, petition for judicial review, and issue any remedy it deems appropriate.[396] The FOI Commission administers and enforces the provisions of the Connecticut Freedom of Information Act, hearing complaints from persons who have been denied access to the records or meetings of public agencies in Connecticut. Any person denied the right to inspect a record, to get a copy of a public record, or to gain access to a meeting of a public agency may file a complaint against the public agency. The FOI Commission will conduct a hearing, and the Commission can order the disclosure of public records, void a decision reached during a public meeting, or impose other appropriate relief.[397]

---

[391] The Connecticut FOI Commission website, at http://www.state.ct.us/foi.

[392] Codified as amended at Conn. Gen Stat. ch.14, §§ 1-200 to 1-241 (2001), at http://www.state.ct.us/foi/2001FOIA/2001FOIAStatutoryIndex.htm. The Commission was established and is enabled by section 1-205. The regulations governing Commission activities, Conn. Agencies Regs. §§ 1-21j-1 to 1-21j-57, at http://www.state.ct.us/foi/Regs/regsIndex.htm. The exemptions in the FOI Act are superseded by federal law or other state statutes. There are approximately 20 exemptions listed in section 1-210(b), but hundreds of exemptions can be found throughout the Connecticut statutes.

[393] Conn. Gen Stat. ch.14, § 1-205(d) (2001).

[394] *Id.* § 1-205(e).

[395] *See* Mitchell W. Pearlman, *Freedom of Information Commission: Commissioners and Staff: July 1975 – July 2000,* (2000), at http://www.state.ct.us/foi/FOIC_Commissioners/FOIC_Commissioners.htm, for a history and review of the Commission and its Commissioners (Pearlman is Executive Director of the Commission).

[396] Conn. Gen Stat. ch.14, § 1-205(d) (2001).

[397] *Id.* § 1-206(b)(2).

When an individual files a privacy-related complaint in the context of the FOI Act, the Commission and its staff generally handle the complaint as follows.[398] Generally, an appeal of an agency action must be filed with the Commission within 30 days of the violation alleged by a complainant. If an appeal concerns a request for records contained in a public employee's personnel file, medical file or similar file, the Commission requires the agency in question to notify the subject employee(s) of the appeal and who may intervene as a party to the appeal. The Commission staff is available to assist complainants with procedural questions. The staff may refer individuals to specific sections of the law and cases interpreting the law, but only the Commission, not its staff, has the power to interpret and apply the law.

A FOI Commission staff member is assigned as an ombudsman in each appeal, acting as liaison between the parties. That staff member will attempt to effect a settlement, and the hearing officer may do so as well on the date assigned for hearing. If a settlement does not occur, the matter will proceed to a hearing. A member of the FOI Commission or a staff member presides over the hearing, which is an official proceeding conducted as a contested case under Chapter 54 of the Connecticut General Statutes and the Regulations of the Commission. A staff attorney, who answers procedural questions, usually assists the Hearing Officer. After the hearing is concluded, the Hearing Officer prepares a report for the full Commission's consideration, consisting of findings of fact, conclusions of law, and a recommended order. Before becoming a final decision, the Hearing Officer's Report is considered by the FOI Commission, which may approve the report as is, approve it with amendments, or reject it completely. Orders of the Commission may be appealed to the Connecticut Superior Court, which would sit as an appellate court in review of the Commission's order and record.

The Commission and its staff routinely interact with other elements of the Connecticut government. The Commission is typically consulted by the General Assembly on relevant legislation, and it will affirmatively present an opinion on other relevant legislation when not consulted.

Other recent efforts in Connecticut involving privacy issues include a survey of state agency FOI practices underway by the Legislative Program Review and Investigations Committee of the Connecticut General Assembly. An interim staff briefing has been made publicly available, stating that agencies are successfully implementing and enforcing FOI regulations. In addition, the FOI Commission Executive Director chairs a Government Information Policy Advisory Committee, which is seeking to develop a FOI policy for all state agencies. A draft with FIP elements is currently being discussed with agencies and the Advisory Committee is seeking their input. Lastly, the FOI Commission undertakes a "horizon project" each year, looking at issues on the horizon, including privacy, which are investigated and reported upon annually.

The Connecticut approach to administering privacy-related issues has occurred strictly in the context of its FOI Act and the associated Commission set up to oversee compliance. Thus, unless an

[398] This information is summarized from *A Citizen's Guide to the Freedom of Information Commission* (1998), at http://www.state.ct.us/foi/1998CITIZENSGUIDE.htm.

allegation involving access to public records and meetings—or the denial thereof—triggers privacy considerations, privacy is not the focus of government enforcement activity. The state does have a statute explicitly concerned with informational privacy: the Personal Data Act.[399] However, in the absence of an enforcement agency, office, or commission (as exists with the FOI Act), there has been little activity in this area and none on a systematic basis by the State of Connecticut. Accordingly, the difference in the approaches taken with two highly related laws in the same state is particularly revealing of the potential impact of having an enforcement structure, versus having none at all.

4.3.3 Florida

Florida is currently in the process of establishing and implementing an office to oversee privacy concerns within the state. On June 15, 2001, the Governor approved an act relating to information technology, which is the first statute in Florida to contemplate a state office dedicated to privacy concerns.[400] This act gave the Chief Information Officer the power to designate a State Chief Privacy Officer.[401]

The State of Florida provides an explicit individual right to privacy in its Constitution: "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."[402] However, reflecting the state's history of government-in-the-sunshine, that section of the Constitution further provides: "This section shall not be construed to limit the public's right of access to public records and meetings as provided by law."[403]

The State Chief Privacy Officer will be responsible for the continual review of policies, laws, rules, and practices of state agencies that may affect the privacy concerns of state residents.[404] The State Chief Privacy Officer has not yet been appointed as of late 2001, and it does not appear the Office is active yet in any sense. Once established, the CPO will report to the CIO, who is the agency head of the State Technology Office within the Department of Management Services. The Department of Management Services will provide administrative support and service to the office to the extent requested by the CIO.

---

[399] 1976 Conn. Acts 421, codified as amended at Conn. Gen. Stat. §§ 4-190 to 4-197 (2001). "Personal data" is defined in the statute as "any information about a person's education, finances, medical or emotional condition or history, employment or business history, family or personal relationships, reputation or character which because of name, identifying number, mark or description can be readily associated with a particular person." Conn. Gen. Stat. § 4-190(9).

[400] Chapter 2001-261, *Laws of Florida,* at http://www.leg.state.fl.us/data/session/2001/House/bills/billtext/pdf/h1811er.pdf

[401] An amendment to Fla. Stat. 282.102 (2001), section 11 of that act created a new subsection 282.102(30), which establishes the State Chief Privacy Officer.

[402] Fla. Const. at. I, § 23.

[403] *Id.*

[404] Fla. Stat. 282.102(30) (2001).

The Task Force on Privacy and Technology was created in 2000[405] as a temporary organization to study and make policy recommendations on issues such as identity fraud and the collection, use, and sale of personally identifiable information by the government. Recommendations were submitted to the Governor and Legislature, and many of the recommendations appeared as bills during the 2001 Legislative Session.[406]

As Florida is still in the earliest stages of developing the position of CPO, it is difficult to draw inferences about the role the Office, the range of issues the Office may address, or the extent of the Office's power. The creation of the Task Force in 2000 and the CPO in 2001 demonstrates that privacy is considered an important issue in the State of Florida.

4.3.4 Hawaii

The Hawaii Constitution provides that: "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."[407]

Unique within the United States, Hawaii has adopted laws that combine many aspects of concern with government information: namely, FOI and FIPs. In 1988 Hawaii adopted the Uniform Information Practices Act (Modified) (UIPA),[408] which among other provisions, created the Office of Information Practices (OIP)[409] and set forth its powers and duties. OIP is also responsible for overseeing Hawaii's "Sunshine Law."[410] Part III of UIPA embodies Hawaii's FIPs,[411] but FIPs are otherwise embedded throughout the UIPA.[412]

The Governor appoints the OIP Director for the Governor's term. The Director is the chief executive officer of OIP. OIP reports to the Governor and the Legislature, and is an independent office not part of the Cabinet. The law refers to OIP as "a temporary office ... for a special purpose," but OIP has operated continuously since 1988 and is ongoing in nature.

The office is administratively situated within the Lieutenant Governor's Office.[413] Though it is an independent office within that structure, it is less independent than might otherwise be the case because the Director is a political appointee. The Director is empowered to employ all necessary

---

[405] 2000 Fla. Laws ch. 164, s. 22, codified at Fla. Stat. § 282.3095 (2001).

[406] The reports of the State Technology Office Privacy and Technology Task Force, at http://www.myflorida.com/myflorida/government/taskandcommissions/pttf/.

[407] Haw. Const. *at* I, § 6.

[408] 1988 Haw. Sess. Laws 262. Hawaii's UIPA is based on the Uniform Information Practices Code, which was promulgated by the National Conference of Commissioners on Uniform State Laws in 1980. 13 U.L.A. 277 (1986). No other state has ever adopted that uniform law. *Id.* at 112 (Supp. 2001).

[409] OIP website, at http://www.state.hi.us/oip.

[410] Haw. Rev. Stat. ch 92, pt. 1 (2000), at http://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch046-115/hrs092/.

[411] Hawaii Rev. Stat. §§ 92F-21 to -28 (2000).

[412] Available at http://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch046-115/hrs092f/.

[413] Haw. Rev. Stat. ch. 92F-41 (2000), at http://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch046-115/hrs092f/HRS_92F-41.htm.

personal for OIP to fulfill its functions. In 2001, the office had 6.5 full-time equivalent staff positions, with a budget of approximately $700,000.

The Office is in charge of monitoring and enforcing privacy, information practices, and government openness (the "Sunshine Law"). The OIP Director administers Part I of the Sunshine Law, and "shall establish procedures for filing and responding to complaints filed by any person concerning the failure of any board to comply with this part."[414]

OIP investigates complaints regarding granting or denial of access to records, and it may recommend disciplinary action to an agency's department head. OIP's annual report includes compiled summaries of disciplinary recommendations. Most privacy violations have been found to be inadvertent, and thus the recommendations tend to focus on training, education, and structural changes.

Upon request, OIP must "review and rule on an agency denial of access to information or records, or an agency's granting of access..."[415] It also:

- May conduct inquiries regarding compliance by an agency and investigate possible violations by any agency;[416]
- May examine the records of any agency for the purpose of paragraph (4) and seek to enforce that power in the courts of this State;[417]
- May recommend disciplinary action to appropriate officers of an agency;[418] and
- Shall receive complaints from and actively solicit the comments of the public regarding the implementation of this chapter.[419]

Additionally, the OIP Director:

- Upon request by an agency, shall provide and make public advisory guidelines, opinions, or other information concerning that agency's functions and responsibilities;[420]
- Upon request by any person, may provide advisory opinions or other information regarding that person's rights and the functions and responsibilities of agencies under this chapter;[421]
- Shall review the official acts, records, policies, and procedures of each agency;[422]

---

[414] Haw. Rev. Stat. § 92-1.5 (2000), at http://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch046-115/hrs092/HRS_92-1_5.htm.
[415] *Id* § 92F-42(1) (2000), at http://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch046-115/hrs092f/.
[416] *Id.*§ 92F-42(4).
[417] *Id* § 92F-42(5).
[418] *Id.*§ 92F-42(6).
[419] *Id.*§ 92F-42(8).
[420] *Id.*§ 92F-42(2).
[421] *Id.*§ 92F-42(3).

- Shall assist agencies in complying with the provisions of this chapter;[423] and
- Shall inform the public of the following rights of an individual and the procedures for exercising them:
  - The right of access to records pertaining to the individual;
  - The right to obtain a copy of records pertaining to the individual;
  - The right to know the purposes for which records pertaining to the individual are kept;
  - The right to be informed of the uses and disclosures of records pertaining to the individual;
  - The right to correct or amend records pertaining to the individual; and
  - The individual's right to place a statement in a record pertaining to that individual.[424]

Another statutory provision requires plaintiffs "filing a civil action that is under, related to, or is affected by [the UIPA to] notify the [OIP] in writing at the time of the filing."[425] This statute provides a mechanism by which the office may monitor issues in litigation, and intervene when deemed appropriate.

The Hawaiian approach combines several information initiatives in one statutory scheme: FOI, Government-in-the-Sunshine, and FIPs. The cost of compliance has been kept down because OIP readily resolves disputes through mediation and a reliance on its body of published formal opinions (now numbering 225).

OIP provides regular, formal input to the Legislature and the Governor in its statutory annual reports,[426] which are made available to the public along with other publications.[427] It also provides input on relevant issues and legislation before the Legislature. The Office also offers training, advice, and policy recommendations for other state agencies.

In 2000, the Hawaii Legislature required the creation of a Medical Privacy Task Force to study the history of privacy of health care legislation in Hawaii, and to make findings and recommendations regarding legislation on information practices in the health care industry.[428] The task force study was released in "The Report of the Medical Privacy Task Force to the State of Hawaii 2001

---

[422] *Id.*§ 92F-42(9).
[423] *Id.*§ 92F-42(10).
[424] *Id.*§ 92F-42(11).
[425] *Id.* at § 92F-15.3.
[426] Section 92-1.5, Haw. Rev. Stat. (2000) requires OIP Director to "submit an annual report of [Sunshine Law] complaints along with final resolution of complaints, and other statistical data to the legislature." Available at http://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch046-115/hrs092/HRS_92-1_5.htm. Section 92F-42(7), Haw. Rev. Stat. (2000) requires OIP Director to "report annually to the governor and the state legislature on the activities and findings of the office of information practices, including recommendations for legislative changes." Available at http://www.capitol.hawaii.gov/hrscurrent/Vol02_Ch046-115/hrs092f/HRS_92F-42.htm.
[427] Available at http://www.state.hi.us/oip/annual.htm.
[428] 2000 Haw. Sess. Laws 140.

Legislature."[429] At the request of the Hawaii Legislature, OIP conducted a study on "The Commercial Use of Personal Information" in 1999.[430]

Hawaii's approach reflects a strong and very active investigatory office within the executive branch. By focusing on multiple aspects of privacy—including enforcement—within one statutory scheme, it presents a compelling case for how an American jurisdiction has comprehensively addressed privacy concerns.

4.3.5 Minnesota

The Minnesota state office that addresses privacy issues most directly—at least in the context of governmental data practices generally—is the Information Policy Analysis Division[431] (IPAD) within the Department of Administration. With seven staff members, this office is headed by a Director, who reports to the Commissioner of Administration, who in turn reports to the Governor. The Commissioner of Administration has various legal responsibilities under data practices, records management, and other information policy laws, and IPAD assists the Commissioner in the performance of these duties.

There is no language in the state constitution that addresses privacy responsibilities. The Minnesota Government Data Practices Act[432] (MGDPA) is the key statute relevant to data protection in Minnesota, with other pertinent statutes arising in various substantive areas. The act "regulates the collection, creation, storage, maintenance, dissemination, and access to government data in state agencies, statewide systems, and political subdivisions."[433] The term "government data" includes "all data collected, created, received, maintained or disseminated ... regardless of its physical form, storage media or conditions of use."[434]

The MGDPA "establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is federal law, a state statute, or a temporary classification of data that provides that certain data are not public."[435] The statute implements this presumption by specifying:

- What information can be collected;
- Who may see or have copies of the information;
- The classification of specific types of government data;
- The duties of government personnel in administering the provisions of the Act;

[429] Available at http://www.state.hi.us/oip/medical_privacy_task_force_report.htm.
[430] Available at http://www.state.hi.us/oip/privacy_study_home_page.htm.
[431] The Division website, at http://www.ipad.state.mn.us.
[432] Minn. Stat. §§ 13.01-13.99 (2001), at http://www.revisor.leg.state.mn.us/stats/13/.
[433] Minn. Stat. § 13.01(3).
[434] Minn. Stat. § 13.02(7).
[435] *Id.*

- Procedures for access to the information;
- Procedures for classifying information as not public;
- Civil penalties for violation of the Act; and
- The charging of fees for copies of government data.[436]

The statute gives the Commissioner of Administration the authority to approve new uses and dissemination of private and confidential data on individuals,[437] and specifies powers with regard to approving temporary classifications of data.[438] Upon request of a state agency, statewide system, or political subdivision, or upon request of an individual who disagrees with such a body's determination regarding data practices, the Commissioner may issue an advisory opinion concerning the rights of data subjects and the classification of government data.[439] The opinions are not binding on the agency, but must be given deference by courts in related proceedings.[440] Moreover, government entities or persons that act in conformity with a written opinion are not liable for compensatory or exemplary damages or attorney's fees in actions brought under sections 13.08 and 13.09 of the MGDPA.[441] Those two sections—enabling private litigation not instituted by the state—are the primary mechanisms for enforcement of data protection rights.

In support of these statutory roles and responsibilities of the Commissioner, IPAD provides technical assistance and consultation, offers advice regarding proposed and draft legislation, assists in the research and drafting of opinions by the Commissioner of Administration, evaluates appeals regarding data, prepares publications to assist government entities, consults on relevant issues, provides training, and consults with the information technology community to ensure information systems are developed that comply with data practices laws. IPAD issues model documents, advisory opinions, training materials, summaries and guidance materials; annual reports are not produced.

IPAD is linked to the Governor's office through the bureaucratic hierarchy as part of the Department of Administration. Though independent of the Attorney General's office, that office does have the authority to review and overrule the Commissioner's opinions[442] (which has happened only twice in approximately 500 occurrences).

---

[436] Minnesota Department of Administration, A Brief Overview of the Minnesota Government Data Practices Act, in *Public Access to Government Data and Rights of Subjects of Data,* at http://www.admin.state.mn.us/data_practices_i.html#overviewofmgdpa.
[437] Minn. Stat. § 13.05(4).
[438] Minn. Stat. § 13.06.
[439] Minn. Stat. § 13.072(1)(a). Available at http://www.ipad.state.mn.us.
[440] Minn. Stat. § 13.072(2).
[441] *Id.*
[442] Minn. Stat. § 13.072(1)(c).

In 1997, the Minnesota Legislature established an Information Policy Advisory Task Force to assess the MGDPA.[443] The resulting report[444] was completed in January 1999, offering twenty-three recommendations that were summarized by the following five general conclusions:

1. There is no substantial sentiment to discard the State's Data Practices Act and to replace it with another model, for example, the federal "Freedom of Information Act."
2. There is general agreement, by both citizens and representatives of government entities, that using litigation to resolve disputes that arise out of information law and to enforce information policy law is ineffective for citizens and counterproductive for government agencies. Adoption of a variety of forms of alternative dispute resolution are much more preferable to resolve disputes and to promote compliance.
3. In most instances, representatives of government entities do their best to comply with information policy laws. However, there is an ongoing need for training for employees of government entities in what is actually required of them by information policy laws.
4. Not enough resources have been provided by the Legislature and other institutions of government to ensure that information policy laws are carried out so that citizens receive the benefits of these laws and government entities are not overly burdened by providing those benefits.
5. The resources that are allocated can be better spent if a stronger role is assigned to some organization at the state level that can assist both citizens and government entities in assuring that the objectives that the Legislature is trying to attain in the enactment of information policy laws are actually met.[445]

Among other significant issues in Minnesota, a key factor identified in the report and recommendations is the reliance on private litigation to attempt resolution of what may be local or systemic problems with data handling and protection. The knowledge and expertise developed in IPAD and made available to the government and citizenry through written opinions, educational materials and presentations, and legislative consultation is a great resource for the state. However, the lack of stronger statutory roles, including enforcement powers and resources, is a major constraint on privacy protection.

4.3.6 New York

The Committee on Open Government of the New York State Department of State[446] was originally created in 1974 as the Committee on Public Access to Records as part of the Freedom of Information Law[447] to advise individuals making requests regarding public access to public

[443] 1997 Minn. Laws ch. 202, *at.* 2, § 56.
[444] Minnesota Information Policy Advisory Task Force, *Report of the Information Policy Task Force to the Minnesota Legislature,* (1999).
[445] *Id.* at 6-7.
[446] The Committee website, at http://www.dos.state.ny.us/coog/coogwww.html.
[447] NY CLS Pub. O. Law, *at.* 6, §§ 84-90 (2001).

information. The Committee name was changed in 1981 to reflect the role of the Committee's work regarding open meetings and records. The Committee works with three laws, the Personal Privacy Protection Law,[448] the Freedom of Information Law,[449] and the Open Meetings Law.[450] The Personal Privacy Protection Law, which relies on Fair Information Practices principles, was passed in 1984.[451]

The Committee functions independently and is a part of the Department of State. Until 1978, it was a part of the Office of General Services. The Director of the Committee on Open Government serves at the pleasure of the Governor. The Committee has eleven members. Six of those members are from the public sector; another five are from the government. Of the public members, the governor appoints four and two of the governor's appointees must have a connection to the news media. The respective leaders of the Senate and the Assembly each appoint one of the two other public members. The five government members are the Lieutenant Governor, the Secretary of State, the Director of Budget, the Commissioner of General Services, and an appointee of the Governor. The Committee has four full-time equivalent employees.

The Committee oversees laws about personal privacy, freedom of information, and open meetings and open records. Under these laws, the Committee is responsible for: making recommendations about privacy laws; investigating appeals about data accuracy or access; furnishing advisory opinions to any individual who requests advice; encouraging state agencies to use fair information practices in the collection, maintenance, use, and disclosure of personal information; overseeing open access to public records and meetings of public bodies; preventing unauthorized release of personal information; and enabling individuals to correct and amend records pertaining to them.

The Committee offers advisory opinions upon request to all those who make inquiries. The Committee submits an annual report to the Governor and the Legislature. In New York, many different state statutes address specific types of information that may or may not be collected, as well as specific exemptions to the privacy and information laws.

A Task Force on privacy was set up by the New York Senate in 1999.[452] The Task Force described its primary objective as focusing on accessibility and control of information privacy.[453] The report offered numerous recommendations for privacy protections in a diverse range of areas, including state agency records, motor vehicle records, insurers, credit agencies, financial institutions, telemarketers, student records, and medical records.[454]

---

[448] NY CLS Pub. O. Law, *at.* 6-A, §§ 91-99 (2001). Available at http://www.dos.state.ny.us/coog/textdocs/pppl.txt.
[449] NY CLS Pub. O. Law, *at.* 6, §§ 84-90 (2001).
[450] NY CLS Pub. O. Law, *at.* 7, § 100 (2001).
[451] *Id.*
[452] The report of the Senate Majority Task Force on the Invasion of Privacy, issued in March 2000, at http://www.senate.state.ny.us.
[453] *Id.*, at p. 9.
[454] *Id.*, at p. 5 – 8.

Though the Committee on Open Government operates under three different laws, its work is focused primarily on substantive protections of open government. The Committee operates with considerable independence in an ombudsman role, offering assistance and advice to any party that makes an inquiry.

4.3.7 Wisconsin

Wisconsin, though it lacks a right to privacy in the state Constitution, does have a statutorily guaranteed right to privacy for its citizens.[455] This right to privacy provides protection against invasions of privacy, including the unauthorized use of an individual's specific name or image and the offensive intrusion into private areas.[456] Further, one of the duties of the state division of technology services is to "[f]acilitate the implementation of statewide initiatives, including development and maintenance of policies and programs to protect the privacy of individuals who are the subjects of information contained in the databases of state agencies…."[457]

Wisconsin had an Office of the Privacy Advocate, which acted primarily in the role of ombudsman and liaison. A law passed in 1991 created the Office,[458] but those statutes were repealed in 1995.[459] The Privacy Advocate reported to the Deputy Director of Administration, who reported directly to the Governor's Office. The Office was independent and advised by an advisory committee known as the Privacy Council. The Office was required to issue an annual report. Aside from the Privacy Advocate, a Program Assistant staffed the Office.

The Office was intended to promote policies that protected individual privacy at the state and local levels of government. It also worked to educate citizens about their rights and to assist citizens in making challenges to data. The Office served primarily as an ombudsman and liaison for state government, individual state agencies, the public, and the private sector. The Office had no legal authority to prosecute, investigate, or enforce privacy laws. The Office of the Privacy Advocate engaged in the following activities:

- Receiving and reviewing complaints from the public about privacy issues (e.g., an agency requiring personal information that the complainant thought was inappropriate);
- Conducting mediation between various stakeholder groups (e.g., individuals and state agencies; educating stakeholders about issues and concerns regarding privacy);

---

[455] Wis. Stat. § 895.50 (2001). Available at http://folio.legis.state.wi.us/cgi-bin/om_isapi.dll?clientID=212656&infobase=stats.nfo&j1=895.50&jump=895.50&softpage=Browse_Frame_Pg.
[456] Wis. Stat. § 895.50(2) (2001). Available at http://folio.legis.state.wi.us/cgi-bin/om_isapi.dll?clientID=212656&infobase=stats.nfo&j1=895.50&jump=895.50&softpage=Browse_Frame_Pg.
[457] Wis. Stat. § 16.974(3) (2001). Available at http://folio.legis.state.wi.us/cgi-bin/om_isapi.dll?clientID=212812&infobase=stats.nfo&j1=16.974&jump=16.974&softpage=Browse_Frame_Pg.
[458] 1991 Wis. Laws 39, as amended by 1991 Wis. Laws 269, codified at Wis. Stat. §§ 19.62-.63 (1991). The recommendation for creating the Office of the Privacy Advocate came from a Special Legislative Council Committee on Privacy and Information Technology in 1991.
[459] 1995 Wis. Laws 27, §§ 459-61.

- Offering opinions about the appropriateness of actions taken by state agencies in terms of privacy;
- Providing a clearinghouse function of information and activities in the state related to privacy; conducting studies on various privacy-related topics;
- Distributing model privacy statements (based on FIPS) to stakeholder groups, but primarily state agencies;
- Making public presentations and speeches about privacy topics and legislation that may affect privacy (e.g., proposed computer matching laws); and
- Encouraging other state agencies to deal with privacy issues (e.g., the Public Records Board to produce a directory of state agency databases containing personal information).

In the course of performing its duties, the Office of the Privacy advocate was advised by the Privacy Council.[460] The Council offered opinions on the policies and procedures of the Office of the Privacy Advocate. The Council also recommended legislation relating to privacy. The Governor appointed nine members of the Council, although five members had to be nominated by other state officials. The members were appointed to three-year terms. The members of the Council appointed the Privacy Advocate.

Since the closing of the Office of the Privacy Advocate in 1995, privacy has remained a much-discussed issue in Wisconsin. The members of the legislature of the State of Wisconsin have made numerous attempts to create a new privacy agency. In 1999, the Governor created a Governor's Task Force on Privacy, which issued a report with many suggestions for increasing privacy rights in the state.[461] The Governor's Task Force on Privacy made a number of very explicit and detailed recommendations for what the State of Wisconsin should do in the future. One that was particularly interesting stated: "No Wisconsin person should be required to comply with the European Union privacy directive."[462] Some of the other suggestions from this Task Force included:

- Prohibiting personal information from being released for marketing or advertising purposes;
- Clarifying access to public employee personnel records and certain other public records containing personal information;
- Prohibiting state agencies from gathering names, addresses, and other personally identifiable information from any individual visiting an agency website without the individual's consent;

[460] The Privacy Council was also authorized by 1991 Wis. Laws 39, as amended by 1991 Wis. Laws 269. The legislation creating the Council was codified at Wis. Stat. § 19.625 (1991). The Council was repealed at the same time as the Office of the Privacy Advocate.
[461] Governor's Task Force On Privacy, *Final Report And Recommendations*, (2000). This report is no longer available online.
[462] *Id.* 14.

- Requiring businesses that disclose personal information to third parties to establish written policies for such activities; and
- Requiring governments and businesses to explore ways to identify people without using Social Security Numbers. [463]

In 2001, the legislature was presented proposed legislation that would create a constitutional amendment establishing an independent right of privacy for residents of the State of Wisconsin.[464]

4.3.8 Summary of State Structures

The foregoing review provides a summary of seven states' efforts in the area of privacy protection, regulation, and oversight, with a focus on the privacy offices established for those purposes. These offices can work in a wide range of related areas, including, though not limited to, open records, open meetings, freedom of information, protection of personal privacy, data protection, consumer protection, sunshine laws, and identity theft investigations. The states analyzed in this section were selected to provide insight into the variety of functions these offices can serve and the similarly wide range of activities in which the offices can engage. They display the wide array of state approaches to privacy offices, from the complex structure of the Hawaii's Office of Information Practices to the entirely abandoned Office of the Privacy Advocate in Wisconsin. The roles of the agencies also vary greatly, ranging from acting as an ombudsman to acting as a referral service to issuing legally binding orders. Additional analysis may be found later in this report.

4.4 International Structures

Privacy and data protection policies on the international level have been defined in large part by the policies of the European Union (EU). ~~Regarding privacy and data protection, nations may be divided into nations that are members of the EU and nations that are not.~~ The policies of the EU define what EU member states must do, but also establish standards that other states are pressured to follow if they want to export personal data from EU member nations.

~~Within the EU, t~~The European Union Data Protection Directive ~~provides~~ establishes a minimum standard of privacy and data protection with which EU member states must comply. Some EU member states have passed laws that have privacy and data protection standards beyond the minimum requirements of the Data Protection Directive. Section 4.4.1.1 examines the EU Data Protection Directive and its impact on EU member states as a whole. Appendix D compiles the agency names, websites, and available laws of the nation discussed in this section.

---

[463] *Id.* The American Civil Liberties Union of Wisconsin has also been active in working to expand privacy protection in the state through its ongoing Data Privacy Project, which was established in 1996. Available at http://www.aclu-wi.org/issues/data-privacy/. In April 2001, the Data Privacy Project published a report entitled *Wisconsin's Electronic Government,* on the status of privacy in the state.

[464] Wis. AJR 23 (2001). The proposed Constitutional Amendment, at http://www.legis.state.wi.us/2001/data/AJR-23.pdf.

The EU Data Protection Directive has also had an effect on the privacy and data protection policies of many non-EU nations. Adoption of EU-compliant policies allows a nation the opportunity to conduct transactions involving the export of personal data from EU Member States without difficulty ~~with EU nations~~. The adoption of an EU-compliant law is especially important ~~in the realm of~~ for business, and also helps any nation that hopes to join the EU in the future. Section 4.4.2 examines several non-EU member states that have passed legislation attempting to comply with the requirements of the Data Protection Directive. Section 4.4.3 examines several non-EU nations that have passed privacy and data protection laws not modeled on the EU Data Protection Directive.

Given the importance and influence of the EU structure, many non-EU nations have even adopted EU terminology for privacy and data protection. This section uses these specific terms as well. In EU terminology, *data protection* is used rather than *privacy*. *Data controller* (also known as *controller*) is the EU term for natural or legal bodies that possess, use, process, or provide personal data. A data controller can be anything from a major multinational corporation to a self-employed business owner.

The nations are discussed in alphabetical order in each subsection; the sequence in which they are discussed does not reflect any ranking or rating. The information in these subsections is drawn from the material available through government sources, such as official privacy and data protection agency websites, from academic literature and from other reliable secondary materials. Problems with the availability of some materials, especially in English, limited the amount of information reviewed and presented for certain nations.

4.4.1 ~~4.4.1 European Union Nations~~ European Union Member States

Several EU member states first passed legislation protecting rights of individuals with regard to privacy and data processing in the 1970s.[465] In 1980, the Organization for Economic Cooperation and Development (OECD) promulgated a set of principles to serve as a minimum standard for protection of personally identifiable information.[466] A Council of Europe convention, Treaty 108, established the first set of basic principles for protection of personal data in Europe.[467] The basic principles of Treaty 108 of 1981 can be found in the data protection laws of all EU member states.[468]

[465] *Data Protection: Background Information,* a European Union report, at http://www.europa.eu.int/comm/internal_market/en/dataprot/backinfo/info.htm.
[466] Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data,* 1980, at http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM.
[467] *Data Protection: Background Information*, a European Union report, at http://www.europa.eu.int/comm/internal_market/en/dataprot/backinfo/info.htm.
[468] *Id.*

4.4.1.1 Overview of European Union Data Protection Directive

The EU Data Protection Directive[469] was formally approved on October 24, 1995, and went into effect three years later. The directive establishes minimum requirements for national data protection laws and requires each EU member state to enact laws governing the "processing of personal data," including but not limited to activities of data "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[470] Personal data is broadly defined as "any information relating to an identified or identifiable natural person,"[471] and includes textual information, photographic and audiovisual images, and sound recordings of any identified or identifiable person, living or otherwise. The exceptions to the policies on the processing of personal data are for activities outside the scope of European Community law, including criminal law and national security, as well as processing of data by natural persons in the course of purely private and personal activity.[472] Without the consent of the subject, the use of sensitive data or special categories of personal data, such as data about "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" is narrowly restricted.[473]

The personal data that is processed must be accurate, up-to-date, relevant, necessary for the intended purpose, limited to the specified purpose, and can only be collected with the consent of the subject or to protect "the public interest" or the "legitimate interests" of a private party.[474] Individuals must have access to their personal data that is being processed and the opportunity to correct "incomplete or inaccurate" data.[475] Individuals also have the right to object on "legitimate grounds" to the processing of data.[476] In many contexts, data controllers are required to notify the national data protection agency of their identity and their intent and uses for data before beginning the collection and processing of data.[477] Data collectors must inform data subjects of their identity, the purposes of the processing, the "obligatory or voluntary" nature of replying, the impact of failing to reply, third parties who may receive the data, and the rights of the subject in access to and ability to correct the data.[478] Data controllers also must ensure security in the processing of data through

---

[469] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data, Official Journal L 281, 23/11/1995. The Data Directive, at http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html. EU privacy policy statements and other relevant EU documents on privacy and data protection, at http://www.europa.eu.int/comm/internal_market/en/dataprot/index.htm.

[470] *Id.* 2(b).

[471] *Id.* 2(a).

[472] *Id.* 3(2).

[473] *Id.* 8.

[474] *Id.* 6-7.

[475] *Id.* 12.

[476] *Id.* 14.

[477] *Id* 18-21.

[478] *Id* 10.

"appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access."[479]

Each nation must have at least one supervisory authority that operates with complete independence in exercising its functions with a specific set of powers and duties.[480] The supervisory authority must be consulted on the creation of administrative measures and regulations regarding personal data.[481] Each supervisory authority has the powers to investigate data processing activities, including the abilities to:

- Access and collect data;
- Intervene in the processing of data;
- Order blocking, erasure or destruction of data;
- Impose bans on processing, issue warnings and admonitions;
- Refer matters to legal institutions; and
- Engage in legal proceedings or bring violations to the attention of judicial authorities.[482]

Each supervisory authority must also hear claims by any person or association of persons concerning the protection of rights and freedoms in the processing of personal data.[483] Those who file claims must be informed of the outcome by the supervisory authority.[484] Each supervisory authority must make a public report regarding its activities at regular intervals.[485] The members and staff of supervisory authorities, even after employment has ended, are required to maintain professional secrecy regarding all confidential information encountered during job performance.[486]

Each nation must also establish judicial remedies and civil liabilities for use against data controllers that fail to follow proper procedures or that engage in unlawful data processing activities.[487] Nations are expected to encourage national trade associations and other professional and industry organizations to create codes of conduct for data control and processing.[488] Each nation is further obliged to prohibit transfer of personal data to non-EU nations that do not ensure adequate

[479] *Id.*16-17.
[480] *Id.* 28.
[481] *Id.* 28(2).
[482] *Id.* 28(3).
[483] *Id.* 28(4).
[484] *Id.* 28(4).
[485] *Id.* 28(5).
[486] *Id.* 28(7).
[487] *Id.* 22-24.
[488] *Id.* 27.

protection of data,[489] though numerous exceptions are provided to this prohibition, such as if the transfer is legally required, necessary to fulfill a contract, or is for an "important public interest."[490]

The Directive establishes two institutions with advisory and other powers. The Article 29 Working Party consists primarily of representatives of national supervisory authorities, and it considers questions, gives opinions to the European Commission, and makes recommendations.[491] The Article 29 Working Party ~~is~~ primarily focuse~~d~~s on issues regarding the application of national measures to ensure uniformity of data protection within the EU; the level of protection within EU member states and non-EU nations; and the evaluation of any proposed changes to the Data Protection Directive.[492] The Article 29 Working Party also makes recommendations on all matters regarding privacy and data protection within the EU.[493] An annual report about the activities of the Article 29 Working Party is published and made available to the public.[494]

The other advisory institution established by the EU Data Protection Directive, the Article 31 Committee, consists of representatives of the Member States.[495] It has authority to give opinions to the European Commission on proposals relating to the level of compliance by third countries and on other matters.[496]

In summary, the EU Data Protection Directive ~~has~~ creates a minimum set of privacy and data protection rights. These rights include limitations on the collection, use, or processing of sensitive or individually identifiable data. The personal data that is processed is required to be accurate, up-to-date, relevant, and limited to the specified purpose. Individuals have the right of access to their personal data that is being processed, the right to correct incomplete or inaccurate data, and the right to object on legitimate grounds to the processing of data. The EU Data Directive also places affirmative obligations on the EU member nations to establish agencies with powers and duties to supervise data protection at the national level. The structure established by the EU Data Protection Directive has not only significantly influenced data protection and privacy rights in EU member nations, but has had an impact in many non-EU nations as well. The following subsections provide a case-by-case review of selected EU Nations.

---

[489] *Id.* 25.
[490] *Id.* 26.
[491] *Id.* 29.
[492] *Id.* 30(1).
[493] *Id.* 30(2).
[494] *Id.* 30(6). The annual reports of the Article 29 Working Party, at http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm.
[495] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data, Official Journal L 281, 23/11/1995, *at.*31.
[496] *Id.*

4.4.1.2 France

The National Data Processing and Liberties Commission (Commission Nationale de l'Informatiuqe et des Libertes) was created in 1977 by the Act on Data Processing, Data Files, and Individual Liberties.[497] The Act went into effect on January 6, 1978, and establishes rights of access, clarification, updating, and correction of data and establishes guidelines for data processing.[498] France is one of three EU Member States that has yet to amend its law to reflect the requirements of the EU Directive.

The Commission, commonly known as the CNIL, is comprised of 17 members of parliament, magistrates, and other members of government. The appointments for the chairperson and for the other members are for five years. The broad-based membership consists of: two deputies and two senators elected respectively by the national Assembly and the Senate; two members of the Economic and Social Council, elected by it; two members or former members of the Conseil d'Etat, one ranking as "conseiller" or higher, elected by the general assembly of the Conseil d'Etat; two members or former members of the Cour de Cassation, one ranking as "conseiller" or higher, elected by the general assembly of the Cour de Cassation; two members or former members of the Cour des Comptes, one ranking as "conseiller-maitre" or higher, elected by the general assembly of the Cour des Comptes; two persons qualified by their knowledge of data processing applications, appointed by decree on proposals by the speaker of the National Assembly and the speaker of the Senate respectively; three persons appointed by decree made in the Council of Ministers on account of their authority and competence.

The Commission is an independent agency that advises the government on issues of privacy and data protection. The federal government and the judiciary rely on the Commission to provide research about and monitoring of data activities. The Commission reports on legitimacy of proposed data processing systems. The Commission oversees compliance with Act and ensures public access to information. The Commission issues opinions on disclosure and access. These opinions are binding unless overturned by Conseil d'Etat. The Commission also maintains a register of Data Collectors. Once Data Collectors notify the Commission of their intent, data processing may begin. Public sector processing can only be authorized by a law or regulation of the government adopted after obtaining the "reasoned opinion" of the Commission. The Commission can be overruled by the Conseil d'Etat.

---

[497] The CNIL website, at http://www.cnil.fr.

[498] The 1977 Act on Data Processing, Data Files, and Individual Liberties, as amended, at http://www.cnil.fr/textes/index.htm. An unofficial English version, at http://ccweb.in2p3.fr/secur/legal/a78-17-text-local.html#renv.

4.4.1.3 Germany

The Federal Data Protection Commissioner (Bundesbeauftragten für den Datenschutz) was created by the Federal Data Protection Act.[499] The Federal Data Protection Act of 1990, as amended, is an omnibus law replacing the Federal Data Protection Act of 1977. [500] The law was further amended in 2001 in an attempt to bring Germany into full compliance with the EU Directive. The law has not yet been translated into English, but it does not appear to make any significant structural changes in the Commissioner's office. Further amendments to the law are planned. There is some controversy whether the new amendments meet the requirements of the EU Directive.

The Commissioner is elected by Parliament, needing to receive affirmative votes from more than half of the statutory members. Once elected by the Parliament, the Federal President officially appoints the Commissioner. The Commissioner must be at least 35 years old at time of appointment. The term of appointment is for five years and may be renewed once. The Commissioner is independent, but subject to legal supervision of the national government, and advises the government and individual ministers. The Commissioner has the right to consult with Parliament at any time.

The office of the Commissioner is located administratively within the office of the Federal Minister of the Interior. The Commissioner is subject to hierarchical supervision of the Federal Minister of the Interior, though the Commissioner's budget is separate from that of the Federal Minister of the Interior. These administrative matters do not reduce the independence of the Federal Data Protection Commissioner.

There are also 16 provincial commissioners, each within a provincial data protection agency. Most provincial agencies are responsible for the government agencies within the province, but five (Berlin, Bremen, Hamburg, Lower Saxony, and Northrhine-Westphalia) are also responsible for the private sector.

The Commissioner monitors compliance and keeps a register of all Data Controllers with data files that store personal data. The Commissioner hears appeals from individual citizens regarding potential privacy violations and investigates these potential violations. The Commissioner refers violations of the law to the judiciary for prosecution, which can result in financial penalties or imprisonment. The Commissioner also makes recommendations to the government for improving data privacy laws.

The regulatory schemes for public and private bodies overseen by the office of the Commissioner have some differences. Private bodies with more than five employees in automatic data processing or twenty persons using other forms of data processing must have a data protection officer (DPO)

[499] The Commissioner's website, at http://www.bfd.bund.de.
[500] The Federal Data Protection Act of 1990, as amended, at http://www.bfd.bund.de/information/bdsg_eng.html.

within the organization to monitor the data processing activities of the organization. The DPO must also educate the data processing employees regarding data protection and privacy rights.

4.4.1.4 Ireland

The Office of the Data Protection Commissioner (Coimisineir Cosanta Sonrai) was created by the Data Protection Act, 1988.[501] The Data Protection Act, 1988, as amended, incorporates the Council of Europe Convention as a schedule.[502] Ireland has not yet amended its law to conform to the EU Directive. In the near future, Ireland is scheduled to implement the EU ~~EU Data Protection~~ Directive.

A single Commissioner ~~is~~ appointed by the government ~~to~~ serves a fixed term not to exceed five years. The Commissioner may be reappointed. The Commissioner is independent in the performance of his or her functions. The Commissioner may be removed only if ill and unable to perform the functions or in case of misbehavior. At age 65, the Commissioner must vacate the Office.

The Commissioner oversees compliance by government and private bodies with privacy laws. The Commissioner oversees compliance by all Data Controllers with the laws and standards for the handling of personal data. The Commissioner handles complaints about personal privacy and investigates those complaints. The Commissioner can get any relevant information requested for an investigation. The Commissioner issues orders to privacy complaints and has enforcement powers for those orders, including correction of data, supplementing data, or erasing data. Failure to comply with an order is a criminal offense. The Commissioner can prohibit overseas transfer of data. The Commissioner can inspect Data Controllers for compliance. The Commissioner encourages trade associations and other professional groups to prepare codes of practice. Any code approved by the Commissioner can be placed before the Oireachtas (Parliament) for approval. Once approved, the code has the force of law for that particular association or organization.

The Commissioner keeps a public register about data handling practices of government departments and private bodies, financial institutions, and any person or organization that keeps personal data. The register includes names of Data Controllers, types of information kept, purpose for information use, and a list of who has received the data.

[501] The Commissioner's website, at http://www.dataprivacy.ie.
[502] Available at http://www.dataprivacy.ie/6ai.htm.

4.4.1.5 Italy

The Italian Data Protection Commission (Garante Perla Protezione Dei Dali Personali) was created in 1993 by the Processing of Personal Data Act.[503] The Processing of Personal Data Act of 1999 was amended by the Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data, the Act Enabling the government in the Field of the Protection of Individuals and Other Subjects with regard to the Processing of Personal Data, Presidential decree No. 318 of 28.07.99, Legislative decree No. 135 of 11.05.99, and Legislative decree No.281 of 30.07.99.[504] The laws have been amended to implement the EU Data Protection Directive ~~95/46/EC~~.

The Commission ("the Garante") has four members; the Chamber of Deputies selects two of the members. The elected members appoint the Chairperson, who has the tie-breaking vote. If no majority is achieved by the third ballot in the election of the chairperson, the oldest member shall be elected the chairperson. The Garante appoints the deputy-chairperson. In cases of a tie vote on any issue, the Chairperson breaks the tie by casting a second vote. The terms of appointment are for four years and can be renewed once. The Garante is autonomous and independent in its activities. Members of the Garante must have proven experience in either the field of law or computer science. Members must also have a background that will ensure independence.

The Garante oversees compliance with laws and advises the government about the need for further legislation. The Garante can investigate, order technical assessments, issue orders based on the investigations, order changes to data use, or stop data operations entirely. The Garante can force payment of damages for improper processing of personal data and can seek imprisonment and administrative remedies. The Garante can also order public and private authorities to cooperate in an investigation. The Garante informs the public of the legal rights of citizens regarding privacy.

Data Controllers must notify the Garante, stating: name, trade, and domicile; purposes and methods of processing; type of data; where data stored; any communication of data; any proposed transfer of the data; and description of technical and organizational safeguards. There are exemptions in the law for defense, state security, and crime control, judicial offices, and criminal records from on-going proceedings. Public offices are limited to collecting only data that is necessary to comply with legal obligations and carry out institutional duties.

---

[503] The website for the Commission, at http://astra.garanteprivacy.it/garante/HomePageNs.
[504] Available at http://astra.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG=2.

4.4.1.6 Netherlands

The Netherlands Data Protection Commission (College Bescherming Persoonsgegevens) was created in 1989 by the Data Protection Act.[505] The Personal Data Protection Act, as amended through Session 1999-2000 Nr. 92 (25892), has been amended to implement the EU Data Protection Directive ~~95/46/EC~~.[506]
~~The Netherlands is a recognized leader in the use of industry codes. The Chairman of the Netherlands Data Protection Commission is currently chair of the Article 29 Committee established under the EU Directive.~~

The Office of the Data Protection Commission is comprised of a chairperson and two other members. The Chairperson is appointed by royal decree on a proposal from the minister for a six-year term. The Chairperson can be reappointed. The other two members, plus special members representing other sectors, are appointed by royal decree on proposal from minister for a four-year term. They can be reappointed, but are automatically discharged at age 65. The Commission is independent in the performance of its tasks. An advisory board was established to advise the Commission on general aspects of data protection and privacy. Members of the advisory board are drawn from various sectors of society and are proposed by the Commission and appointed by the Minister.

The Commission mediates disputes, but can send matters to courts, if necessary. The Commission can impose fines for violations resulting in property loss or other harms. The Commission can also impose administrative costs. The Commission educates the public about data protection and privacy rights. The Commission advises Parliament regarding proposed legislation and issues opinions on proposed legislation.

The Commission must be notified of fully or partly automated processing of personal data before processing begins. The Commission maintains a public register of approved Data Controllers. The data protection rules apply to government bodies except armed forces, intelligence, security, police, and elections.

The Commission reviews and approves appropriate codes of conduct for organizations or sectors. The Commission strongly encourages each sector to use different system for keeping track of individuals and not to use unique personal identification numbers. The Commission officially publishes the approved codes. The Netherlands is a recognized leader in the use of industry codes.
~~The data protection rules apply to government bodies except armed forces, intelligence, security, police, and elections.~~

[505] Available at http://www.registratiekamer.nl.
[506] Available at http://www.registratiekamer.nl/bis/top-1-11.htm.

4.4.1.7 Portugal

The National Data Protection Commission (Comissao Nacional de Protecto de Dados) was created in 1991 by Law for Protection of Personal Data.[507] The Law for the Protection of Personal Data with Regard to Automatic Processing (1991) was Portugal's initial data protection and privacy statute. That law was expanded by the Act on the Protection of Personal Data, no. 67/98, as amended, which came into effect on October 26, 1998.[508] The law implements the EU Data Protection Directive. The workload of the Commission increased markedly since passage of the 1998 amendments.

The Commission has seven members recognized for integrity and merit. The members of the Commission are appointed for non-renewable five-year terms. The assembly elects the chairperson and two members; two members are magistrates, one a legal magistrate and the other from the Public Prosecution Service, with over ten years experiences each; and the government appoints two members. The Commission is a national independent authority that operates within the Assembly of the Republic. The Commission is represented in legal proceedings by the Public Prosecution Service.

The Commission monitors and supervises compliance with the data privacy laws. The Commission inspects Data Collectors in overseeing compliance. The Commission has investigative powers and may access any data necessary to carry out its duties. The Commission can order blocking, erasing, or destruction of data. The Commission can issue fines for minor violations of data privacy laws and can make referrals for prosecution for criminal violations of data privacy laws. The Commission promotes public awareness of data privacy laws and must be consulted on any legal provisions and on legal instruments in preparation in community or international institutions relating to the processing of personal data. The Commission can suggest legislation to the assembly.

The Commission has authority to promote the drawing up of codes of conduct and may declare whether the codes are in accordance with applicable law. Data Controllers must notify the Commission about automated processing activities. Some types of processing may be exempted from notice. Commission approval is required for the processing of credit, sensitive, and some other types of data. The Commission maintains a register for processing that must be noticed or approved. The Act applies to the processing of personal data regarding public safety, national defense, and State security.

[507] Available at http://www.cnpd.pt.
[508] Available at http://www.cnpd.pt.

4.4.1.8 United Kingdom

The Office of the Information Commissioner was originally created (as the Office of the Data Protection Registrar) in 1984 by the Data Protection Act.[509] The Office now oversees compliance with the Data Protection Act of 1998 and the Freedom of Information Act 2000.[510] The Data Protection Act was amended to implement the EU Data Protection Directive. The Office is in charge of both data protection and freedom of information.

The Office is an independent supervisory authority. The Commissioner is appointed for a five-year term by Her Majesty by Letters Patent and may be reappointed. The Queen may only remove the Commissioner from office in pursuance of an address from both Houses of Parliament.

The Commissioner is advised by a Data Protection Tribunal, consisting of a chairman appointed by the Lord Chancellor after consultation with the Lord Advocate, such number of deputy chairmen so appointed as the Lord Chancellor may determine, and such number of other members appointed by the Secretary of State as he may determine. Some members of the Tribunal are persons who represent the interests of data subjects, and persons to represent the interests of data controllers

The original law and its registration requirements overwhelmed the small staff of the British Data Protection Registrar. Over the years, and with the 1998 changes, the registration requirements ~~have been~~were simplified and more exemptions ~~have been~~were created.

The Commissioner's mission is to develop respect for the private lives of individuals and encourage the openness and accountability of public authorities by promoting good information handling practices and enforcing data protection and freedom of information legislation; and by seeking to influence national and international thinking on privacy and on information access issues. The main principles of data protection include: no unfair processing; no inaccurate data; no unsecured data; data cannot be inadequate, irrelevant, or excessive; no unlawful disclosure of data; and data must be published in line with individual's legal rights. Priority is given to ensuring that public bodies give due weight to both the public's right to know and the individuals' right to respect for private life. The Commissioner ensures individuals are aware of the rights of privacy and information.

The Commissioner has enforcement powers, including inspections, conducting formal investigations, making orders based on investigations, and monitoring to ensure compliance. The Commissioner may publish codes of practice for guidance as to good practices under the Act. The Commissioner may also offer opinions to trade association whether a proposed code promotes the following of good practice. The Office maintains a public register of Data Controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by a data controller. The Data Protection Act 1998 requires every data

[509] Available at http://www.dataprotection.gov.uk.
[510] The Data Protection Act 1998, Ch. 29, as amended, at http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm.

controller who is processing personal data to notify the Commissioner unless they are exempt. The law covers government agencies, but provides an exemption from a number of provisions of the Data Protection Act if exemption from any such is required for the purpose of safeguarding national security.

4.4.2 Non-European Union Nations Following European Union Model

Many non-EU nations are implementing laws addressing privacy and data protection issues to meet the standards established by the EU Data Protection Directive. Some of these nations, such as the Czech Republic, have actually created laws with greater protection than ~~that is~~ required by the Data Protection Directive. The EU prohibition against the transfer of data to nations with inadequate data protection has led a significant number of non-EU nations, including the Czech Republic, Hungary, Iceland, Liechtenstein, Lithuania, Monaco, Norway, Poland, Russia, Slovakia, Slovenia, and Switzerland, to implement legislation that meets the requirements of the Data Protection Directive.[511] Non-EU nations have two reasons for taking this action. First, it will facilitate business transactions with EU-based companies and within the EU itself. Second, it will help the non-EU nations in gaining membership to the EU in the future. The following subsections provide a case-by-case review of selected Non-EU Nations following EU Models.

4.4.2.1 The Czech Republic

The Office for Personal Data Protection (Úřad pro Ochranu Osobních Údajů) was created in 1992 by the Act on Protection of Personal Data in Information Systems.[512] That law was replaced by the Act No. 101 of April 4, 2000 on the Protection of Personal Data and on Amendments to Some Related Acts, as amended by Act No. 227 of June 29, 2000.[513]

The Czech Republic passed a European Union-style privacy law in 2000 to replace an earlier privacy law. The Czech Republic is seeking membership in the European Union. The privacy law has some provisions that exceed the privacy protections in the EU Directive.

The Office is an independent organization. The President appoints the Chairperson of the Office~~is appointed by the President~~ for a 5-year term, renewable once, ~~for a 5-year term, which can be renewed one time.~~ based on a proposal from the Senate. The Chairperson can be recalled at any time for failure of duties. To be appointed Chairperson, an individual must enjoy legal capacity, be a university graduate, have no criminal record, and have the proper experience and moral qualities to perform the job. Seven inspectors carry out the activities of the Office. The inspectors of the Office are also appointed by the President on recommendation from the Senate. The inspectors are appointed for a period of ten years, which can be renewed. The inspectors must meet the same criteria as the Chairperson does. The Chairperson consults on level with the Cabinet.

---

[511] Scott Blackmer, *The European Union Data Protection Directive,* (paper presented at the Privacy & American Business Meeting on Model Data Protection Contracts and Laws, February 1998). Available at http://Privacyexchange.Org/Tbdi/EU_PDR/Blackmerdirective.html. See also Curtis D. Frye, *Privacy-Enhanced Business: Adapting to the Online Environment,* 57-59 (2001).

[512] Available at http://www.uoou.cz/eng/index.php3.

[513] Available at http://www.uoou.cz/eng/101_2000.php3.

The Office supervises the observance of legally mandated responsibilities in the processing of personal data, maintains a register of instances of permitted personal data processing, deals with notifications and grievances from citizens concerning infringements of the law, and provides consultations in the area of personal data protection. The Office reviews relevant drafts of legislative intents, bills, and legal regulations. Powers of the Office include: overseeing fulfillment of all legal obligations of data protection law in public and private sectors; compiling database of permitted data processing activities; recording and investigating complaints about data privacy; ensuring compliance with international treaties regarding data privacy; educating the public about privacy issues; harmonizing national laws with international laws; and establishing a policy on electronic signatures.

The Office gives permission to and registers Data Controllers and their uses of personal data. Data Controllers must have the consent of the subject to use personal data and may only use the personal data for the specified purpose through the specified means and manners. The law requires that Data Controllers get written approval from agency prior to commencing data collection or processing. The Office has data protection power over all government functions except: intelligence services, police, National Security Office, Ministry of Finance, and Ministry of Interior.

4.4.2.2 Hungary

The Parliamentary Commissioner for Data Protection and Freedom of Information (Orszaggyulesi Biztosok Hivatala) was created by the Data Protection and Freedom of Information Law of 1992.[514] The Data Protection and Freedom of Information Law of 1992, Act No. LXIII of 1992, was amended and expanded in 1995 and 1999.[515] The Hungarian Constitution guarantees protection of personal data and freedom of information.

The Hungarian law was the first information rights law in Europe to address both privacy and freedom of information. Passed in 1992, the law was drafted prior to the creation of the EU Data Protection Directive, yet the Hungarian law included many similar provisions. It was later amended to move closer to the Directive's requirements. The European Union determined that the Hungarian law provides an adequate level of protection.

The Commissioner is elected by the Parliament for a period of six years. The Commissioner is independent. The Commissioner is also a member of the Hungarian Statistics Council, which determines some uses of personal identification data. The Commissioner is integrated into a common organizational structure with the Parliamentary Commissioner for Human Rights and the Parliamentary Commissioner for Ethnic Minorities. The organizational structure of these three Commissioners employs a staff of approximately 120 persons.

---

[514] Available at http://www.obh.hu/adatved/indexek/index.htm.
[515] Available at http://www.obh.hu/adatved/indexek/index.htm.

The Commissioner oversees implementation of laws and investigates complaints. The Commissioner issues opinions on draft legislation and proposes laws and regulations. The Commissioner can inspect the operations and records of any Data Controller and can stop the operations of a Data Controller for unlawful data practices. The Commissioner informs the public of the identity of Data Controllers engaged in unlawful data practices. Orders by Commissioner do not have legally binding force. The Commissioner must inform the public of data protection and information rights.

Registration by data controllers is required, however there are major exceptions, especially for government records. The Commissioner maintains the data protection register. The Act applies to government bodies except for designated state secrets and official secrets.

4.4.2.3 Poland

The Bureau of the Inspector General for the Protection of Personal Data (Generalny Inspektor Ochrony Danych Osobowych) was created by the Act on Personal Data Protection of August 29, 1997.[516] A right to personal privacy is guaranteed by three Articles of the Constitution of Poland.

The Inspector General for the Protection of Personal Data is appointed and dismissed by the Diet of the Republic of Poland with the consent of the Senate. The term of office is four years, and one reappointment is permitted. The bureau is comprised of six sections: the Office of the Inspector General; the Legal Department; the Inspection Department; the Computer Department; the Administrative and Budgetary Department; and the Personal Data Files Registration Department. The Inspector General oversees and directs the operations of all six sections. The Inspector General appoints a Director General to function as a primary assistant.

The Bureau delivers opinions on legislation and ordinances relating to personal data. The Bureau investigates complaints and issues administrative decisions. The Bureau inspects Data Controllers for use and protection of data. The Bureau trains private sector data handlers on proper usage and security of personal data.

The Bureau maintains and manages a data files register. Most Data Controllers must notify the Bureau about their processing activities. The Bureau may reject a notice. The Bureau maintains a public register of notifications. The Bureau provides information regarding the register to the public.

The law applies to state and local government authorities, to other state and municipal organization units, and to non-governmental bodies carrying out public tasks. The Bureau monitors government compliance and trains government data handlers on proper usage and security of personal data.

---

[516] The Bureau's website, at http://www.giodo.gov.pl/English/english.htm. The Act on Personal Data Protection of August 29, 1997; at http://www.giodo.gov.pl/English/english.htm.

4.4.3 Non-European Union Nations Not Following European Union Model

Several other nations have established types of privacy and data protection offices that are not directly based on the EU Data Protection Directive scheme. Most countries that have privacy and data protection laws that are not based on the EU model are now working to make their laws acceptable to the EU members. Several of these models are worth noting for their unique characteristics, specifically Australia, Canada, Hong Kong, and New Zealand. Along with the federal government of Canada, several of Canada's provincial agencies (British Columbia, Ontario, and Quebec) will be examined in this subsection. The following subsections provide a case-by-case review of selected Non-EU Nations not following EU Models.

4.4.3.1 Australia

The Office of the Federal Privacy Commissioner was created by the Privacy Act 1988.[517] The Privacy Act 1988 covered the activities of the federal government. The Privacy Amendment (Private Sector) Act 2000, an amendment to be implemented on December 21, 2001, is designed to extend privacy protections to include information held by private Data Collectors, though it has an exception for data collection by political parties. The Privacy Act 1988, as amended by Privacy Amendment (Private Sector) Act 2000, includes National Privacy Principles (Schedule 3).[518] It is not clear that the EU will consider the Australia private sector privacy provisions to be adequate. Several Australian states have privacy laws as well.

The Commissioner is appointed for up to seven years and is eligible for re-appointment. The Commissioner's appointment ends automatically at age 65. The Commissioner investigates complaints and performs audits of compliance. The Commissioner also provides "policy advice" to public and private organizations. The Commissioner monitors government data matching programs and issues guidelines for protection of privacy in data matching activities, including the monitoring of compliance and the investigating of complaints. The Commissioner can limit use of tax file numbers, consumer credit information, and personal credit information in private sector. The Commissioner provides advice on the operation of the privacy laws. The Commissioner examines proposed laws with relevance to privacy issues and can make submissions to legislature. The Commissioner educates the public about the rights to privacy and data protection. The Commissioner reviews privacy codes and publishes guidelines for information usage.

The Privacy Act of 1988 regulates primarily national government agencies and functions. It has no power over state or local government bodies. The law strictly limits collection, storage, use, and disclosure of information. The law also guarantees individuals access to and correction of personal data.

---

[517] Available at http://www.privacy.gov.au.

[518] The Privacy Act 1988, Act No. 119, as amended by Act No. 55 of 2001, and the Privacy Amendment (Private Sector) Act 2000, Act No. 155 of 2000, at http://www.privacy.gov.au/news/pab.html/#6.

4.4.3.2 Canada

The Office of the Privacy Commissioner of Canada was created in 1982 by the Privacy Act,[519] which Canada's original privacy law covered the federal sector only.[520] The Personal Information Protection and Electronic Documents Act, which took effect in part on January 1, 2001, and is to be completely implemented by January 1, 2004, extends data privacy rights to private sector activities and organizations not covered by the Privacy Act.[521] The 2000 amendments extended privacy rules to the private sector beginning in 2001, phasing in over three years. Some Canadian provinces have privacy laws, and the new 2001 federal law delicately describes how power will be shared between federal and provincial governments. The Canadian law is likely to be considered as adequate by the European Union.

The Governor in Council and the Senate and House of Commons appoints the Commissioner to a 7-year term, which can be renewed. The Commissioner is an Officer of Parliament who reports directly to the House of Commons and the Senate. Each province, as noted below, may also have its own provincial data protection commissioner.Each province also has its own data privacy commissioner.

The Office investigates privacy complaints involving both the public and the private sector. The Office has established policy favoring negotiation and persuasion, using mediation and conciliation, rather than other actions against violators. The Office has power to summon witnesses, administer oaths, and compel the production of evidence in formal hearings. The Office has limited ability to send issues to courts, and may do so only when a government agency is refusing an individual access to his or her own personal information. The Office investigates organizations and conducts audits of compliance. The Office educates the public about rights and provides compliance advice to companies and organizations. The Commissioner's duties include encouraging organizations to develop organizational codes of practice. The Office of the Privacy Commissioner has authority to oversee compliance in government activities.

4.4.3.3 British Columbia, Canada (Provincial Authority)

The Information and Privacy Commissioner was created in 1992 by the Freedom of Information and Protection Act.[522] The Commissioner is recommended by the legislature and appointed by the Lieutenant Governor. The Commissioner is appointed for 6-year, non-renewable term. The Commissioner is an officer of the legislature but is independent of the government in function.

The Commissioner only has power over public agencies in the province. Public bodies can only collect information if authorized by law, if for law enforcement, or if necessary for the operation of

---

[519] Available at http://www.privcom.gc.ca.
[520] The Privacy Act, as amended, at http://www.privcom.gc.ca/legislation/02_07_01_e.asp.
[521] The Personal Information Protection and Electronic Documents Act, at http://www.privcom.gc.ca/legislation/02_06_01_e.asp.
[522] Available at www.oipbc.org. Freedom of Information and Protection of Privacy Act (1992), at www.oipcbc.org/BCLAW.html.

a public body. Public bodies must make all reasonable efforts to ensure information is accurate and complete. Public bodies may only use information for specified, lawful purpose related to functioning of the agency.

The Commissioner monitors access to information and privacy protection by public agencies in the province, including ministries, public corporations, government agencies, boards, commissions, universities, and local public bodies. The Commissioner conducts reviews and investigations of the decisions of these bodies for correctness of information, adequate access to information and adequate protection of personal privacy. The Commissioner issues orders with which agencies must comply, unless a judicial review of the order is sought. The Commissioner comments on proposed legislation and public policy. The Commissioner monitors self-governing professional bodies, such as lawyers and physicians.

4.4.3.4 Ontario, Canada (Provincial Authority)

The Information and Privacy Commissioner was created in 1988 by Freedom of Information and Protection of Privacy Act.[523] Quebec has two major privacy laws: the Freedom of Information and Protection of Privacy Act[524] and the Municipal Freedom of Information and Protection of Privacy Act.[525] The Commissioner is appointed by the legislature to a 5-year term. The Commissioner is independent, ~~but~~ and reports directly to the legislature. The Commissioner is an officer of the legislature.

The Commissioner only has power over provincial government bodies. These bodies must design and implement records systems that protect personal privacy and assist in locating personal records. The Commissioner monitors activities of the provincial ministries, agencies, colleges, and health district councils. The Commissioner monitors collection, retention, use, disclosure, and disposal of personal information. The Commissioner oversees access to personal records and investigates complaints of privacy violations and refusals to provide information. Decisions by the Commissioner can be appealed to courts. The Commissioner educates the public about privacy rights and comments on legislation and programs, as well as consults ministries, regarding privacy laws. The Commissioner also conducts research on access and privacy issues. The Commissioner has an established fee schedule for requesting access to appeal decisions.

---

[523] The Commissioner's website, at www.ipc.on.ca.

[524] The Freedom of Information and Protection of Privacy Act, as amended, at www.ipc.on.ca/english/acts/prov-act.htm. The regulations for enforcement, Regulation 459, at www.ipc.on.ca/english/acts/prov-reg.htm.

[525] The Municipal Freedom of Information and Protection of Privacy Act, as amended, at www.ipc.on.ca/english/acts/mun-act.htm. The regulations for enforcement, Regulation 823, for the Act, as amended by O. Reg. 395/91; O. Reg. 22/96; and O. Reg. 480/97, at www.ipc.on.ca/english/acts/mun-regs.htm.

4.4.3.5 Quebec, Canada (Provincial Authority)

The Access to Information Commission (Commission d'acces a l'information) was created in 1982 by Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information.[526] Quebec has two major privacy and data protection laws: the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (1982)[527] and the Act Respecting the Protection of Personal Information in the Private Sector (1993).[528]
The Commission has a chairperson and four members. The members of the Commission are appointed by the national assembly to ensure independence. Each member of the Commission must receive approval from at least two-thirds of the national assembly. The Commission acts as an administrative tribunal, an advisory body, and a supervisory body.

The Commission has supervisory and control functions, as well as adjudication functions as an administrative tribunal. The Commission oversees application of and compliance with the Acts by the provincial government departments and agencies, municipalities, educational services, health services, and social network institutions, as well as all private enterprises that supply goods or services. The Commission monitors the proper collection, storage, use, and communication of private data, as well as proper access by individuals to personal data. As an administrative tribunal, the Commission mediates, investigates, and rules on accessibly and privacy claims against both public and private sector organizations. The Commission has full decision-making power in issuing holdings as a quasi-judicial tribunal. The decisions are subject to appeal to courts. The Commission decisions are final on questions of fact. The questions of law can be appealed to the courts. The agency advises both public and private sector bodies about requirements for compliance.

4.4.3.6 Hong Kong

The Privacy Commissioner's Office was created in 1996 by the Personal Data (Privacy) Ordinance.[529] The Personal Data (Privacy) Ordinance gives individuals the right to know whether data is being used, the right to know what that data is, and the right to have incorrect data changed.[530]

The Chief Executive to a five-year term appoints the Privacy Commissioner for Personal Data with the possibility of reappointment for another five-year term. ~~Plus he~~ The Commissioner may be removed from office by the Chief Executive with the approval of the Legislative Council only on grounds of inability to perform or misbehavior. The term of the first Privacy Commissioner expired in 2001 and the commissioner was not reappointed.

---

[526] Available at www.cai.gouv.qc.ca.
[527] The Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (1982), as amended, at www.cai.gouv.qc.ca/en/index_en.htm.
[528] The Act Respecting the Protection of Personal Information in the Private Sector (1993), as amended, at www.cai.gouv.qc.ca/en/index_en.htm.
[529] Available at http://www.pco.org.hk.
[530] Personal Data (Privacy) Ordinance, Ch. 486 (1996), as amended, at http://www.pco.org.hk/english/ordinance/ordfull.html.

The Commissioner reviews proposed legislation. The Commissioner inspects activities and records of Data Controllers. The Commissioner investigates unlawful uses of data, which can result in severe financial penalties or imprisonment. The Commissioner informs the public of data protection rights and policies.

The Office issues Codes of Practice for government agencies, industries, and professions for compliance with the Personal Data (Privacy) Ordinance. The Office maintains a register of approved Data Collectors. Certain categories of Data Collectors are required to make annual reports of their activities.

The Hong Kong Law, like most other national laws, is based on fair information practices. However, the government is exempted from the Act in any case of a "competing social interest."

4.4.3.7 New Zealand

The Office of the Privacy Commissioner was created in 1991 by Privacy Commissioner Act of 1991.[531] That law was updated and expanded by the Privacy Act 1993, which also gave effect to OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[532] New Zealand is considering amendments so that its law will be recognized as adequate by the EU.

The Commissioner is appointed to an initial term of five years and can be reappointed. The Commissioner can only be removed for inability to perform the duties of the office, bankruptcy, neglect of duty, or misconduct. The Office is independent of the Executive. The Office reports to Parliament and can report directly to Prime Minister if necessary. The Commissioner must review operations of the Act every three years. A Deputy Commissioner may also be appointed in the same manner as the Commissioner, if needed.

The Commissioner proposes legislation and reports on proposed laws and policies. The Commissioner makes public statements regarding privacy and monitors activities of information matching programs and public registers. The Commissioner can seek judicial remedies for violations of privacy. The Commissioner has the power to investigate complaints and issue opinions on those investigations. The settlement options include an apology, compensation, and correction of information, restorative action, and granting of access to information. The Commissioner educates the public about information privacy. The Commissioner has the authority to allow exemptions to the privacy guidelines for clear public interest or necessity to an individual. The Commissioner can issue codes of practice for government agencies, industries, and professions. The Privacy Commissioner has issued several industry codes, including an extensive Health Information Privacy Code. With some exceptions, privacy laws apply to government bodies as well as to the private sector.

---

[531] Available at http://www.privacy.org.nz.

[532] The Privacy Act 1993, as amended, at http://www.privacy.org.nz/slegisf.html.

4.4.4 Observations from the 23rd International Conference of Data Protection Commissioners

The 23rd annual international conference of Data Protection Commissioners was held in Paris, France, from September 24-26, 2001. Mr. Robert Gellman was an invited speaker at the Conference, where interviews were conducted with fifteen current and one former data protection official. The interviews included officials from nine different national jurisdictions and seven provincial jurisdictions. The heads of eight national data protection authorities were interviewed, including five major EU member states. Some officials interviewed also have responsibility for freedom of information functions, but questions only covered privacy activities. In order to accommodate requests that some answers be treated as off-the-record, the results of the interviews are reported in aggregate. Because of the limited time and informal nature of the interviews, not all officials were asked all of the planned questions.

Questions were designed to illuminate major subjects such as privacy standards, structure, and effectiveness. Some issues, such as enforcement, were deemed too complex for the type of interviews possible and the available time. The principal questions were:

1. How does the government use your office in privacy matters? Is it consulted in advance? Does the government only listen when the office intervenes? Does the Parliament ask for comments on pending legislation?
2. Are there alternatives to fair information practices as organizing principles for data protection? Are fair information practices the subject of criticism in your jurisdiction?
3. What would you identify as a major success of your office?
4. Are there any structural problems with your office? Do you have sufficient independence to carry out your work effectively?
5. Does your office produce an annual report? Are the reports important to your office, the government, the Parliament, the press, or the public?

~~*4.4.4.1 Follow-up questions and additional probes produced further information that was also useful to this study.*~~

~~4.4.4.2~~4.4.4.1 *Consultation with Government*

Privacy officials appeared to be generally pleased with the use of their offices by their governments and by their Parliaments. In many instances, the data protection law or other policy requires advance consultation with the data protection office on some matters.[533] In one country, failure to consult can be a matter for judicial review, and judicial enforcement has occurred. In another, a minister is obliged to report to the Cabinet whether the privacy office was consulted in advance.

[533] The EU Data Protection Directive requires Member States to provide for consultation with supervisory authorities when drawing up administrative measures or regulations. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data, Official Journal L 281, 23/11/1995, article 28(2).

Consultation with the Parliament is also common, sometime in response to a request from the Parliament.

Even when required, consultations are not always undertaken or conducted with serious intent. Several officials reported that consultations were better and more likely when departments developed a sense that they could trust the data protection office and when they found the office useful. Newer data protection offices sometimes encountered a lack of sensitivity or awareness about privacy. They reported that developing an effective role took time, and improvements over time were nearly universal.

Consultations do not always take place at the formative stage of policy developments, and the privacy office may not be asked for an opinion until later in the process. Sometimes the consultations are pro forma. Consultations may be greater in jurisdictions where privacy is perceived as a major political or popular issue. One official said that maintaining useful contacts with government departments required "constant renewal and refreshment." Most officials recognized formal requirements for consultation were helpful but that to be effective, an office needed to be useful and not simply mandatory.

A lack of consistent consultation seemed to be the most serious problem. No one reported any significant degree of hostility from government, although reactions varied from department to department. Several offices readily admitted neither the government nor the Parliament followed all of their advice. This result was not a surprise to the privacy officials. However, several offices advised that they succeeded in obtaining changes in proposed legislation even when they were unable to stop legislation that they opposed.

~~4.4.4.3~~4.4.4.2 Alternatives to Fair Information Practices

Data protection officials uniformly found FIPs to be the "right way" to define privacy. Support for FIPs is understandable because of the international importance of the OECD Privacy Guidelines and the use of FIPs as the basis for data protection laws. No one reported any meaningful national or other interest in property rights. Some expressly rejected property rights as inconsistent with the view that privacy is a fundamental human right or with the idea of informational self-determination.

While support for FIPs was universal, officials frequently volunteered that "balance" or "common sense" or "pragmatism" in the application of FIPs was important. Privacy offices do not address conflicts over FIPs at the abstract level but in the application of the principles in specific contexts. Achieving the proper balance was the problem and not the principles themselves. Conflict was more common in countries where data protection law was relatively new and a culture of privacy did not yet exist.

Technology-based approaches were not viewed as an alternative to FIPs but as a way to enforce and implement privacy principles. Several officials talked about the need to combine FIPs and technology in a conceptual and practical framework. One official spoke about the need to harness market forces to achieve the right policy result. This view did not represent a rejection of FIPs, but

the official wanted to consider how market forces might further the desired policy. The official saw privacy rules, like other government policies, as encumbering private rights so that rules and enforcement had to be properly tailored to the circumstances. One official mentioned the role of self-regulation, but as an alternate enforcement method rather than a new set of fundamental principles.

~~4.4.4.4~~4.4.4.3 Privacy Office Successes

Some officials pointed to specific activities as particular successes. Some of these activities were winning or influencing legislative battles, developing codes of practice, influencing governmental proposals, assisting local governments in implementing data protection policies, or making progress with specific policy proposals.

The most common answer, however, was to point in some fashion to the data protection office's routine functioning in carrying out its basic mission. It is the "normal operation" of the office that was noteworthy. Some broadened this view to the growth of public and political interest in privacy. One official pointed to the "political importance of privacy as a fundamental value." Another said that the "cultural shift" in public attitudes toward privacy was a success.

Another thought that "making sure that privacy was considered at all governmental levels" was a significant accomplishment. One official thought that the public perception, backed by polls, that the office was "regarded as objective" was noteworthy. Several newer offices that were not yet fully operational or were brand new pointed to the establishment of the office as a particular success. One cited an increased budget as a sign of success. Another official from a small jurisdiction noted that the commissioner's function started as a part-time position, and the office now had a staff of three.

Not everyone said that public or political concern about privacy was necessarily at a high level. Nevertheless, most officials seemed to be pleased with their ability to have an influence on government and on public opinion. Overall, there was a sense of political reality; with officials recognizing that having an effect was as important or more important than the resolution of any particular issue.

~~4.4.4.5~~4.4.4.4 Structural Problems

This broad question was almost uniformly interpreted as an inquiry into the degree of independence that the office had. The EU Directive requires that supervisory authorities act with "complete independence" in carrying out their missions.[534] No data protection official reported any problem with his or her degree of independence. One said that the office had "plenty of independence" and that view was universal. Another said that the office was "remarkably independent" and that the power of independence was "used to the utmost" in carrying out its mission.

---

[534] *Id.* 28(1).

A few officials also reported on the need for bigger budgets, but this point was not pursued because the need for more resources is too common a problem in government agencies. No one reported being starved for resources. One provincial official wanted to have greater jurisdiction over private sector privacy issues. Several others thought that their laws could be fruitfully amended to make smaller order adjustments in operations, enforcement, or authority.

~~4.4.4.6~~4.4.4.5 Annual Reports

All data protection officials stated that their offices produced an annual report. Most felt that these reports were "important," "very important, or "key." A few questioned the value of the report. One found the report to be a "pain" but still "useful." One stated expressly that the report was "not important" and provided "no return" for the effort. That was a distinctly minority view. One office does a biennial report and thought that reporting annually might be too frequent.

Annual reports are important for a variety of reasons, and most officials gave more than one reason. External uses include review of the report by the Parliament for oversight of the privacy office. The government sometimes reviews reports, as do particular departments that are the subject of discussion in the report. Annual reports may receive more attention in smaller jurisdictions. Some officials said that the report attracts significant interest by the news media and by the public. However, external interest varies considerably from country to country. In some countries, for example, the data protection office's annual report is invariably the subject of a hearing before a parliamentary committee. In other jurisdictions, Parliament ignores the report. Press interest is also highly variable. To the extent that the annual report summarizes previous activities, it may be seen as old news.

Some uses of the annual reports are internal. The report is a useful "historical document" or "forces the office to consider its own work." Preparing the report provides some offices with an opportunity for internal assessment and for planning.

One official said that the report had lost some of its importance as a public communications tool because of the Internet. Information about current activities can be easily posted on the office's website throughout the year. By the time the annual report appears, everything in it is old news. Whether the Internet will affect the importance of the data protection annual report elsewhere remains to be seen, but it is a development worth watching.

~~4.4.4.7~~4.4.4.6 Conclusions from Interviews of Commissioners

It is difficult to offer broad or definitive conclusions based on the limited interviews. Impressions are distinctly one-sided because interviews did not include any of the companies or government agencies regulated, monitored, or overseen by the data protection authorities. It is impossible to assess the success or operations of any specific office. Nevertheless, a few observations include the following.

The offices interviewed range in age from recently established to well established. The interviews suggested a sense of development. Newer offices were learning the best strategies for making

themselves useful and for educating others in government as well as the press and the public about addressing privacy. Older offices may have been more adept at waving the privacy flag in visible and useful ways. One official reported having a "network of journalists" that could be counted upon to bring matters to public and governmental attention. Another noted that scandals are especially valuable in attracting public attention, a point well recognized in the United States.

Independence is important to these data protection offices. Being able to criticize the government is essential because government actions have major effects on privacy. Independence by itself, however, does not bring influence or guarantee success. Data protection offices need to cultivate a sense of trust so that other governmental components – as well as private sector companies – will work cooperatively with them. However, the ability to speak publicly and independently remains important. One national office recently adopted a more confrontational tone, and this is generally viewed as unusual. The results are sure to be carefully watched by other data protection officials. There is insufficient evidence to assess whether the budgetary process imposes a restraint on independence.

Nothing in the interviews suggested that FIPs have become outdated, irrelevant, or unimportant. Every official recognized the value of FIPs, and no one offered an alternative standard for identifying the elements of privacy. The interviews revealed an express recognition among data protection officials that applying FIPs in the real world requires common sense and balance. Several officials see technology and self-regulation as methods for achieving privacy objectives, but no one suggested that these approaches would offer independent standards for privacy. FIPs remain relevant and central to privacy.

Privacy offices win some battles and lose others. The limited evidence collected suggests that the offices savor their successes and seek to apply their resources where they can be most effective. There were some hints that offices recognize they are fighting long-term battles and that they need to live to fight again another day.

Annual reports are important in the data protection world. They provide a way for offices to speak to their governments, to the press, to the public, and to each other. External interest in annual reports varies considerably from country to country.

Other still-tentative conclusions were suggested by the conference itself. First, data protection officials learn from one another. Activities and developments in one country or area help others to finds responses to common problems. This is particularly true for new technologies. Several conference sessions considered current technological threats to privacy, such as biometrics, face recognition, location techniques (e.g., determining the location of a cell phone), as well as technologies for privacy protection. It is common for the annual conferences to consider changes in technology. Several data protection offices cooperate in assessing new technologies and share the results widely on the Internet for use by other offices and by the public.

Second, the annual conferences are important for building relationships and fostering understanding of common challenges in the data protection community. The world of data protection is still a small world, and most officials know most of their colleagues. Networking and cooperative activities are routine and valuable. Occasionally, the United States has been formally represented at the annual conferences, but rarely by the same person or office. The absence of a regular official contact with the United States leaves foreign officials to listen more to privacy advocates and other U.S. participants. Mozelle Thompson, Commissioner at the Federal Trade Commission, was the only representative of the U.S. government on the program, and he is a Democrat who did not represent the Bush Administration.

Third, this was the first data protection conference where the national sponsor made a special effort to invite representatives from third world countries. Invited speakers included representatives from Burkina Faso, Mali, Senegal, and Argentina. The broader international participation helps to foster international recognition and acceptance of the common principles on which most data protection laws are based. Countries that are just deciding how to approach privacy is more likely to look at existing and actively promoted data protection models for guidance.

Fourth, data protection is clearly recognized by the private sector to be an international issue. Conference attendees included corporate data protection officials from many countries, and speakers included the CPO from Microsoft, the Chief Data Protection Officer from Daimler Chrysler, and comparable officials from Intel, AOL Time Warner, and other companies. The multinational corporate presence underscored the increasing internationalization of privacy. Presentations considered the challenges of addressing privacy on worldwide Internet sites.

Finally, data protection has become institutionalized in most parts of the industrialized world. Independent offices in most countries other than the United States oversee and implement data protection laws. Government support remains adequate. Support for data protection in France might be measured by the high-ranking officials who participated in the conference. French President Jacques Chirac was scheduled to speak by video teleconference, although current events prevented him from appearing. Chirac's remarks were presented to the conference anyway. French Prime Minister Lionel Jospin delivered the closing address in person. The Chairman of the National Assembly and the Mayor of Paris each sponsored and attended conference receptions.

Professor David Flaherty, the author of an academic study of data protection agencies and who later served as Information and Privacy Commissioner for the Canadian Province of British Columbia, expressed concern in his 1989 study that the agencies would not be effective in carry out their mission:

> The harsh reality is that data protectors run the risk of being only a tiny force of irregulars equipped with pitchforks and hoes waging battles against large technocratic and bureaucratic forces equipped with lasers and nuclear weapons.[535]

[535] *Id.* at 393 (1989).

It appears that data protection has fared better than Professor Flaherty feared.

4.4.5 Summary of International Structures

Through the Data Protection Directive, the EU has established a standard system for privacy and data protection that has had an impact not only on EU member nations, but on many other nations as well. A significant number of non-EU nations have implemented privacy and data protections to match the requirements of the EU Data Protection Directive. Many of the non-EU nations that do not have legislation directly based on the Data Protection Directive are nevertheless amending and modifying their laws to comply with the EU requirements.

This subsection, in providing summaries of these national structures and enabling laws, is not intended as a critique or a comment on the overall effectiveness of one type of structure over another. However, the pervasive influence of the EU Data Protection Directive and its principles of privacy and data protection on international law cannot be understated. The most common structure on the international level is clearly one that meets the requirements of the EU Data Protection Directive.

4.5 Corporate Structure

Currently, most organizations that have decided to address privacy issues – and many do not have privacy policies – do so on a voluntary basis. Private sector privacy laws regulate limited aspects of data processing activities for the financial sector (including the credit reporting industry), cable television providers, video service providers, and some telecommunications operations. Portions of the health care sector will be covered in 2003 by a federal privacy law. Voluntary privacy activities by corporations and other organizations sometimes include:

- Creation of the position of a chief privacy officer or privacy office to consolidate, focus on, and address privacy concerns.
- Development and deployment of Privacy Enhancing Technologies (PETs) that can mitigate misuse or abuse of personal information or provide individuals with a greater ability to control the use and disclosure of their personal information.
- Establishment of trade association guidelines or codes of conduct for dealing with consumer privacy.
- Development of privacy seal programs that establish privacy standards and offer privacy dispute resolution services.

A review of each of these initiatives (excluding the discussion of PETs, which is provided in Section 2. Fair Information Practices and Other Approaches to Privacy) is provided in the following subsections.

4.5.1 Chief Privacy Officer

The CPO position surfaced in the late 1990s as privacy issues took on greater importance as a result of legislative, consumer, and international pressures. Some organizations, including healthcare organizations, large financial institutions, technology enterprises, dot-coms, and interactive media companies created the CPO positions. One advantage of having a CPO is that privacy is the primary focus of someone's job. Privacy tends to be an issue that cuts across traditional lines of responsibility in any organization. The legal department handles legal issues, customer service resolves consumer complaints, information technology departments plans and operates networks, systems, and databases, and separate offices may handle physical and technical security. Privacy issues can arise in any and all of these places. The lack of clear responsibility for privacy may also mean that privacy can be more easily ignored.

The idea of a CPO may have originated in Germany, where the data protection law has for many years required most organizations to designate a privacy officer. The only comparable requirement in U.S. law can be found in the Health Insurance Portability and Accountability Act (HIPAA), which will require many health care organizations to designate a privacy officer. The HIPAA requirements will not take effect until 2003, but some organizations have already appointed privacy officers to assist in preparation for compliance with the Act. Gramm-Leach-Bliley (GLB), a recent privacy law affecting financial institutions, encouraged some banks and other covered entities to create CPOs to manage compliance, but GLB does not require that covered organizations have a CPO.

Federal agencies are not required to have CPOs, although a few have comparable offices and positions. In 1998, President Clinton ordered the heads of each departments and agencies to designate a senior official within the agency to assume primary responsibility for privacy policy.[536] Informal reports suggest that the designation of a senior privacy official did not result in any meaningful change in many agencies. The new title did not necessarily bring with it new staff, resources, or defined responsibilities.

The CPO appears to be a significant and substantive function in some private sector organizations. In early 2001, it was estimated that there were 200 to 300 CPOs, and it is anticipated that the number could jump up to tens of thousands by 2003, when all entities regulated by HIPPA must be compliant[537]. As Richard Purcell, the CPO at Microsoft Corporation, noted, "This position represents a transition to an active corporate stance on privacy. It's no longer a case of defensive risk management, but a recognition that privacy is a product that establishes our organization's credibility and trust with consumers and society."[538]

---

[536] Presidential Memorandum for the Heads of Executive Departments and Agencies on Privacy and Personal Information in Federal Records, May 14, 1998.

[537] Maria Trombly, *New York Life Names Chief Privacy Officer,* Computerworld (April 23, 2001), at http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59897,00.html

[538] John Goff. *CPO Sharpies: Chief privacy officers work to establish credibility and trust with consumers and society,* eCFO, (September 2000), at http://www.ecfonet.com/articles/al_cpo_sharpies.html.

There is some evidence that the CPO position in some organizations is only a figurehead used in corporate public relations to assuage consumer's fears of abuse and invasion of privacy. Some CPO positions have been called "celebrity CPOs". However, it is impossible to assess the overall situation, and it is certain that a wide variation in the legitimacy of CPOs can be found. Without question, many CPOs represent sincere efforts by organizations to deal with privacy matters.

4.5.1.1 Chief Privacy Officer Structure

In some instances, the CPO functions as an arm of the legal department and reports to the general counsel. In larger companies, usually financial and healthcare organizations, the CPO may be an entity unto itself with a dedicated staff and may report directly to the Chief Executive Officer (CEO) or the CIO.

PricewaterhouseCoopers conducted an informal survey[539] of 66 companies to identify strategic positioning of CPOs. Forty-seven percent of the companies reported that the CPO was part of the Office of the General Counsel or legal department. The CPOs of the other companies were evenly spread across other divisions, such as engineering, ethics office, marketing, senior management, e-business, and government affairs.

The key to the effectiveness and influence of the CPO is directly related to their reporting structure, and a major question is whether they sit at "the table". Two authors from the Computer Professionals for Social Responsibility (CPSR) Privacy Working Group identified two qualities that the CPO reporting structure should retain:[540]

- Internal legitimacy – appropriate enterprise-wide scope and the opportunity to offer meaningful executive opinion on organizational activities involving privacy.
- External legitimacy – to ensure that the position is not perceived by the public to be one of a straw man.

A CPO's responsibilities can vary significantly from company to company. A CPO may address internal and external privacy issues within all stages of the business, from business development and strategic partnerships to interactions and compliance with government agencies. A CPO may also coordinate with other corporate entities to ensure compliance, such as the IT security managers to protect the IT architecture, and Human Resources for training of appropriate staff. Others potential areas of responsibility can range across many lines of business for an organization, including:

- Product design and development,

---

[539] Ruth Nelson, Anne Ladd, *The Chief Privacy Officer: PricewaterhouseCoopers Surveys an Emerging Role,* PricewaterhouseCoopers Insights & Solutions Web page (November 2000), at http://www.pwcglobal.com/extweb/manissue.nsf/DocID/BD73BCD4420B713E85256A640048E4C0.

[540] Keith P. Enright, Esq. and Michael McCullough, J.D. on behalf of the Computer Professionals for Social Responsibility's (CPSR) Privacy Working Group, *The CPO Guidelines Presentation,* (May 4, 2001), at http://privacylaw.net/cpo_guidelines.htm.

- Information collection and use practices,
- Corporate administration,
- Public and government relations,
- Privacy compliance, and
- Employee privacy.

The responsibilities and placement of the CPO position may depend in part on the size of the organization, any relevant legislative mandates, the industries in which a company participates, and available resources. For example, the privacy rules for health care providers, payers, and clearinghouses issued by the Department of Health and Human Services (HHS) under the HIPAA requires that covered entities designate a *privacy official*.[541] HHS commentary on the rules states that not every covered entity must have either a full-time privacy official. It also gives covered entities complete flexibility in the placement of the function.[542]

In response to the HIPAA requirement, the American Health Information Management Association (AHIMA) developed a sample position description for the Privacy Officer[543]. While intended for the healthcare industry, the AHIMA description nevertheless offers a comprehensive list of objectives and actions to be performed by any organization's privacy office or official. The range of skills and diversity of functions implied by the AHIMA description is especially noteworthy. According to AHIMA, a CPO:

- Provides development guidance and assists in the identification, implementation, and maintenance of privacy policies and procedures in coordination with management and administration, the Privacy Oversight Committee, and legal counsel.
- Works with organization senior management and corporate compliance officer to establish an organization-wide Privacy Oversight Committee.
- Serves in a leadership role for the Privacy Oversight Committee's activities.
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.
- Works with legal counsel and management, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

---

[541] 45 C.F.R. §164.530(a)(1)(i).
[542] 65 Fed. Reg. 82744 (December 28, 2000).
[543] Sample (Chief) Privacy Officer Job Description, American Health Information Management Association, at http://www.ahima.org/infocenter/models/PrivacyOfficer2001.htm.

- Oversees, directs, delivers, or ensures delivery of initial and privacy training and orientation to all employees, contractors, alliances, business associates, and other appropriate third parties.
- Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- Establishes with management and operations a mechanism to track access to protected information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity.
- Works cooperatively with other applicable organization units in overseeing an individual's rights to inspect, amend, and restrict access to protected information when appropriate.

Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
- Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.
- Reviews all system-related information security plans throughout the organization's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.
- Works with all organization personnel involved with any aspect of release of protected information, to ensure full coordination and cooperation under the organization's policies and procedures and legal requirements.
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Serves as information privacy consultant to the organization for all departments and appropriate entities.
- Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Works with organization administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

In some organizations, some of these duties are likely to be assigned to positions other than the CPO, such as the information systems manager or the legal counsel.

The real significance of the development of CPOs is the recognition that privacy is an issue of continuing importance to an organization. It is less important whether responsibilities and functions are transferred directly to the CPO or whether the CPO coordinates privacy related activities that are carried out by other parts of the organization. A CPO is essentially an acknowledgement by an organization that privacy must be managed in order to protect the organization's customers and employees, as well as the organization's own interests.

4.5.1.2 Chief Privacy Officer Qualifications and Challenges

An ideal CPO may be an individual with a broad background and an understanding of an organization and its business. Many CPOs have legal or compliance backgrounds, and it is increasingly useful for a CPO to have an IT background, or at least a understanding of technology and its use. A CPO may be asked to audit and assess the information systems and the data flows across the organization and between business partners, and to evaluate the privacy implications of such information flows. Michael Lamb, AT&T's CPO and lawyer, believes that a legal background is an asset to a CPO when it comes to interpreting privacy laws, but legal expertise does not take the place of technical expertise when it becomes necessary discuss the intersection of technology and privacy with IT managers. On the other hand, Thomas Warga, Senior Vice President and General Auditor for Compliance at New York Life Insurance, who functions as the CPO, believes that the advantage of having an audit background is broad knowledge of the entire management team, which makes it easier to pursue privacy initiatives. As with any position, people with different skills bring different advantages to the position. Some suggest that the person who fills that role should be well versed in seven key areas: information technology, auditing, company policies and practices, ethics, state regulatory agencies, federal laws, and consumer issues.[544] Individuals with all of those talents may well be hard to find.

Organizations face numerous challenges to implementing privacy policies and procedures, and to establishing a privacy office or CPO position. Many organizations are struggling to identify the role of the new position within the existing organizational structure. Some industry analysts feel that corporations have not made the necessary cultural and organizational changes, and that this position must be given more importance, authority, and senior management support to effectively protect the company and consumer information.[545]

---

[544] Steve Alexander, *The IT-CPO link – The chief privacy officer works closely with the IT department – but will an IT professional ever hold that office?,* InfoWorld (September 10, 2001), at http://www.findarticles.com/cf_0/m0IFW/37_23/78053011/print.jhtml.

[545] A. Hallawell and T. Hicks, *Chief Privacy Officer: Corporate Fad or Permanent Fixture?,* Gartner Research, Strategic Planning, SPA-13-3180 (April 17, 2001).

The biggest challenge for the CPO is to understand and control how personal data is used in everyday business practices and within Information Technology (IT) systems, and develop policies that the company will adhere to in all areas of the business.

4.5.2 Corporate Privacy Policies

Many corporations are creating and posting privacy policies driven by legislation or consumer fears. Federal legislation, such as the Gramm-Leach-Bliley Act requires financial service firms to have privacy policies and to send notices to customers. Firms have had difficulty in providing straightforward, simple privacy policies. Citicorp Inc., addressed the problem by creating two versions of their privacy policy, one that met the requirements of the law, and another that provided 10-points of the program in a "plain English" version easier from the public to understand.[546]

Numerous studies and reports have shown that consumer concerns over privacy and the use of their personal information affected their use of the Internet and online business. According to Forester Research, privacy fears cost U.S. businesses approximately $12.4 billion last year in lost online sales.[547] Industry associations are advocating clear and simple privacy policies that inform and provide choice to the consumer in regard to the information collected about them and how that information is used. At the Privacy and Data Protection Summit in May 2001, U.S. Federal Trade Commissioner Sheila Anthony stated that "many privacy policies are beginning to look like complex legal documents that do not give consumers real choice", and that there "was a tendency among some companies to establish privacy policies that grant companies sweeping rights to sell and transfer customer data".[548]

Whether the often-limited privacy policies are effectively meeting the needs of consumers remains unclear. More substantive privacy policies sometimes create problems in another direction. Privacy policies are a complicated area and this subsection only provides a high-level review of the subject. Corporate privacy policies and their efficacy is fertile ground for more research and analysis that could provide noteworthy information and lessons learned for federal agencies.

4.5.3 Industry Codes

Some industry associations are addressing privacy concerns by establishing best industry standards and practices. Trade association privacy codes of conduct are typically specific to an industry. In 1998, the FTC requested and received nine industry-specific online information practice guidelines and principles in an attempt to gauge the status and effectiveness of current self-regulatory efforts.[549] The FTC found that the guidelines do not address all of the core fair information practice principles, but all encourage companies to provide notice of at least some of their information practices, and most encourage choice with respect to the disclosure of personal information to third

---

[546] Patrick Thibodeau, *Corporate privacy policies scrutinized,* ComputerWorld (May 4, 2001), at http://www3.cnn.com/2001/TECH/industry/05/04/corporate.privacy.idg/.

[547] Tischelle George, *Say Hello To Your Friend, The Chief Privacy Officer*, InformationWeek.com (May 14, 2001), at http://www.informationweek.com/837/ethics_cpo.htm.

[548] *Id.*

[549] 63 Fed. Reg., 10,916 (1998).

parties. For the most part, the submitted guidelines do not address access or security. Most importantly, very few provide any kind of enforcement mechanism, an essential element of effective self-regulation."[550] The following groups are some of the more prominent in privacy concerns and industry codes:

- Direct Marketing Association (DMA) is the largest trade association for direct mail and marketing companies.
- Online Privacy Alliance (OPA) is a group of corporations and associations that introduce and promote business-wide actions that create an environment of trust and foster the protection of individual's privacy online. The OPA has also "undertaken a campaign to nip Internet-privacy legislation in the bud…by identifying expensive regulatory burdens, raising the issues of U.S. Internet law on non-Internet industries, and assuring lawmakers that privacy is best guarded by new technology, not new laws."[551]
- Coalition for Advertising Supported Information and Entertainment (CASIE) has formulated "Goals for Privacy" to serve as a framework for marketers to address consumers' privacy as the virtual marketplace grows.

Despite the adoption of these principles, there is currently no independent information about how well these procedures and practices are working or what level of industry compliance has been achieved. Furthermore, industry coalitions are not always able to reach a consensus on all aspects of privacy, as seen when members voice a different opinion from the organization. For example, America Online and Intel advocate baseline privacy rules, but Experian and Microsoft are currently not in favor of federal legislation, yet all belong to OPA.[552]

4.5.4 Seal Programs

There are several seal programs that online organizations can join to "certify" that they protect their customers' privacy. All of the programs provide guidelines that a member organization must comply with and a mandatory dispute resolution process. The origins of the web seal concept started in March 1996, at a PC Forum's lecture on trust, when two attendees "espoused the need for branded symbols of trust on the Internet similar to the UL Labs or Good Housekeeping seals of approval".[553] The three most recognized seal programs are:

- BBBOnline is a seal program offered by the Better Business Bureau that helps consumers finds reliable companies that pledge to meet tough advertising and dispute settlement standards, including responsible advertising to children.

---

[550] *Privacy Online: A Report to Congress*, Federal Trade Commission (June 1998), at http://www.ftc.gov/reports/privacy3/industry.htm#Industry%20Association%20Guidelines.
[551] Ted Bridis, *High-tech titans put the squeeze on privacy regs*, Wall Street Journal Online (March 13, 2001), at http://slashdot.org/article.pl?sid=01/03/13/157259&mode=thread.
[552] Doug Brown, *Corporate Privacy: Disunited Front*, Interactive Week (March 20,2001), at http://www.zdnet.com/zdnn/stories/news/0,4586,26981,00.html.
[553] Raphael Franze, *Privacy Standards for Websites: Web Seals*, The Internet Law Journal (February 5, 2001), at http://www.tilj.com/content/ecomarticle02050103.htm.

- TRUSTe is an online privacy seal program that offers advice and information about online privacy. The TRUSTe Privacy Seal, or "Trustmark," program awards seals to responsible websites that meet privacy policy requirements and enforcement criteria. For compliance with the program, the website must post a privacy policy that gives full disclosure of how the information is used, meaningful choice to the customer, reasonable access and security to the information.
- WebTrust is a certification program whereby Certified Public Accountants (CPAs) verify the security systems of participating web sites every 90 days and awards icons of certification and approval.

As of April 2001, "it did not appear that any major online seal program has ever revoked seal privileges, although there were dozens of complaints that merited careful examination. A privacy seal, in the end, means only that you pay dues for a seal."[554] Other limitations of seal programs are illustrated by the Toysmart case.[555] Toysmart was a TRUSTe seal holder. When the company went bankrupt, maintenance of the seal no longer had any importance to the company, and it planned to sell a customer list in violation of its privacy policy. TRUSTe notified the Federal Trade Commission, and the Commission intervened and reached a settlement with the company. The settlement then drew objections from a coalition of 40 state attorneys general. The matter was ultimately resolved when a buyer paid for and retired the list. The case also illustrates the complexity of privacy matters that attract considerable public attention and formal agency involvement.[556]

Despite the standards that the participating company must adhere to, the efficacy of the seal programs and their enforcement mechanisms has yet to be determined. In a Joint Project of the Ontario Office of the Information and Privacy Commissioner and the Office of the Federal Privacy Commissioner of Australia on Web Seals, they generally concluded:

> "[t]hat each of the three assessed seals addressed privacy protection, dispute resolution and compliance/enforcement to some degree, although none of them completely satisfactorily. The web seal evaluation project found that each of the seals had its own strengths. For example, although all of the seals performed well in relation to our dispute resolution assessment, BBBOnLine probably offered the most customer-friendly dispute resolution system (scoring five out of six in our assessment). WebTrust probably offered the most rigorous compliance regime. In terms of privacy principles, while

---

[554] Peter Seebach, *The cranky user: Respecting user privacy, Part 3,* IBM DeveloperWorks (April 2001), at http://www-106.ibm.com/developerworks/usability/library/us-cranky5.html.

[555] Available at www.ftc.gov/opa/2000/07/toysmart.htm.

[556] Raphael Franze, *Privacy Standards for Websites: Web Seals*, The Internet Law Journal (February 5, 2001), at http://www.tilj.com/content/ecomarticle02050103.htm.

> TRUSTe scored the highest in our assessment, it was clear that none of the seals required their participants to meet all of the OECD principles."[557]

4.5.5 Corporate Structures Conclusion

Since the mid-1990s, corporate America has been forced to face numerous privacy-related issues due to advances in information technology, the proliferation of online business transactions, increased litigation over privacy, international pressures, and some new federal and state legislation. It is no longer sufficient that organizations take a reactive stance to the collection and use of customer's personal information. Rather to protect their reputation, revenues, and consumer trust, organizations must be proactive to the fears and abuses of private information for both the corporation and their customers.

Although protecting corporate secrets has always been part of the business landscape, the recent privacy initiatives have more to do with protecting the bottom line by retaining customer loyalty. Because privacy is of such a concern for consumers (e.g., constituents), especially online consumers, many companies fear that federal and state politicians will take the reins of privacy protection if they do not do something now. CPOs, privacy policies, PETs, industry guidelines, and seal programs may be partly responses to political pressures, and where this is so, it is not clear that they will make those pressures go away.

Many feel that not enough has been done regarding self-regulation of privacy in the commercial arena. Because privacy is a nascent idea, corporate practices and procedures are still emerging, as Harriet Pearson, IBM's CPO notes, "only a few years ago, many companies had no privacy policies, and today there are ongoing industry initiatives to improve policies."[558]

It's too early to fairly or comprehensively evaluate the CPO movement, since there are not enough facts or experience in this arena. The development of the CPO position can be viewed as recognition by some organizations of the importance of privacy and of privacy management. Some corporate privacy activities are responsive to international pressures and to multinational activities.

Like the corporations that are establishing CPOs, government agencies face complex privacy issues that cut across traditional agency lines. Internet technology is pervasive in government as it is in corporations, and the pressures to address privacy may be similar. President Clinton required every agency to designate a senior privacy officer, but in many instances, this was just a figurehead type of activity, much like the celebrity CPOs.

---

[557] A Joint Project of The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, *Web Seals: A Review of Online Privacy Programs*, presented at the 22nd International Conference on Privacy and Personal Data Protection, Section 5.1, Venice, Italy (September 2000), at www.noie.gov.au/projects/consumer/roundtable/webseals_comparative_table.htm.

[558] Patrick Thibodeau, *Corporate privacy policies scrutinized*, ComputerWorld (May 4, 2001), at http://www3.cnn.com/2001/TECH/industry/05/04/corporate.privacy.idg/.

States are not necessarily the only "laboratory" to be studied. Government may have something to learn from corporate CPOs. It remains to be seen just what, of course, but CPOs may offer one approach to addressing privacy in a complex bureaucratic and legal environment. Further research and analysis of the CPO position, and corporate privacy principles and practices, and industry self-regulation could prove to be insightful for federal agencies.

4.6 Analysis of Approaches to Structure

This section brings together the preceding information about structures to analyze a set of representative current approaches to the structure of privacy protection. The approaches are detailed examinations of the operations of current privacy and data protection structures by selected states or countries.

For each structural approach that follows, a textual summation of the approach is provided along with an operational diagram depicting how the approach functions. Each review concludes with a distillation of the primary characteristics of the approach as it is applied. Overall, this section shows that there are significant variations in the way in which states and countries have organized themselves to deal with privacy laws and issues. The way in which a state or country organizes itself has important implications for the implementation of that state's or country's privacy laws and policies.

4.6.1 Canada: A Federal-Provincial Approach

As reflected in Figure 4.2, Canada's federal-provincial approach places the national agency apart from the rest of the government in function and also features separate provincial privacy agencies. Although the Commissioner of Canada's national privacy agency is appointed by the Governor in Council and the House of Commons and the Senate, the agency works independently of the legislature and the executive branch. The Commissioner is an officer of Parliament and reports to the House of Commons and the Senate.

As the following diagram reflects, the national agency investigates privacy complaints from both the public and private sectors at the national level, and attempts to act as a mediator to resolve issues. The national agency also encourages organizations to develop codes of privacy. The national agency works parallel to the provincial privacy agencies. These provincial agencies oversee application of and compliance with provincial data privacy laws by the agencies and departments of the provincial and local governments within the province. The privacy institutions in Canada were created in a decentralized manner, as the provincial agencies were created independently of the national agency.

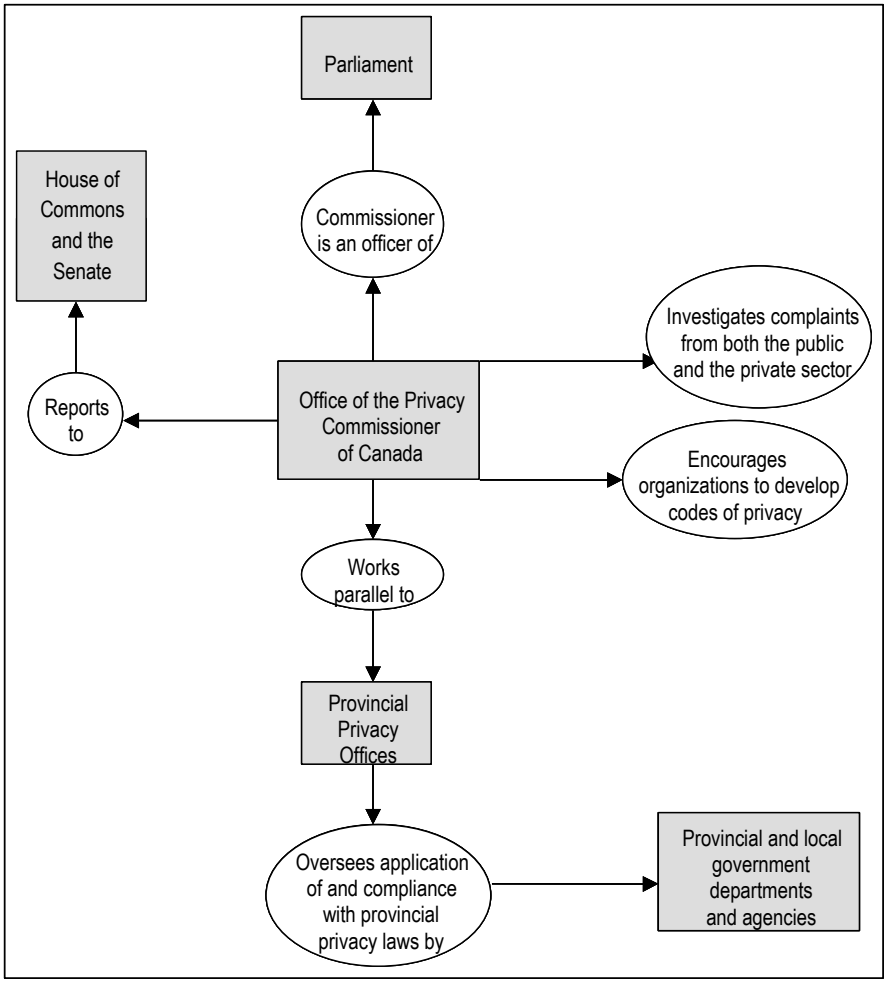


Figure 4.2 Canada's Federal-Provincial Approach

The federal-provincial approach has important characteristics at both the federal and provincial level. At the federal level, the characteristics of this approach include:

- Commissioner is independent, but is an officer of Parliament
- Reports to the legislature
- Works with both public and private organizations at national level
- Encourages development of privacy codes

- Works parallel to provincial agencies

At the provincial level, the characteristics of this approach include:

- Responsible for intra-provincial matters and local government agencies
- Works parallel to federal agency

Overall, Canada's federal-provincial approach has the benefit of providing privacy and data protection rights at both the national and the regional levels; however, the approach has the potential to cause problems if the federal and provincial privacy agencies do not cooperate.

4.6.2 California: A Bureaucratic Approach

The bureaucratic approach embeds the privacy agency within several levels of the government, creating a system of reporting procedures throughout the government structure. Figure 4.3 shows that California's agency is placed within a consumer protection department that reports to a member of the cabinet, who in turns reports to the governor regarding the activities of the privacy agency. The agency issues annual reports to the legislature as well. From within this hierarchy, the agency makes recommendations to public and private organizations about privacy issues. It also provides advice, information, and referrals about privacy issues to members of the public. Additionally, the agency has other functions within the state bureaucracy, such as facilitating training of state and local law enforcement officials and assisting in investigations and prosecutions for identity theft.

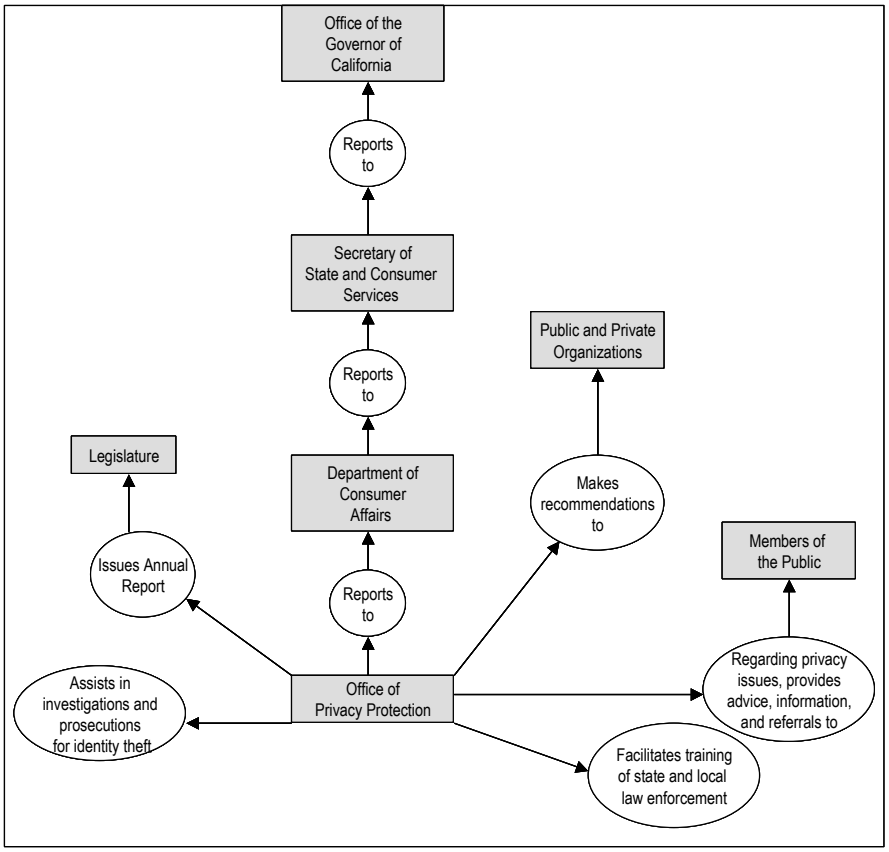


Figure 4.3 California's Bureaucratic Approach

The important characteristics of the bureaucratic approach include:

- Placement within bureaucratic hierarchy
- Makes recommendations to public and private organizations
- Reports to the legislature
- Provides public information services
- Provides training services to other state agencies

The efficiency and effectiveness of a bureaucratic approach depends heavily on the exact placement of the agency within the hierarchy; the powers, mission and resources it is given; and how restricted it is by the bureaucracy.

4.6.3 Connecticut: An Oversight Commission Approach

Connecticut's oversight commission works with members of the public, the government agencies, the legislature, and the executive to oversee freedom of information issues principally and some privacy issues. Though the governor appoints the commission members, the commission is not attached to any part of the government. It advises the legislature on privacy issues. As Figure 4.4 reflects, the public can file complaints with the commission regarding public records problems with state agencies—problems that may sometimes involve privacy issues as well. The commission may act as an ombudsman between the public and the state agencies. The commission also oversees compliance with privacy laws by the state agencies, and the commission can hear claims about and issue orders to the agencies to compel compliance. These orders may be appealed to the judiciary.

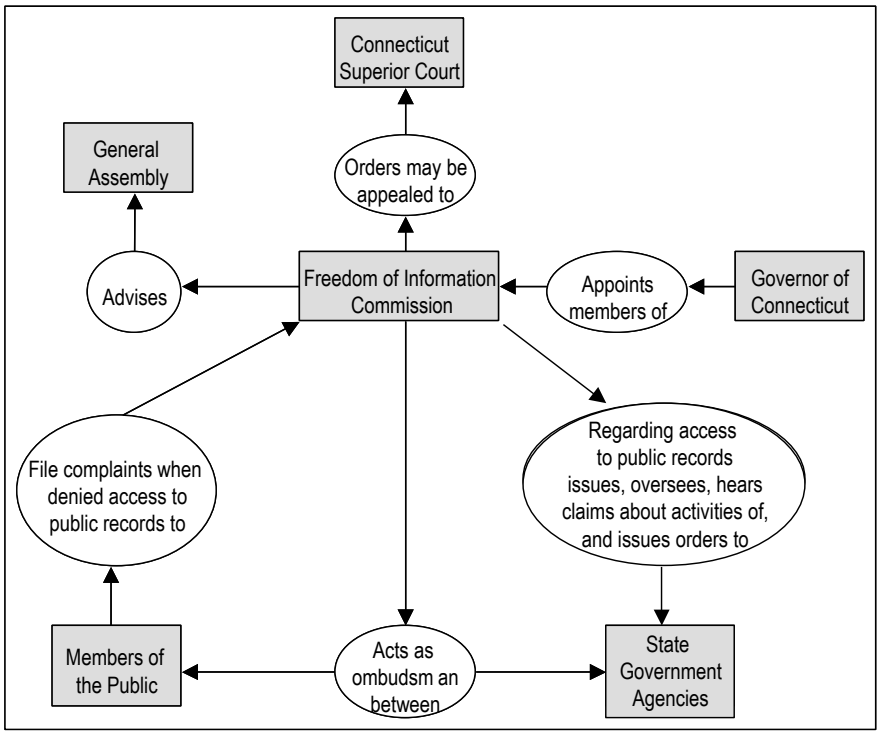


Figure 4.4 Connecticut's Oversight Commission Approach

The important characteristics of the oversight commission approach include:

- Appointed by the executive branch
- Orders can be appealed to the judiciary

- Advises the legislature
- Hears complaints filed by members of the public
- Acts as an ombudsman between the public and state agencies
- Can issue orders to state agencies compelling compliance

The effectiveness of an oversight commission approach depends greatly on the extent of its enforcement powers and resources, as well as the degree to which those enforcement powers and resources are exercised.

4.6.4 The European Union: A Harmonizing Extranational Approach

The European Union member states created the Council and Parliament of Europe to act as the legislative body for the EU. The Council and Parliament passed the Data Protection Directive, which places affirmative obligations on the member states. These affirmative obligations are designed to harmonize national laws that provide privacy and data protection rights for the citizens of each member state. As Figure 4.5 depicts, the Data Protection Directive dictates that each member state must create a national supervisory authority to oversee privacy and data protection. One representative from each state's national supervisory authority is a member of the Directive's Article 29 Working Party, which monitors application of the Data Protection Directive. The Article 29 Working Party also makes recommendations regarding the implementation of the Directive to the Article 31 Committee, which drafts additional measures for implementation of the Directive when necessary. The Article 31 Committee reports to the Council and Parliament, which has review power over the decisions of the Article 31 Committee.

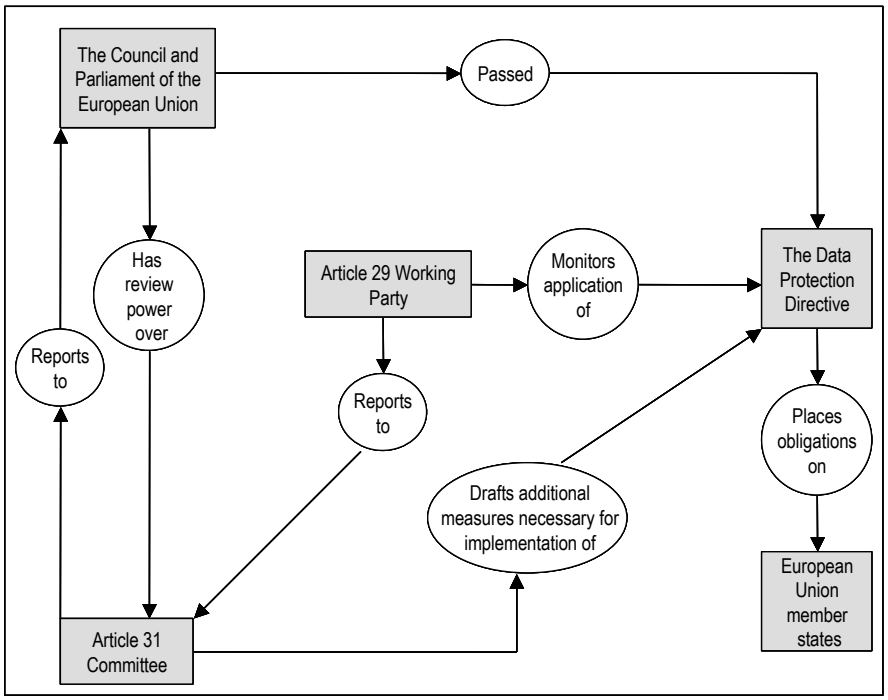


Figure 4.5 The EU's Harmonizing Extranational Approach

The important characteristics of the harmonizing extranational approach include:

- International agreement on privacy standards.
- Treaty or other mechanism for international agreement.
- National implementation of the privacy standards.
- Enforcement/oversight mechanisms.

The harmonizing extranational approach depends on cooperation by a critical mass of nations to reach and implement an agreement on privacy.

4.6.5 The European Union Member State: A Traditional Independent Regulatory Approach

The typical approach for individual European Union member states is one of a traditional regulatory agency that is established by the national government, through act of the legislature, the executive, or a combination of the two. The agency can be assigned to a particular part of the government in

an administrative capacity, but the agency is independent from the other parts of the government in the execution of its functions. The agency consults, advises, and make recommendations on administrative measures, regulations, and proposed and future laws and policies to the other parts of the government. The agency oversees privacy compliance as shown in Figure 4.6, in both the public and private sectors with the power to conduct investigations, issue orders, and seek legal penalties for improper use of data. The data controllers may be obliged to register or notify the agency about data processing activities.

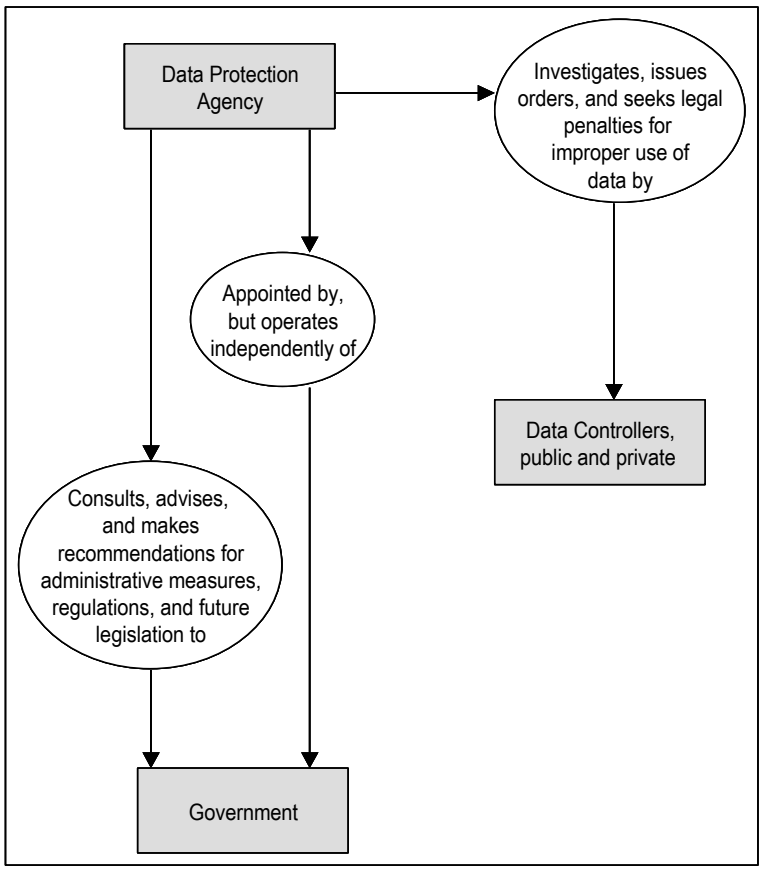


Figure 4.6 The EU Member States' Traditional Independent Regulatory Approach

The important characteristics of the traditional independent regulatory approach include:

- Appointed by, but operates independently of, the national government

- Oversees privacy-related activities of public and private data controllers
- Has some degree of independence from both the executive and legislative branches of government
- Consults and advises the government on administrative measures, regulations, and proposed and future legislation

The traditional independent regulatory approach has the advantage of working with all major parties, public and private, involved in privacy-related issues.

4.6.6 Hawaii: A Strong Investigatory Approach

One approach to privacy and data protection at the state level is to have a strong investigatory office within the executive branch. As Figure 4.7 demonstrates, Hawaii's structure is a good example of this approach. The Office of Information Practices (OIP) of Hawaii is administratively attached to the Lieutenant Governor's office, but the OIP reports to the Governor and the Legislature. The Governor appoints the OIP Director for the Governor's term. The Director is the chief executive of the OIP. Members of the public have the ability to file complaints with the OIP. The OIP issues advisory opinions regarding these complaints and may take other actions as well. The OIP may conduct compliance inquiries of, investigate possible violations of, examine the records of, and make recommendations regarding disciplinary actions to the state and county agencies of Hawaii. A member of the public is not required to appeal a denial of access to the OIP before filing suit.

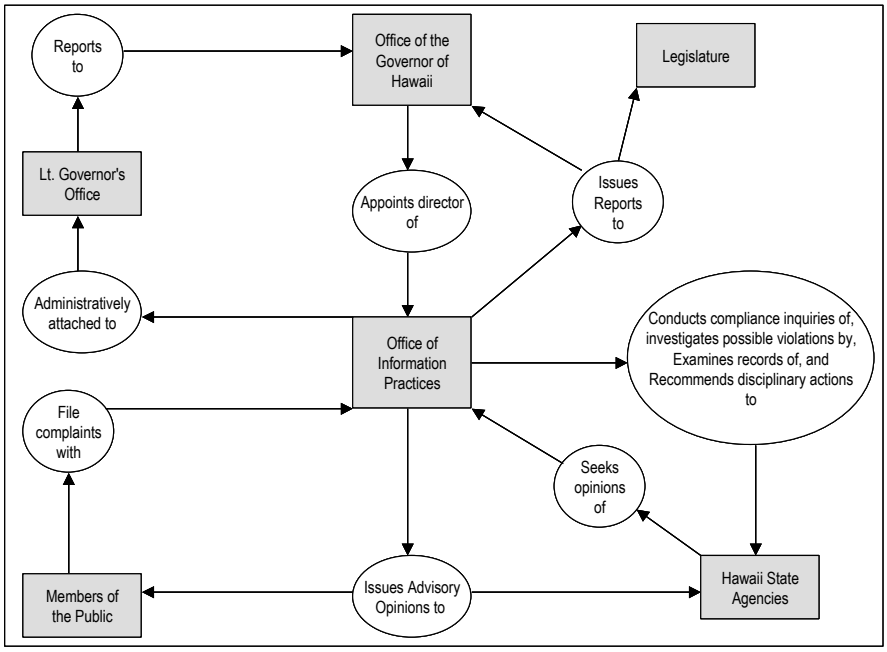


Figure 4.7 Hawaii's Strong Investigatory Approach.

The important characteristics of the strong investigatory approach include:

- Administratively attached to the executive branch
- Issues reports to the executive and legislative branches
- Hears complaints from members of the public
- Investigates activities of state agencies
- Issues advisory opinions to state agencies and to members of the public

The strong investigatory approach focuses on facilitating cooperation between government agencies, the executive, the legislature, and members of the public regarding privacy-related issues. This approach offers a much more "action oriented" means to deal with privacy and data protection than other approaches.

4.6.7 New York: An Ombudsman Approach

New York's ombudsman agency acts an intermediary and a liaison between all parties involved in privacy issues. As reflected in Figure 4.8, the agency works with members of the public, state agencies, the legislature, and the executive to foster compliance with the privacy laws. In order to ensure compliance by state agencies with the laws about personal privacy, freedom of information, and open government, the agency offers advisory opinions and assistance to any party, public or private, who requests the help of the agency. The agency also investigates appeals by members of the public regarding data accuracy, unauthorized release of data, and access to data. The governor appoints some members of the agency, others are appointed by the legislature, and some members serve as part of their government position. [Note: New York's agency works not only with privacy issues, but also more generally with issues of open government and freedom of information.]

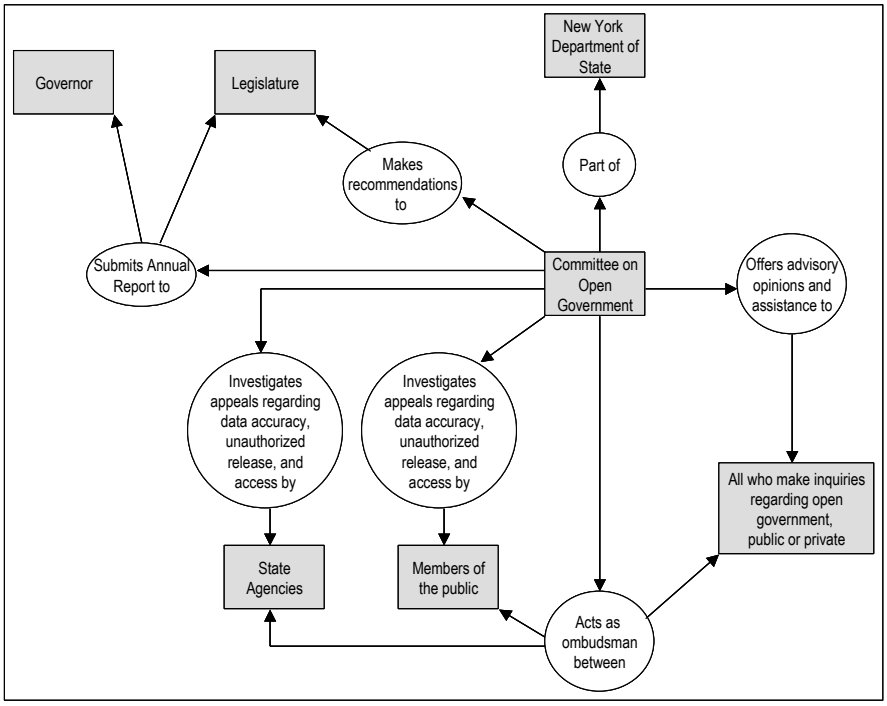


Figure 4.8 New York's Ombudsman Approach

The important characteristics of the ombudsman approach include:

- Acts as part of the executive branch
- Makes recommendations to the legislature

- Issues reports to the executive and legislature branches
- Acts as ombudsman between state agencies, members of the public, and all who make inquiries to the agency
- Oversees privacy-related activities of state agencies
- Investigates claims by members of the public
- Offers advisory opinions to all who make inquiries

The primary benefit of the ombudsman approach is that the privacy agency assists all those who express privacy concerns, facilitating resolution of privacy-related issues between state agencies and members of the public. However, the nature of such an approach—at least when implemented to the exclusion of other approaches—does not provide for any agency enforcement mechanisms or resources.

4.7 Structures Conclusions

Each privacy and data protection agency reviewed in this study has unique structural characteristics that are particular to the specific approach used in each case. However, the typical privacy and data protection agency has basic, common structural characteristics that are as follows:

- Reports to another part of government
- Works with multiple types of parties
- Hears complaints filed by members of the public
- Makes recommendations

Though these traits are fairly straightforward, the consistency with which these particular traits appear merits attention. These agencies generally have a reporting requirement to another part or parts of the government. These reports can include annual reports and reports about specific issues. Most agencies also work, in some fashion, with multiple types of parties in addressing privacy-related concerns. The types involved can include the public, the private sector, and government agencies. The interactions with these parties can involve mediating, acting as an ombudsman, investigating, and issuing orders. Most privacy and data protection agencies also hear complaints from members of the public about privacy-related concerns. Lastly, most privacy and data protection agencies have a recommendation-making function. These recommendations can be made to a wide array of parties, including government agencies, the legislature, the executive, and the private sector.

While these structural characteristics are not necessarily essential to the operation of a privacy agency, the commonness of these traits indicates that experience has proven they have real value for privacy protection. Any contemplation of the structure of Federal privacy activities should include careful consideration of the merits of these basic, common characteristics.

Finally, it should be noted that the implementation of any of the these structural approaches could produce varying results in different situations due to the inherently political nature of government and the influence of that political situation on the privacy office. At a broad level of analysis, structure can be used as a means to describe and suggest ways in which privacy laws and policies can be implemented. Any given structure, to a certain extent, will promote or limit the ways in which privacy laws can be implemented.

Section 5: Conclusions and Options

As GAO requested, this report reviews and analyzes "leading strategies, principles, or models used for protecting personal privacy and appropriately balancing privacy rights with other important interests,"[559] including the substance of privacy, enforcement mechanisms, and structural approaches currently in use around the world. This chapter provides analysis of "the possible application of such leading strategies, principles, or models to the U.S. federal government … [including] the implications for (and needed changes to) current laws, policies, and organizational structure."[560]

The fundamental constraint identified in the course of this study is that most current privacy issues and conflicts arise~~over issues related to~~ in the politic al~~s~~ and policy arenas. The debates are still at such a high level and the disagreements so sharp that the prospect of assessing basic privacy policy or finding operational improvements for privacy activities is ~~limited~~circumscribed. Until consensus has reached those political and policy matters, practical recommendations for addressing privacy ~~are circumscribed~~will often remain controversial. One step forward in any direction usually leads to an encounter with yet another unresolved policy dispute.

Because of the lack of consensus, the conclusions in this report are general and the options are limited. The analysis in this report still provides a useful description of information privacy issues and a framework that can improve basic understanding~~s~~ of privacy policy, assist with policy and political discussions, and serve as a solid foundation for further analysis and proposals for change.

5.1 Conclusions

The U.S. public policy system encourages debate among competing stakeholder groups with differing values, goals, and political philosophy, so it is not surprising to find a range of opinions for how the development of information privacy law might proceed. The views of stakeholders are widely divergent, ranging from privacy advocates who seek strong, centralized privacy legislation and regulation to other advocates who seek to prevent the adoption of any privacy legislation or privacy remedies. Achieving a consensus is difficult, while there is plenty of middle ground between these two extremes.

---

[559] Commerce Business Daily, Solicitation No. OAM-2001-N-0018, *Privacy-related Research and Analysis & Information Resources Management Services,* April 23, 2001, at Section II.
[560] *Id.*

5.1.1 Complexity of Privacy Issues

Privacy is a complex, multi-faceted concept that is hard to define precisely since it reflects values that are not directly translatable into consensus elements and that are not easily applied in practice. Multiple sub issues within the scope of "privacy" are also poorly defined. Focusing on information privacy (data protection) is useful because it narrows the scope of the subject and more specifically identifies many aspects of privacy that are currently the subject of debate and international attention. The narrower focus reduces but does not eliminate the complexity of privacy. Figure 5.1 illustrates the range of factors affecting the development and implementation of information privacy policy. Implementation of information privacy laws is affected by factors such as the resources available to implement the laws, the organizational structure selected to implement and operate information privacy laws, and the degree to which the various agencies or offices are committed to enforcement. The enforcement of information privacy laws depends on the mechanisms at the disposal of the person or institution that bears the responsibility for enforcement and on the degree to which those responsible are committed to utilizing those enforcement mechanisms.

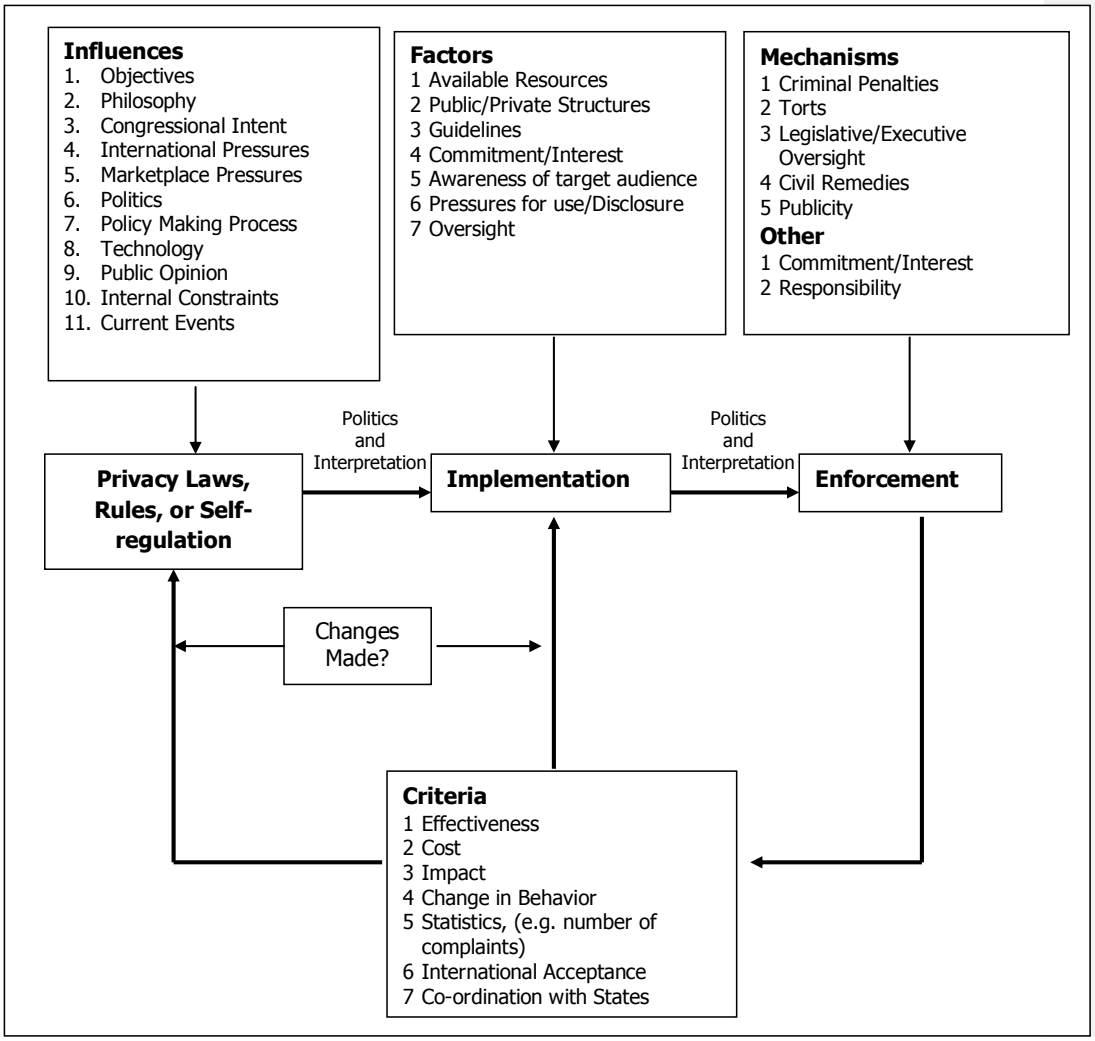
Figure 5.1 shows the process used to review the effectiveness of the laws, implementation, and enforcement has a significant impact on the development of information privacy policy. While criteria such as cost, impact, and effectiveness suggest assessing information privacy laws, rules or self-regulation, little such assessment is routinely undertaken. In this respect, privacy is not necessarily different from other policy areas where attention to fundamental objectives or to an overall assessment of actual implementation is fitful at best.

Figure 5.1 suggests that the political and interpretative process for information privacy law, implementation, and enforcement can vary significantly among organizational settings based on local politics and traditions. For example, the historical context of populism and the citizen's right to know continues to affect information privacy development in Wisconsin. A change in the context would be likely to affect privacy development elsewhere.

The diversity of opinions also makes it difficult to suggest what type of approach or structure (as discussed in Section 4.7) would be most suitable for a particular organization or governmental setting. No right or wrong answers are readily identified. The problem can become even more difficult where existing models for privacy organizations (invariably small organizations) are heavily influenced by the enthusiasm and competence of the particular individuals who run the organizations. A change in personnel may turn a seemingly successful model into a failure or vice versa.

5.1.2 Wide Acceptance of Fair Information Practices

Fair information practices reflect core principles of information privacy in almost every country that has formally addressed privacy. International statements of FIPs are useful for examining American privacy laws and policies. No other approach to privacy offers the detail found in FIPs or has a wider base of support. FIPs principles break the issues down into manageable elements that can be



discussed and applied, for the most part, independently of one another. The framework of FIPs is beneficial even when there is no political or policy agreement on substance because it identifies specific elements and helps to pinpoint the areas of agreement and disagreement.

In the U.S., FIPs are not as widely recognized as elsewhere, but the~~ir appearance is~~ are becoming more commonplace in public policy debates. The FIPs principles have occasionally been restated by some in the U.S. in ways that omit or significantly revise core elements. The divergence between the international consensus on FIPs and some American FIPs restatements is noteworthy and may be the cause of increased tensions on international privacy matters in the future. As a result, it is important that any differences in statements of FIPs be transparent and not ~~hidden~~ obscured by~~under~~ the use of ~~a~~ misleading ~~common~~ label~~s for divergent policies~~.

5.1.3 Effect of Value Judgments and Political Philosophies on Implementation

Even when privacy laws, practices, and operations rely on the same core set of FIPs principles, implementation of these principles can result in a wide diversity of applications that vary with the type of record-keeper, the nature of the information, the circumstances under which the records were collected, the uses and disclosures planned for the records, and other contextual factors. Implementation of FIPs requires value judgments rather than precise, definable calculations to determine when a particular application is sufficiently rigorous to satisfy the objectives of a given principle.

Objective consensus implementation of FIPs standards is difficult. The lack of bright lines and clear demarcations is a reflection of the diversity of record keeping activities throughout government and the rest of the economy; the large number of important institutions that affect privacy interests; and the need to strike a balance between privacy and other socially desirable goals. This makes privacy a challenge, not unlike other desirable but hard-to-define concepts such as justice, ethics, and safety.

5.1.4 Difficulty of Enforcement

Enforcement is a central issue in privacy. As with other aspects of FIPs, enforcement of privacy laws and policies can be accomplished through many different mechanisms, each of which has advantages and disadvantages. Choices among the available options are significantly affected by the broader political context and by other criteria external to privacy.

Value judgments and alternative interpretations influence the effectiveness of enforcement. For example, the absence of enforcement actions may have different meanings. It may reflect broad compliance, making enforcement unnecessary, or popular indifference, making enforcement impossible. Or it may be evidence that data subjects do not know how their information is being used or misused. Still another interpretation is that the remedies are not attractive enough to plaintiffs and lawyers to warrant lawsuits. The list of possible reasons for any given level of enforcement would be very long.

While this study did not set out to collect factual information on privacy enforcement, it does appear that limited, incomplete, and inconsistent enforcement of existing privacy laws is commonplace. Identifying the reasons for limited enforcement of some laws and the effective enforcement of a few others (e.g., the Privacy Act of 1974) would require fact-finding beyond the scope of this project.

5.1.5 Decentralized and Uncoordinated Privacy Law

Of the federal privacy laws currently in force in the U.S. all reflect FIPs to varying degrees. Implementation of the laws, organizational structure, and enforcement mechanisms vary considerably. The laws were~~were~~ passed at different times and under a variety of circumstances, often originated with different Congressional committees, and~~may~~ lack consistency. ~~A lack~~The absence of coordination is a ~~regular~~ familiar feature of the American system of policy making and not unique to privacy. Inconsistency in scope and standards is a particular consequence of what is often described as the American "sectoral" approach to privacy legislation. Whether this is a virtue or a vice is primarily a matter of political philosophy and personal judgment.

The decentralized and sectoral U.S. approach to privacy protection requires specific knowledge of each law and regulation to understand the actual and potential use of the laws as a basis for privacy protection. Figure 5.2 suggests criteria that could be used to compare and assess existing privacy policy instruments. The criteria offer a beginning approach for the types of questions to ask and the analytic criteria to employ in (1) assessing existing privacy policy instruments, and (2) considering how new privacy initiatives compare to existing policy. An assessment of the actual implementation of the laws would require highly refined criteria and the collection of large amounts of new data.

Ambiguity

- Can a reasonable outsider infer what the policy is (briefly summarize the policy)?
- Can the policy be interpreted in multiple ways, and if so, how?
- Are key terms carefully defined?
- Does the policy contain examples or application to minimize confusion?
- Does the policy cover one or multiple record categories and record keepers, and are the boundaries clearly defined and consistent with other privacy laws?

Contradictions

- Do policies appear in other government-wide document or laws that contradict this particular policy?
- Do policies appear in (internal) agency documents that contradict this particular policy?
- Are there judicial decisions that contradict this particular policy?

Duplication

- Does the same policy or wording appear more than once within the same document?
- Does the same policy or wording appear in other government-wide or agency documents?

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Gaps
- Are there areas where additional guidance in how to interpret or implement the policy is needed?
- Should more detail, explanation, or justification be provided in the policy?
- Would specific examples clarify how to implement the policy?

Inconsistencies (gray areas that are not necessarily contradictions)
- Are different directions for implementation of policies provided within a given document?
- Are different directions for implementation of policies provided across similar policy instruments?
- Are responsibilities and roles of policymakers the same for similar policies across different policy instruments?
- Can a record keeper be subject to different laws or policies for the same record?
- Will record keepers subject to multiple laws have to comply with significantly different substantive rules or procedures?

Enforcement
- Are there explicit statements as to how the policy will be enforced?
- Are there explicit statements as to who or which agency will have oversight for agency compliance?
- Are penalties and consequences for non-compliance made explicit?

Modifications and Updates
- Is there an explicit process for collecting user feedback (users both within and outside the agency)?
- Is there a process that insures regular and ongoing review of the policies given the passage of time and the likelihood that other similar policies have been passed or approved?

Figure 5.2 Selected Criteria for Assessing Privacy Policy Instruments

The relatively narrow scope of existing privacy laws, especially laws governing the private sector, may limit the value of these comparisons. However, for some areas, a review could well produce broader lessons. For example, a comparison of the content, delivery, effectiveness and readability of consumer notices—a feature found in several laws—may offer more guidance to policy makers considering how to frame a notice requirement in a new law or how to reshape an existing requirement. Notice provisions may have enough commonality to permit a substantive, non-policy assessment of their effectiveness.

5.1.6 Matching Intent with Structure

Having a clearly defined, empowered structure to oversee, implement, and enforce privacy laws is an important part of privacy regulation in most of the world. This well-established aspect of international privacy policies is beginning to be reflected in the U.S. Formal privacy structures are increasingly found in both the U.S. public and private sectors. As shown in Section 4.7, the

operational approaches used to implement and enforce information privacy laws have strengths and weaknesses in terms of matching the intent of the privacy law. Many of the approaches are unevaluated for their and many are too new to evaluate properly.

Privacy structures (e.g., privacy agencies, privacy commissions, chief privacy officers, ombudsmen, dispute resolution mechanisms) appear to have evolved as ~~institutional~~ better understanding of privacy developed and as the search for a higher-order approach to privacy intensified. The presence of privacy-specific expert organizations—with or without significant enforcement authority—may be useful in overcoming some of the inherent uncertainties that arise in applying privacy principles in practice. The privacy structure is an important means of addressing the natural ambiguities in broad policy pronouncements. The structure can make consistent experience and expertise available within an organization to those who only occasionally need to address privacy issues. The ~~unprompted~~ development of private sector structures such as chief privacy officers, unprompted by legislation or even by self-regulatory codes, suggests that the value of privacy expertise ~~has been~~ is being more widely recognized.

Yet to be understood is how the factors that comprise structure (see Section 4.7 and Figure 5.1) affect implementation, enforcement, and overall effectiveness of privacy laws. For example, if the intent of policymakers is to have strong enforcement capability, then it is advantageous to charge an agency or office that already has such capability with enforcement. If the intent is that little or no enforcement occurs, then a structure with different powers and responsibilities can be developed.

5.1.7 Changing Environment for Privacy

Privacy rules for federal agencies come principally from the Privacy Act of 1974 as amended. At the time Congress passed the Act, the Internet and web-based services and resources were not even imagined. During the Clinton administration, the federal government began to strongly encourage and promote e-government and e-commerce as a means of conducting government business both with its citizenry and among government agencies. The rapid evolution of the networked environment has brought Internet privacy issues to the forefront because:

- The new network, telecommunications, and computing technologies allow for rapid identification, sharing, and analysis of personal information that was not possible or practical in the past.
- E-government and e-commerce cannot operate effectively without the inclusion and authentication of personal information.
- Collecting personal information on a regular ongoing basis is a primary objective for many networked services as a means to better market network services.
- Information sharing among agencies and between agencies and private firms may be more commonplace.
- Reported ~~A~~abuses in the use and dissemination of personal information by criminals, by private sector firms, and by governments ~~others~~ have increased the public's knowledge of

Formatted: Bullets and Numbering

privacy issues and have also increased the fear that personal information may be misused in significant ways.

While some debate whether privacy issues in the networked environment are fundamentally different from privacy issues in the offline world, the networks clearly have brought increased attention to privacy. The Privacy Act of 1974 was not written to address ~~unforeseen~~ networked technology and it has not been ~~properly~~ regularly amended to address recent technological developments. As a result, the Privacy Act of 1974 ~~as amended~~ does not currently meet the current technological demands related to privacy.

5.1.8 Assessing the Effectiveness of Information Privacy Approaches and Compliance

Determining the effectiveness of any particular *approach* to privacy, such as a strong central agency or a privacy commission or a market-based approach, calls for much more than simply assessing whether a law has achieved~~compliance~~ *compliance* by those ~~affected~~subject to the law. Assessment of a privacy approach must be based on a broad range of political and policy objectives that the approach is meant to accomplish. Criteria would include structural factors that enhance or detract from accomplishing political or other objectives. Assessing a privacy approach would entail consideration of international pressures as well. In an interconnected world, a privacy approach that addresses domestic needs may still fall short because of the routine exchange of personal data with other countries.

Determining the degree of *compliance* with a particular privacy law in terms of its legal basis, implementation, and enforcement would require a set of agreed-upon criteria with operational definitions. These criteria would be based primarily on the details of the law and the judgment of those who created the criteria and operational definitions. An example of these criteria might include:

- ***Timeliness*:** Privacy disputes between citizens and a government agency should be acted upon promptly by the agency and resolved within a fixed period.
- ***Cost:*** Agency spending on managing privacy issues or resolving privacy disputes should fall within a defined range of an overall budget.
- ***Organizational structure*:** Each agency should have at least one person with responsibility for the management, implementation, and resolution of privacy.

Formatted: Bullets and Numbering

These are offered only as examples, but they suggest the potentially arbitrary nature of each criterion. An agency with a vast database of personal information (e.g., Social Security Administration) might require greater privacy resources than an agency principally responsible for producing "things" (e.g., National Aeronautics and Space Administration). Both agencies might have the same standards for resolving disputes, and both might have a privacy structure, although the size, scope, and powers of the privacy offices would differ.

Alternatives to specific criteria with operational definitions are open-ended criteria such as "appropriate," "responsive," or "timely," which have a much greater potential for interpretation in counterproductive ways. Without some tension to ensure a fair application of privacy policies, the policies will be harder to evaluate and broad inconsistencies are more likely to develop in practice.

The question remains as to how best to assess the overall effectiveness of a particular privacy approach. Ultimately, such assessment would require: (1) a process for conducting the assessment, detailing who does what in the assessment; (2) a set of criteria with operational definitions (drawn, in part, from the original privacy legislation); (3) a means for reporting the degree to which an agency or policy does or does not met the agreed upon criteria; and (4) a process that enables or requires the agency to better meet the criteria. In such an assessment, the criteria might range from extremely structured to unstructured and the evidence could range from quantitative to qualitative. This kind of compliance oversight may require considerable resources to implement.

Another issue with assessing the effectiveness of privacy compliance in agencies is the fact that different privacy laws may require different responses and approaches by the agency. An assessment of the degree to which one agency is effectively enforcing privacy legislation may require a very different process than the assessment of the extent to which enforcement is effective in another agency.

5.1.9 No Consensus on Privacy Policy Initiatives

Many stakeholders increasingly are asking their state and federal policymakers to "do something" about privacy protection. Some ~~individuals~~ data subjects want assurance that their personal information is used only for the intent for which it was originally collected, that third parties not have access to their personal information, that the rise in identify thefts be reversed, and that they have control over who has access to their personal information. ~~Others~~ Data users and record-keepers seek ~~"responsible"~~ access to and use of personal information for a variety of commercial and marketing reasons. Public policy advocates, Congress, commercial record-keepers, and government agencies ~~each~~ have offered ~~some~~ their own suggestions for new policies regarding privacy, with little agreement among stakeholders as to what the substance of a privacy policy should be.

The sources reviewed earlier in this report show strong agreement on basic principles of privacy – based primarily on ~~the~~ FIPs. The agreement, however, is limited to the highest level of abstraction. Building consensus on privacy is difficult. Some obstacles include:

- ***Defining Privacy.*** "In spite of the huge literature on the subject, a satisfactory definition of privacy remains as elusive as ever."[561] The most fundamental issue to a privacy policy is what is meant by the word *privacy* and whether privacy can be protected under the chosen definition. How the government defines privacy in establishing privacy policy will affect both the response to the policy and the effectiveness of that policy.

[561] Raymond Wacks, *Personal Information: Privacy and the Law*, 13 (1989).

- ***Privacy versus Other Fundamental Values.*** Though the term privacy is not mentioned in the Constitution, a right to privacy coexists with other explicitly stated protections in the Constitution. Any privacy policy regulating government conduct must contend with other fundamental values and interests that may raise conflicts. Protection of privacy may come into conflict with stated Constitutional rights, such as the rights of freedom of speech and of the press, and with federal laws that embody important societal interests, such as access to government records, national security, public health, economy and efficiency, law enforcement, and other interests.
- ***National Interests in a Federalist Society.*** Many states already have some privacy laws,[562] and they are actively considering new laws. Any federal policy must balance the rights and powers of the state governments with the interest of the national government in addressing privacy issues.[563] In Canada, the federal government and the provincial governments are working to achieve a balance between national and provincial privacy policies (see section 4.4.3.2). The ultimate outcome in Canada remains in doubt, in part because the Canadian Constitution does not grant the Canadian government powers over interprovincial commerce that are as broad as those in the U.S. Constitution. A federal privacy policy in the U.S. will have to consider state and federal interests as well as the value of greater uniformity in the regulation of commerce. Some of the conflicts are over who can regulate, who can set standards, and who can enforce privacy laws.
- ***Conflicting Values among Stakeholders.*** Private citizens, corporations, interest groups, record-keepers of all types, the media, and public entities bring varying and frequently conflicting perspectives to the content and application of privacy policy. The importance of addressing privacy varies tremendously among the stakeholders as well. Some would be just as happy if privacy disappeared entirely from public debate, although public opinion polls show a strong and continuing degree of public concern. The differences in substantive objectives of the relevant stakeholders are quite broad, ranging from no legislation on privacy on one side to a European-style omnibus privacy law on the other. While there is much room in the middle, serious exploration of compromise has been infrequent except in narrow contexts. It is fair to say, however, that some narrowing of the privacy debate has occurred during the last decade. Privacy is perceived as a mainstream issue today and not a fringe matter for fundamentalists.
- ***The Congressional Approach to Privacy.*** During the past five years, Congress has shown strong interest in a spectrum of privacy issues. The range of privacy-related Congressional hearings documented in Appendix A is broad. The range of committees and subcommittees addressing privacy issues is similarly broad. The decentralized nature of privacy issues in Congress may prove to be an obstacle for comprehensive policymaking, as Congress is not likely to assign one committee the power to oversee all privacy issues.[564] The sectoral approach for U.S. legislation tends to bring different sets of stakeholders to the table each

[562] *See* Bruce D. Goldstein, *Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection,* 41 Emory L. J. 1185 (1992).
[563] *See* Ken Gormley & Rhonda G. Hartman, *Privacy and the States,* 63 Temple L. Rev. 1279 (1992).
[564] *See* Lillian R. BeVier, *Information about Individuals in the Hands of the Government,* 4 William & Mary Bill Rts. J. 455 (1995).

time legislation is considered. One consequence is that when new sectoral legislation passes, it is more likely to reflect a different substantive and procedural balance for privacy than existing legislation.

- ***The Organization of Government.*** The size of government and the pervasive importance of personal information to government activities contribute obstacles to a privacy policy. As with other issues that have broad, crosscutting effects, evaluating the consequences of privacy policies for federal agencies can be complex. Like other stakeholders, the agencies themselves have different perspectives and priorities, and it is unlikely that an agency or office can represent the interests of data subjects in policy debates. For example, the Department of Health and Human Services (HHS) has been charged with developing a privacy policy for health records, but HHS has its own interests in using health records for public health, research, cost control, and policy development. Conflicts over health privacy just within HHS can be noticeable, and that occurs before considering the interests and needs of the many other agencies with some jurisdiction over health matters. No one may actually and unambiguously represent the interests of data subjects.
- ***National Interests in a Global Society.*** In the past two decades, many nations adopted some type of national privacy policy. The policy of the EU has had a tremendous impact on what many other nations, including the U.S., have done regarding privacy, although the U.S. has been more resistant to European pressure than many other nations.[565] As demonstrated by Section 4 of this report, privacy policies of other nations vary and are often updated and altered. International differences in privacy protections create conflict in many spheres of international commerce, not the least of which is cyberspace.[566] Further, privacy is not implemented in a uniform manner internationally. Despite the international consensus around FIPs, privacy laws of other nations reflect the cultures and traditions of those nations. Some of the differences in approach and implementation have consequences for the international community. There is no reason that existing institutions for resolving international conflicts will not work for privacy, but experience to date has been limited, and significant international struggles over privacy can be confidently predicted for the future.
- ***Privacy versus Technology.*** Technology may be the most unmanageable impediment for any privacy policy. The competition between privacy and technology has been recognized since before the beginning of the 20th century, and the conflicts have grown much sharper since the beginning of the computer age.[567] Privacy policy, in order to adequately contend with the evolving power of technology, should be flexible, technology-neutral, and able to adapt to changes in technology that affect privacy as these changes occur. Privacy policy will

---

[565] *See, e.g.,* Marie Clear, *Falling into the Gap: The EU's Data Protection Act & Its Impact on U.S. Law & Commerce,* 18 J. Marshall Comp. & Info. L. 981 (2000); Gregory Shaffer, *Globalization and Social Protection: The Impact of the EU and International Rules in Ratcheting Up U.S. Privacy Standards,* 25 Yale J. Int'l L. 1 (2000); Fred H. Cate, *Changing the Face of Privacy Protection in the EU and the U.S.*, 33 Ind. L. Rev. 174 (1999).

[566] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace,* 52 Stan. L. Rev. 1315 (2000).

[567] Paul M. Schwartz, *Data Processing & Government Administration: Failure of the American Legal Response to the Computer,* 43 Hastings L.J. 1321 (1992).

have to be constructed with adaptation to technological evolution as an inherent component of the policy. Creating such an adaptive element in a privacy policy is certain to be difficult.

- ***Substantive Solutions.*** Privacy policy is not only difficult because of the many different perspectives and conflicts that it generates. Each approach to privacy problems – ranging from omnibus legislation to sectoral legislation to self-regulation to doing nothing – tends to exacerbate differences among stakeholders rather than appeal to common interests. None of the existing models for addressing privacy seems to have much hope of attracting broad consensus. Compromise is more likely on details – such as the content of a privacy notice or the terms of data subject access – but a consensus framework for the details is problematic. The lack of a conceptual consensus framework is a significant impediment to discussion and compromise.

This list of obstacles is not comprehensive, but suggests the breadth of scope that the obstacles cover. In addition, the obstacles are suggestive of areas where additional research and investigation could be conducted to better understand their nature and how best to devise ways around them.

5.2 Options

5.2.1 Options for Privacy Policies Based on Structural Models

The U.S. federal government has pursued privacy protection in a manner the report has ~~best~~ described as decentralized, sectoral, and lacking in coordination. Rather than being proactive, most federal policies and laws have been reactive and sectoral. These policies and laws have also been predominantly narrow in scope in terms of the issues addressed and the privacy protections granted. As a result, the U.S. federal government lacks a comprehensive and coherent policy toward privacy protection. Instead, it has taken three, mostly unrelated, general approaches to protecting privacy in limited ways.

The first approach is based in the executive branch. The Office of Management and Budget has been given ~~a limited~~the role of overseeing privacy among the federal agencies, as discussed in Section 4.2.2. As part of its role as coordinator of information and regulatory policies, OMB does some coordination for~~coordinate~~ privacy issues and makes occasional general privacy policies. However, its capacity to effectively implement and enforce these policies is limited. OMB's Office of Information Regulatory Affairs (OIRA) is the statutory office charged with privacy oversight. OIRA's privacy initiatives have been mainly designed to increase awareness about privacy issues. One recent example of OMB's involvement in privacy issues was the issuance of the *Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy* (December 20, 2000), which provided guidelines for federal agencies regarding database matching and the use of personal information.[568] OMB's privacy activities were more robust during the last two years of the Clinton Administration

[568] *M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy* (December 20, 2000). Available at http://www.whitehouse.gov/omb/memoranda/m01-05.html.

when a Privacy Counselor was appointed, but the level reverted to a more traditional level when the Privacy Counselor's function was not continued.
~~The second approach to privacy protection is in the area of the private sector. The Federal Trade Commission has a limited role in oversight and enforcement of privacy protections, as detailed in Sections 3.8.1 and 4.2.1. However, the FTC has limited jurisdiction, allowing it only to oversee the privacy-related activities of private organizations that have adopted a privacy policy, and in the context of unfair and deceptive trade practices.~~

The ~~third~~ second approach to privacy protection results from the policies developed within individual agencies. ~~Given the long tradition of permitting self-regulation in the private sector and placing few constraints on the federal government agencies~~ With limited central management direction, privacy is left to individual agencies to pursue in their own way, if at all. ~~, if the agencies so determine they are interested in pursuing a privacy protection policy.~~ Some examples of agencies that have instituted privacy policies and privacy structures, noted in Sections 4.2.3 and 4.2.4, ~~include~~ are the Department of Defense and the Internal Revenue Service~~, respectively~~. The result has been isolated pockets of agency privacy protections. A comprehensive review and assessment of individual agency efforts related to privacy protection has not been done.

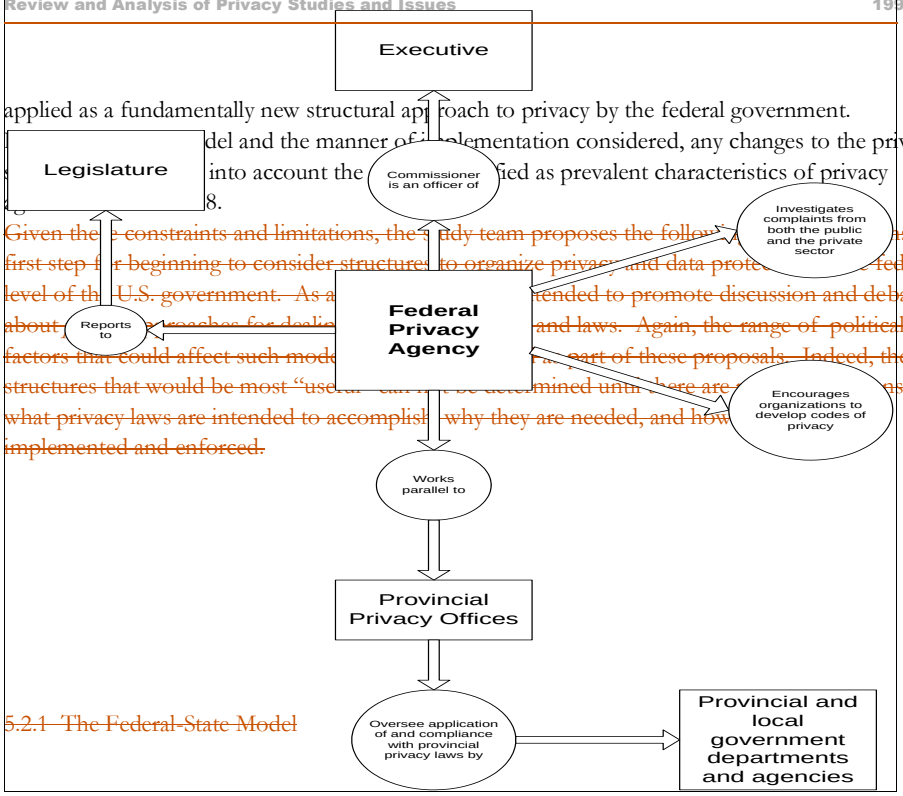
The third approach to privacy protection is in the area of the private sector. The FTC has a prescribed role in oversight and enforcement of privacy protections, as detailed in Sections 3.8.1 and 4.2.1. The FTC has limited jurisdiction, allowing it only to oversee the privacy-related activities of private organizations that have adopted a privacy policy, and in the context of unfair and deceptive trade practices. Recent laws have also given the FTC some responsibility for privacy practices of financial institutions and for commercial websites aimed at children. A few other agencies have narrow privacy roles that are rarely exercised. Federal agency privacy activities for the private sector have never been comprehensive, coordinated, or continuous.

The three basic approaches taken by the federal government, based on the Privacy Act of 1974 and ~~subsequent~~ other legislation, have resulted in a situation where privacy protection, when available, is ~~highly~~ decentralized in implementation and effectiveness. The sporadic availability of privacy protection within the structure of the federal government has certain advantages when considering possible privacy protection structures. ~~A privacy structure could be created to complement and enhance t~~The decentralized privacy activities of the federal government could be continued and, perhaps, enhanced, or a completely new structure could be considered to address privacy-related issues in other ways.

When considering how the structural models of privacy could be applied to a privacy policy of the federal government, two different methods of application can be examined. The first method involves the determination of which models and characteristics could be applied within the current privacy structure of the government. Changes to the current structure could be either the enhancement of activities now underway or the addition of complementary activities ~~to those done now~~. The second method involves the determination of which models and characteristics could be

applied as a fundamentally new structural approach to privacy by the federal government. del and the manner of implementation considered, any changes to the privacy into account the ied as prevalent characteristics of privacy 8.

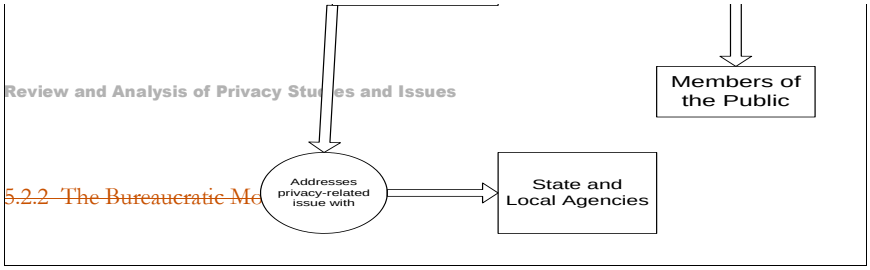
Given the constraints and limitations, the study team proposes the follow as as a first step for beginning to consider structures to organize privacy and data prote federal level of the U.S. government. As a tended to promote discussion and debate about and laws. Again, the range of political factors that could affect such mode part of these proposals. Indeed, the structures that would be most "usef be determined until here are as as to what privacy laws are intended to accomplish why they are needed, and how implemented and enforced.



5.2.1 The Federal-State Model

Figure 5.X. The Federal State Model

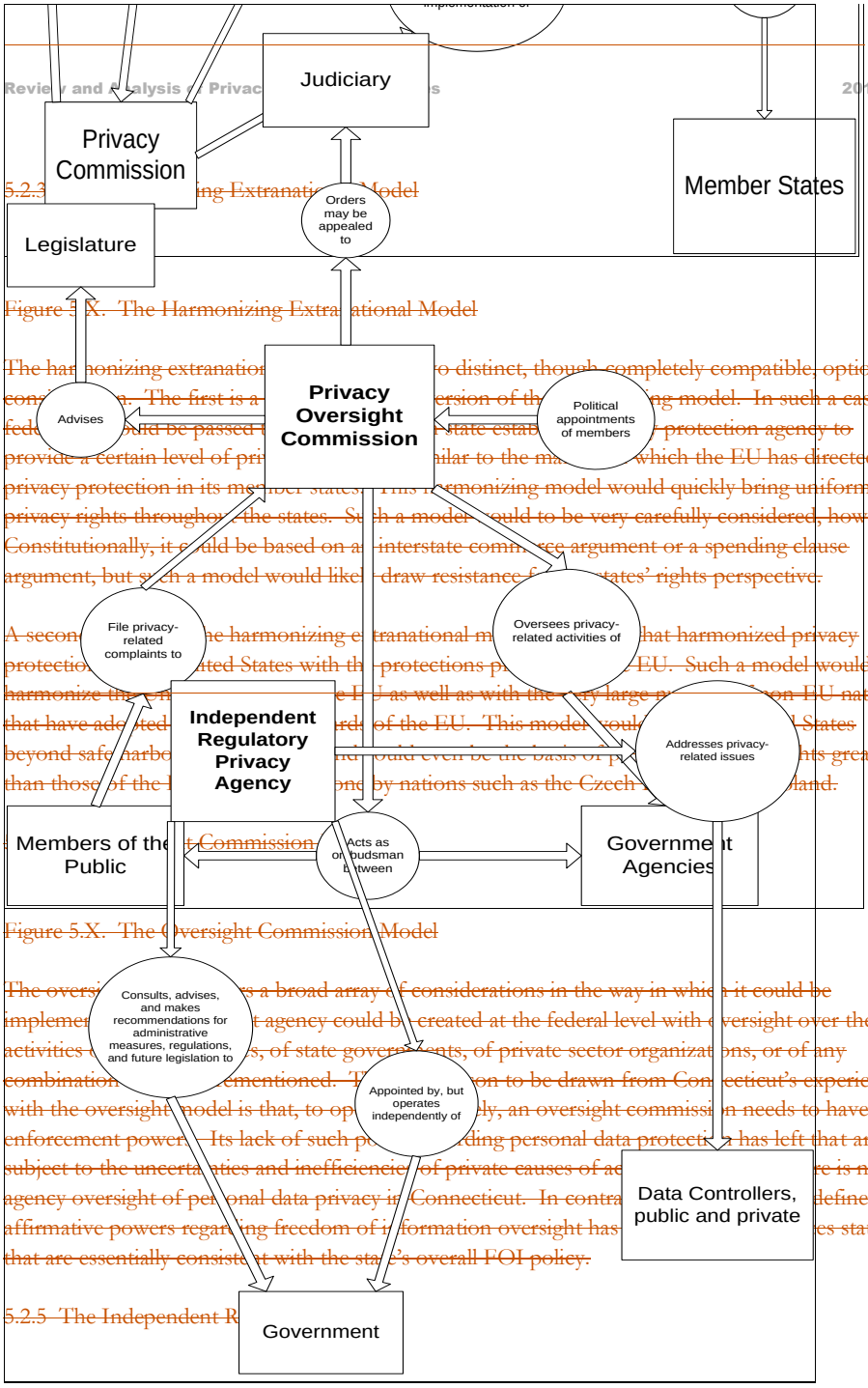
The federal-state model offers several relevant characteristics. As many states already have established privacy laws or protection agencies, a federal-state model could be applied so that a United States federal privacy agency could be functioning parallel to the state agencies. These parallel functions could involve separate efforts, such as is the system in Canada, or could be a coordinated effort between the federal agency and the state agencies. If the federal agency were more oriented toward coordination, such as an expanded and enhanced version of what OMB does now, then the federal agency could take the lead on privacy matters or could work completely in concert with the state agencies.



5.2.2 The Bureaucratic Mo

Figure 5.X. The Bureaucratic Model

The primary consideration drawn from the bureaucratic model is how the placement of an agency within the government structure would affect the ability of the privacy agency to fulfill its mandate. If a bureaucratic model were to be considered, the placement within the federal government structure must be weighed carefully, with respect to lines of authority and reporting, relationships with other agencies, and enabling powers. The amount of power the agency would have and its ability to operate effectively could be greatly constrained by an array of situational factors surrounding the bureaucratic placement.



5.2.3 ing Extranati Model

Figure 5.X. The Harmonizing Extra ational Model

The har onizing extranation o distinct, though completely compatible, options for con a. The first is a ersion of th g model. In such a case, a fed ould be passed t state estab protection agency to provide a certain level of pri ilar to the ma which the EU has directed privacy protection in its me ber states. This h rmonizing model would quickly bring uniformity to privacy rights throughou the states. Su h a model ould to be very carefully considered, however. Constitutionally, it c uld be based on a interstate comm rce argument or a spending clause argument, but s ch a model would likel draw resistance f tates' rights perspective.

A secon he harmonizing e tranational m hat harmonized privacy protectio ted States with th protections p EU. Such a model would harmonize the U as well as with the y large n on EU nations that have ado ted rd of the EU. This model oul States beyond safe harbo ould even be the basis of p hts greater than those of the l ond by nations such as the Czech and.

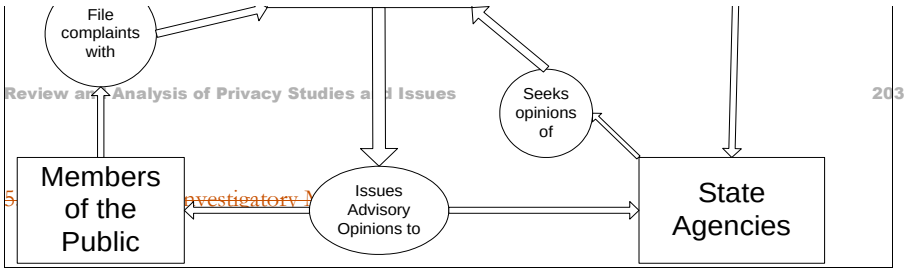
Figure 5.X. The Oversight Commission Model

The oversi s a broad array of considerations in the way in whic it could be implemen t agency could b created at the federal level with oversight over the activities of s, of state governments, of private sector organizat ons, or of any combination mentioned. T on to be drawn from Con ecticut's experiences with the oversight model is that, to op ly, an oversight commissi n needs to have enforcement power . Its lack of such p ding personal data protecti has left that area subject to the uncerta ties and inefficiencies of private causes of ac e is no agency oversight of per onal data privacy in Connecticut. In contra defined, affirmative powers regar ing freedom of i formation oversight has es statewide that are essentially consiste t with the sta e's overall FOI policy.

5.2.5 The Independent R

Figure 5.X. The Independent Regulatory Model

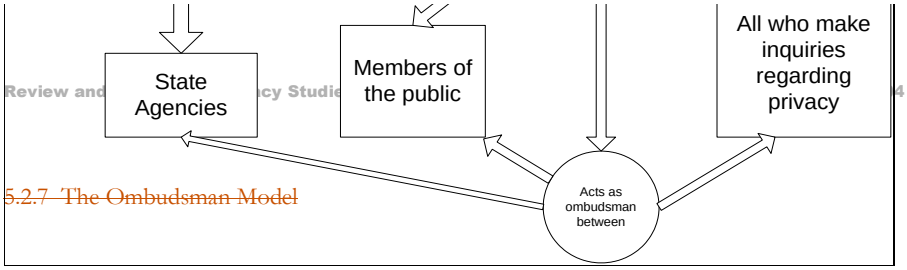
~~The independent regulatory model is worthy of consideration if the specific goal of a federal privacy agency would be to address privacy-related matters in the public *and* private sectors. If implemented, this model has the potential to be a very activist protector of private information in the hands of both private businesses and public organizations. However, as demonstrated by certain EU nations, an independent regulatory agency can be hampered in its functions if too many exceptions are made to the regulatory powers of the agency.~~



5. The Strong Investigatory Model

Figure 5.X. The Strong Investigatory Model

The strong investigatory model is worthy of consideration for the fact that it facilitates the involvement of and the interaction between many different parties involved in privacy-related issues, while also having the ability to enforce privacy protection. The strong investigatory model allows a privacy agency to work in an advisory role on privacy matters, but also to investigate and enforce privacy rights when violations occur. A strong investigatory privacy agency has the potential to be very active and involved in the privacy-related issues involving the public and government agencies.



5.2.7 The Ombudsman Model

Figure 5.X. The Ombudsman Model

The ombudsman model offers a number of issues for consideration and could be applied in two distinct ways. The ombudsman model has the potential to include all potential parties with interests in privacy issues. An ombudsman privacy agency could work simultaneously with federal agencies, state governments, members of the public, and private sector organizations in addressing privacy-related issues. Such an agency could meet a number of privacy-related needs by hearing privacy-related claims, by offering opinions and advice, and by facilitating solutions. To do this effectively a substantial amount of trust respect would first have to be built by the agency and its staff, which can only be earned over time and by gaining a thorough expertise that is recognized by all potential parties. Implementing this model alone, however effective it may otherwise be, will nevertheless be quite limited in its influence compared to an agency that has powers of investigation and enforcement.

A different, though not mutually exclusive, application pf the ombudsman model would be an agency functioning as an ombudsman between the state privacy agencies. In such an ombudsman capacity, a federal privacy agency could work with the state privacy agencies to bring a greater sense of uniformity to privacy protections among the states. The federal agency could ensure certain levels of privacy protection across the states by working to bring consensus among the states about privacy concerns.

5.2.2 Concluding Considerations about Privacy and Structural Models

A number of questions arise when discussing national privacy structure.

- To what extent is the United States federal government interested in acting to expand privacy protections in the U.S.? This is a major question on which no consensus exists at present.
- What models or characteristics could be applied effectively within the current privacy structure of the U.S.? Is there something in the current limited privacy structure that could be fruitfully expanded? Legislative proposals to expand the jurisdiction of the FTC have been offered. Expanding the role of OMB has not been significantly debated. Agency privacy offices have been expanded on the initiative of the agencies themselves, but improvements that might be made at the agency level have been largely unexplored. In the current political environment, it might be more fruitful to concentrate on narrower responses and on changes that affect only individual agencies.
- Should a federal privacy agency be independent like a regulatory commission? Should a privacy agency have one head or be headed by a collegial body? Could an independent privacy agency be established in the U.S. and have a useful set of powers? Would

Formatted: Bullets and Numbering

constitutional limits prevent an independent agency from overseeing or enforcing laws against federal agencies?

- If a federal privacy agency were established, should it have the power to issue regulations? Conduct investigations? Issue subpoenas? Hold hearings? Accept complaints? Represent the U.S. abroad on privacy matters? Assist the private sector on a voluntary basis? Approve industry or company self-regulatory privacy codes? Propose legislation? Comment on legislation? Direct agency compliance with the Privacy Act of 1974? Supplant or work with existing privacy enforcement agencies such as the FTC? Issue advisory opinions? Conduct research? Issue reports?

- ~~What models or characteristics could be legally applied under the Constitution of the United States?~~

- ~~Does the federal government prefer a privacy initiative from the national level or a unification of the state privacy protection activities?~~Is a federal-state partnership on privacy a realistic possibility? State attorneys general have joined together to bring some privacy lawsuits, and they have authority to bring actions under some federal privacy laws. Debates over federal preemption of state privacy activities have not focused on the role of state attorneys general or state privacy offices.

Formatted: Bullets and Numbering

~~5.What external factors, including the interests and reactions of members of the public, other government organizations, and political action committees, will effect the implementation or effectiveness of any attempted federal privacy protection initiate?~~

~~6.What is the political will to address privacy-related issues at this level?~~

~~7.Are privacy-related issues a priority of the current presidential administration and Congress?~~

These issues are just some of the concerns facing any attempt to institute a national privacy protection agenda in the U.S. Which of these issues becomes~~very~~ important will depend on the type of structure that is considered and the proposed implementation of the structure under consideration. At present, the idea of a privacy agency does not appear to have broad support, and it has rarely been the subject of current debate.

5.2.3 Substantive Options for Next Steps

Pending additional direction from policy makers about U.S. privacy activities, ~~there are~~ some substantive options can provide useful information to policy makers or to those implementing existing privacy laws. Given the broad political disagreements about the proper direction for U.S. privacy policies, the Congress must set the direction for privacy. ~~However, t~~Areas that policy makers might explore are:

1. Assess how well existing privacy laws are accomplishing their specific objectives. The Privacy Act of 1974, already under review, is a prime target for this work. It is the broadest of all privacy laws, and some lessons can be learned from how the Act works in different contexts and in different agencies. Some of this work is already under way at GAO. ~~But t~~Other privacy laws could also be assessed in terms of how well they have accomplished their specific objectives. Conducting such a policy analysis and using criteria suggested in Figure 5.2 may be a useful first step to better understanding privacy legislation and policy.
2. Evaluate some FIPs principles across different privacy laws with an eye toward learning what features of privacy policy work better. The best example may be the openness principle. Consumer notices of privacy practices are familiar features of privacy laws. Some conclusions about the best way to inform consumers could be drawn from experience with the different notification practices. Another feature of privacy laws that might lend itself to comparative analysis is the individual participation principle (access and correction). Implementation of that principle raises substantive and procedural questions, and a review of real-world experience might be useful to policy makers and to those charged with the responsibility of providing access and correction rights.
3. Discuss the privacy consequences of new technologies at early stages. Technology constantly raises new privacy issues and concerns. Decisions by agencies, companies, and others about the application of new information technologies are often made wholly independent from existing laws. A current example would be the development of biometric technology. New uses of biometric technology are arising, but the related privacy concerns have received little formal attention. Another example comes from the Internet, where decisions about technical network architecture will have significant consequences for privacy?
4. Evaluating privacy structure in the U.S. Privacy structures in the U.S. and elsewhere around the world have received only occasional evaluations. Structures are particularly noteworthy because recent U.S. developments have been at the grass roots level. Companies on their own initiative have begun to establish chief privacy officers. The role played by federal and state agencies with privacy responsibilities could also be evaluated. An evaluation of privacy structures could be useful to policy makers who will be confronted with structural choices in formulating privacy legislation. A review of the effectiveness of those agencies with established privacy offices could offer lessons for policy makers.

5. Assess the effectiveness of enforcement methodologies under privacy laws. The Privacy Act of 1974 has a wealth of enforcement methodologies, and some have already been the subject of review. Newer features (e.g., the Privacy Counselor at OMB) have yet to be assessed. Evaluation of federal agency enforcement activities under the Family Educational Rights and Privacy Act and the Children's Online Privacy Protection Act might also be particularly ~~worthwhile.~~useful for a Congress that may consider an expansion in the privacy jurisdiction of the FTC and other agencies.

~~5.~~6. Three recent privacy laws affect the private sector: the Children's Online Privacy Protection Act, Gramm-Leach-Bliley, and the Health Insurance Portability and Accountability Act. The last of these will not take effect for another year, but there may be lessons to be learned from the process by which implementing regulations were adopted or by which companies implemented the laws. Did the laws provide data subjects with enhanced privacy protections that were worth the cost? It should be possible to collect information that would bear on this question and that would be useful to the Congress when other privacy legislation is debated.

~~6.~~7. Security is an important element of privacy, and it is clear from the existing record that federal security programs suffer significant lapses. This report has not focused on security because so much attention is being paid to security elsewhere; but the topic is mentioned here simply to highlight its fundamental importance to privacy.

5.3 Addressing Privacy Issues and Moving Forward

This study has examined the significant amount of writing, thought, and assessment of privacy law and policy both in the U.S. and elsewhere. The study suggests that little agreement exists in the U.S. about how best -- or if it is even necessary -- to proceed in addressing privacy laws and issues, although an assessment of structural characteristics does hold substantial promise.

~~To a large extent, the political context for dealing with privacy issues may need to proceed the detailing of possible approaches and structure for addressing privacy laws and issues or determining the need for new laws related to privacy.~~ Given recent events in the U.S., issues related to privacy (and especially as privacy relates to security issues), will continue to be on the forefront. The degree to which there is a national political agenda to address privacy issues and move forward to resolve the issues outlined in this report is unclear.

Appendix A: Selected Congressional Hearings Involving Privacy Since 1995

Congressional Hearings 1995 - 2001

Between 1995 and 2001, Congressional hearings have covered a number of privacy-related issues including the protection of medical records, electronic communications, and financial records and histories. Overall, the protection of medical records and personal medical information has received the most attention. Congressional hearings have also addressed a number of other privacy-related issues, such as: the European Union Data Protection Directive; legislation concerning parental protection of their children with the Internet; issues defining privacy legislation; and financial information other than personal records. Issues relating to privacy have come before a wide variety of Congressional Committees.

Hearings 107th Congress (2001):

Total Hearings – 3

Subcommittee on Health of the House Committee on Energy and Commerce
Subcommittee on Commerce, Trade and Consumer Protection of the House Committee on Energy and Commerce
Senate Committee on Health, Education, Labor and Pensions

Hearings 106th Congress (2000):

Total Hearings – 16

House Committee on Banking and Financial Services
Subcommittee on the Constitution of the House Committee on the Judiciary
Senate Committee on Health, Education, Labor, and Pensions
Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary
Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Banking and Financial Services
Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform (3)
Subcommittee on Health of the House Committee on Ways and Means
Subcommittee on Technology of the House Committee on Science
Subcommittee on Telecommunication, Trade, and Consumer Protection of the House Committee on Commerce (3)
Subcommittee on the Census of the House Committee on Government Reform

Subcommittee on the Constitution of the House Committee on the Judiciary (2)

Hearings 106th Congress (1999)
Total Hearings – 17

House Committee on Banking and Financial Services
Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs
Senate Committee on Aging
Senate Committee on Banking, Housing, and Urban Affairs
Senate Committee on Health, Education, Labor and Pensions
Senate Committee on the Health, Education, Labor, and Pensions
Senate Committee on the Judiciary
Subcommittee on Commercial and Administrative Law of the House Committee on the Judiciary
Subcommittee on Health and Environment of the House Committee on Commerce (2)
Subcommittee on Health of the House Committee on Ways and Means
Subcommittee on Intellectual Property of the House Committee on the Judiciary
Subcommittee on Labor, Health, and Human Services and Education of the Senate Committee on Appropriations
Subcommittee on Regulatory Reform and Paperwork Reduction of the House Committee on Small Business
Subcommittee on Technology of the House Committee on Science
Subcommittee on Telecommunication, Trade, and Consumer Protection of the House Committee on Commerce (2)

Hearings 105th Congress (1998)
Total Hearings – 20

House Committee on Banking and Financial Services
House Committee on Commerce
House Committee on the Judiciary
House Committee on Ways and Means
Senate Committee on Banking, Housing, and Urban Affairs
Senate Committee on Labor and Human Resources
Senate Committee on the Judiciary
Senate Labor and Human Resources Committee
Subcommittee on Administrative Oversight and the Courts of the Senate Committee on the Judiciary
Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary
Subcommittee on Crime of the House Committee on the Judiciary
Subcommittee on Early Childhood, Youth and Families of the House Committee on Education and the Workforce
Subcommittee on Financial and Hazardous Materials of the House Committee on Commerce
Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform and Oversight
Subcommittee on Health and the Environment of the House Committee on Commerce
Subcommittee on Human Resources of the House Committee on Ways and Means
Subcommittee on National Economic Growth, Natural Resources, and Regulatory Affairs of the House Committee on Government Reform and Oversight

Subcommittee on Science and Transportation of the Senate Committee on Commerce
Subcommittee on Security Issues in Asia of the House Committee on International Relations
Subcommittee on Telecommunication, Trade, and Consumer Protection of the House Committee on Commerce

Hearings 105th Congress (1997)
Total Hearings – 11

House Committee on Rules
House Committee on the Judiciary
Senate Committee on Labor and Human Resources
Senate Committee on the Judiciary
Subcommittee of the Senate Committee on Appropriations
Subcommittee on Electronic Payment Systems, Electronic Commerce, and Consumer Privacy of the House Committee on Banking and Financial Services
Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform and Oversight (2)
Subcommittee on Social Security of the House Committee on Ways and Means
Subcommittee on the Telecommunication, Trade, and Consumer Protection of the House Committee on Commerce

Hearings 104th Congress (1996)
Total Hearings – 11

House Committee on the Judiciary
Senate Committee on the Judiciary
Subcommittee on Civil Service on Federal Labor Union Activities of the House Committee on Government Reform and Oversight
Subcommittee on Crime of the House Committee on the Judiciary
Subcommittee on Crime Testimony of the House Committee on the Judiciary
Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform and Oversight (3)
Subcommittee on Postsecondary Education, Training, and Life-Long Learning of the House Committee on Econ. and Education Opportunities
Subcommittee on Science, Technology, and Space of the Senate Committee on Commerce, Science, and Transportation
Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform and Oversight

Hearings 104th Congress (1995)
Total Hearings – 7

Senate Committee on Government Affairs
Senate Committee on Labor and Human Resources
Subcommittee on Domestic and International Monetary Policy of the House Committee on Banking and Financial Services

Subcommittee on Financial Institutions and Regulatory Relief of the Senate Committee on Banking, Housing, and Urban Affairs
Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform and Oversight
Subcommittee on Health and the Environment of the House Committee on Commerce
Subcommittee on Oversight of Government Management and the District Of Columbia of the Senate Committee on Government Affairs

Congressional Hearings by Congress in reverse chronological order

107th Congress

Assessing HIPAA: How Federal Medical Record Privacy Regulations Can Be Improved: Hearing Before the Subcomm. on Health of the House Comm. on Energy and Commerce, 107th Cong. (2001), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_house_hearings&docid=f:71494.pdf.

EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearing Before the Subcomm. on Commerce, Trade and Consumer Prot. of the House Comm. on Energy and Commerce, 107th Cong. (2001), e at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_house_hearings&docid=f:71497.pdf.

Making Patient Privacy a Reality: Does the Final HHS Regulation Get the Job Done: Hearing Before the Senate Comm. on Health, Educ., Labor and Pensions, 107th Cong. (2001).

106th Congress

Changing Face of Healthcare in the Electronic Age: Hearing Before the Subcomm. on Tech. of the House Comm. on Sci., 106th Cong. (2000).

Confidentiality of Health Information: Hearing Before the Subcomm. on Health of the House Comm. on Ways and Means, 106th Cong. (1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house_hearings&docid =f:64128.pdf.

Confidentiality of Patient Records: Hearing Before the Subcomm. on Health of the House Comm. on Ways and Means, 106th Cong. (2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house_hearings& docid=f:66897.pdf.

Electronic Commerce: The Current Status of Privacy Protections for Online Consumers: Hearing Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce, 106th Cong. (1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house_hearings&docid=f:58511.pdf.

Electronic Communication Privacy Policy Disclosure: Hearing Before the Subcomm. on Intellectual Prop. of the House Comm. on the Judiciary, 106th Cong. (1999).

Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearings on H.R. 5018, H.R. 4987, and H.R. 4908 Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 106th Cong. (2000).

Financial Privacy: Hearings Before the Subcomm. on Fin. Institutions and Consumer Credit of the House Comm. on Banking and Fin. Services, 106th Cong. (1999).

Financial Privacy Issues: Hearings Before the Senate Comm. on Banking, Housing, and Urban Affairs, 106th Cong. (1999).

Fourth Amendment and the Internet: Hearing Before the House Judiciary Comm. on the Constitution, 106th Cong. (2000).

Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearings Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 106th Cong. (2000).

Genetics Testing in the New Millennium: Advances, Standards, and Implications: Hearing Before the Subcomm. on Tech. of the House Comm. on Sci., 106th Cong. (1999).

Know Your Caller Act of 1999 and the Telemarketing Victim Protection Act of 1999: Hearing Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce, 106th Cong. (2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house_hearings&docid=f:65901.pdf.

"Know Your Customer" Rules: Privacy in the Hands of Federal Regulators: Hearings Before the Subcomm. on Commercial and Admin. Law of the House Comm. on the Judiciary, 106th Cong. (1999).

Medical Information Protection and Research Enhancement Act of 1999: Hearing Before the Subcomm. on Health and Env't of the House Comm. on Commerce, 106th Cong. (1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house hearings &docid=f:58501.pdf.

Medical Records Confidentiality in a Changing Health Care Environment: Hearings Before the Senate Comm. on Health, Educ., Labor and Pensions, 106th Cong. (1999).

Medical Records Confidentiality in the Modern Delivery of Health Care: Hearing Before the Subcomm. on Health and Env't of the House Comm. on Commerce, 106th Cong. (1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house hearings &docid=f:57441.pdf.

Medical Records Privacy: Hearings Before the Subcomm. on Labor, Health, and Human Services and Educ. of the Senate Comm. on Appropriations, 106th Cong. (1999).

Oversight of the 2000 Census: Mail-Back Response Rates and Status of Key Operations: Hearing Before the Subcomm. on the Census of the House Comm. on Gov't Reform, 106th Cong. (2000), at

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname =106 _house_hearings&docid=f:70056.pdf.

Privacy and Electronic Communications: Hearings Before the Subcomm. on Courts and Intellectual Prop. of the House Comm. on the Judiciary, 106th Cong. (2000).

Privacy Commission: A Complete Examination of Privacy Protection: Hearing Before the Subcomm. on Gov't Mgmt., Information, and Tech. of the House Comm. on Gov't Reform, 106th Cong. (2000), at http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=106_house_hearings &docid=f:70436.pdf.

Privacy in the Digital Age: Discussion of Issues Surrounding the Internet: Hearing Before the Senate Comm. on the Judiciary, 106th Cong. (1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_senate_ hearings &docid=f:68199.pdf.

Privacy Under a Microscope: Balancing the Needs on Research and Confidentiality: Hearing Before the Senate Comm. on the Health, Educ., Labor, and Pensions, 106th Cong. (1999).

Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities: Hearings Before the Permanent Subcomm. on Investigations of the Senate Comm. on Governmental Affairs, 106th Cong. (1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname =106_senate_hearings&docid=f:61699.pdf.

Proposed Rule on the Privacy of Individually Identifiable Health Information: Hearing Before the Senate Comm. on Health, Educ., Labor, and Pensions, 106th Cong. (2000).

Recent Developments in Privacy Protections for Consumers: Hearing Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce, 106th Cong. (2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house_hearings&docid =f:67635.pdf.

The Fair Credit Reporting Amendments Act of 1999: Hearing on H.R. 3408 Before the Subcomm. on Fin. Institutions and Consumer Credit of the House Comm. on Banking and Fin. Services, 106th Cong. (2000).

The Freedom and Privacy Restoration Act: Hearing on H.R. 220 Before the Subcomm. on Gov't Mgmt, Information, and Tech. of the House Comm. on Gov't Reform, 106th Cong. (2000), at http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=106_house_hearings&docid=f:71388.pdf.

The Medical Financial Privacy Protection Act: Hearing on H.R. 4585 Before the House Comm. on Banking and Fin. Services, 106th Cong. (2000).

To Establish the Commission for the Comprehensive Study of Privacy Protection: Hearings on H.R. 4049 Before the Subcomm. on Gov't Mgmt, Information, and Tech. of the House Comm. on Gov't Reform, 106th Cong. (2000), at http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=106_house_hearings&docid=f:71178.pdf.

Too Much Information? The Impact of OASIS on Access to Home Health Care: Hearing Before the Senate Comm. on Aging, 106th Cong. (1999).

U.S. Postal Service's Regulations Regarding Commercial Mail Receiving Agencies (CMRAs): Hearing Before the Subcomm. on Regulatory Reform and Paperwork Reduction of the House Comm. on Small Bus., 106th Cong. (1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house_hearings&docid=f:61646.pdf.

Wireless Privacy Enhancement Act of 1999 and the Wireless Communications and Public Safety Enhancement Act of 1999: Hearing Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce, 106th Cong. (1999), at http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=106_house_hearings&docid=f:55150.pdf.

Wireless Telecommunications Sourcing and Privacy Act: Hearing Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce, 106th Cong. (2000), at http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=106_house_hearings&docid=f:64022.pdf.

105th Congress

Adoption Reunion Registries and Screening of Adults Working with Children: Hearing Before the Subcomm. on Human Resources of the House Comm. on Ways and Means, 105th Cong. (1998), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_house_hearings&docid=f:63457.pdf.

Business Bankruptcy Reform Act: Business Bankruptcy Issues in Review: Hearing Before the Subcomm. on Admin. Oversight and the Courts of the Senate Comm. on the Judiciary, 105th Cong. (1998).

Camera Rule Repeal: Hearing Before the House Comm. on Rules, 105th Cong. (1997), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_house_hearings&docid=f:46219.pdf.

Cellular Privacy: Is Anyone Listening? You Betcha: Hearing Before the Subcomm. on the Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce, 105th Cong. (1997).

Child Protection and Sexual Predator Punishment Act of 1998 and Related Proposals: Hearing Before the Subcomm. on Crime of the House Comm. on the Judiciary, 105th Cong. (1998).

Children's Online Privacy Protection Act of 1998: Hearing on S. 2326 Before the Subcomm. on Sci. and Transp. of the Senate Comm. on Commerce, 105th Cong. (1998).

Consumer Financial Privacy: Hearing Before the Subcomm. on Elec. Payment Systems, Elec. Commerce, and Consumer Privacy of the House Comm. on Banking and Fin. Services, 105th Cong. (1997).

Electronic Commerce: Part 1: Hearings Before the House Comm. on Commerce, 105th Cong. (1998).

Electronic Commerce, Part 2: Hearings Before the Subcomm. on Fin. and Hazardous Materials of the House Comm. on Commerce, 105th Cong. (1998).

Electronic Commerce, Part 3: Hearings Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce, 105th Cong. (1998).

Encryption, Key Recovery, and Privacy Protection in the Information Age: Hearing Before the Senate Comm. on the Judiciary, 105th Cong. (1997).

Financial Information Privacy Act: Hearings on H.R. 4321 Before the House Comm. on Banking and Fin. Services, 105th Cong. (1998).

Financial Services Act of 1998: Hearings on H.R. 10 Before the Senate Comm. on Banking, Housing, and Urban Affairs, 105th Cong. (1998).

Genetic Information and Health Care Hearing before the Senate Labor and Human Resources Committee, 105th Congress (1998).

Health Care Information Confidentiality: Hearing Before the Senate Comm. on Labor and Human Resources, 105th Cong. (1998).

HIV Partner Protection Act: Hearing Before the Subcomm. on Health and the Env't of the House Comm. on Commerce, 105th Cong. (1998).

Issues in U.S.-European Union Trade: European Privacy Legislation and Biotechnology/Food Safety Policy: Hearing Before the Subcomm. on Sec. Issues in Asia of the House Comm. on Int'l Relations, 105th Cong. (1998).

National ID Card: Big Government at Its Worst or Technological Efficiency: Hearing Before the Subcomm. on Nat'l Econ. Growth, Natural Res., and Regulatory Affairs of the House Comm. on Gov't Reform and Oversight, 105th Cong. (1998).

Oversight of Statistical Proposals: Hearing Before the Subcomm.on Gov't Mgmt., Info., and Tech. of the House Comm. on Gov't Reform and Oversight, 105th Cong. (1997).

Parental Freedom of Information Act: Hearings on H.R. 3189 Before the Subcomm. on Early Childhood, Youth and Families of the House Comm. on Educ. and the Workforce, 105th Cong. (1998).

Patient Confidentiality: Hearing Before the Subcomm. on Health of the House Comm. on Ways and Means, 105th Cong. (1998), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_house_hearings&docid=f:49195.

Privacy in Electronic Communications: Hearing Before the Subcomm. on Courts and Intellectual Prop. of the House Comm. on the Judiciary, 105th Cong. (1998).

Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Senate Comm. on the Judiciary, 105th Cong. (1998).

Protecting Health Information: Legislative Options for Medical Privacy: Hearing Before the Subcomm. on Gov't Mgmt., Info., and Tech. of the House Comm. on Gov't Reform and Oversight, 105th Cong. (1998).

Protecting Our Personal Health Information: Privacy in the Electronic Age: Hearing Before the Senate Comm. on Labor and Human Resources, 105th Cong. (1997).

Protection from Personal Intrusion Act and Privacy Protection Act of 1998: Hearing Before the House Comm. on the Judiciary, 105th Cong. (1998).

Reforming Asset Forfeiture Laws: Hearing Before the Subcomm. on Crime of the House Comm. on the Judiciary, 105th Cong. (1997).

Social Security Administration's Website: Hearing Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 105th Cong. (1997).

The Fair Health Information Practices Act of 1997: Hearing on H.R. 52 Before the Subcomm. on Gov't Mgmt., Info. and Tech. of the House Comm. on Gov't Reform and Oversight, 105th Cong. (1997).

Treasury and General Government Appropriations: Hearings on H.R. 4104 and S. 2312 Before the Subcomm. of the Senate Comm. on Appropriations, 105th Cong. (1997), at http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=105_senate_hearings&docid=f:46121.

104th Congress

Child Pornography Prevention Act of 1995: Hearing on S. 1237 Before the Senate Comm. on the Judiciary, 104th Cong. (1996).

Children's Privacy Protection and Parental Empowerment Act of 1996: Hearing Before the Subcomm. on Crime Testimony of the House Comm. on the Judiciary, 104th Cong. (1996).

Civil Asset Forfeiture Reform Act: Hearing Before the House Comm. on the Judiciary, 104th Cong. (1996).

Economic Growth and Regulatory Paperwork Reduction Act: Hearing on S. 650 Before the Subcomm. on Fin. Institutions and Regulatory Relief of the Senate Comm. on Banking, Housing, and Urban Affairs, 104th Cong. (1995).

Federal Information Policy Oversight: Hearing Before the Subcomm. on Gov't Mgmt., Info., and Tech. of the House Comm. on Gov't Reform and Oversight, 104th Cong. (1996).

Federal Record keeping and Sex Offenders: Hearing Before the Subcomm. on Crime of the House Comm. on the Judiciary, 104th Cong. (1996).

Future of Money, Part 1: Hearing Before the Subcomm. on Domestic and Int'l Monetary Policy of the House Comm. on Banking and Fin. Services, 104th Cong. (1995).

Health Information Privacy Protection Act, Hearing before the Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform and Oversight, 104th Congress (1996).

Hearing on Campus Crime and H.R. 2416, To Amend the Higher Education Act of 1965 To Require Open Campus Security Crime Logs at Institutions of Higher Learning: Hearing Before the Subcomm. on Postsecondary Educ., Training, and Life-Long Learning of the House Comm. on Econ. and Educ. Opportunities, 104th Cong. (1996).

HIV Testing of Women and Infants: Hearing Before the Subcomm. on Health and the Env't of the House Comm. on Commerce, 104th Cong. (1995).

Medical Records Confidentiality Act of 1995: Hearing Before the Senate Comm. on Labor and Human Resources, 104th Cong. (1995).

Promotion of Commerce Online in the Digital Era Act of 1996 or "Pro-CODE" Act: Hearing on S. 1726 Before the Subcomm. on Sci., Tech., and Space of the Senate Comm. on Commerce, Sci., and Transp., 104th Cong. (1996).

Taxpayer Subsidy of Federal Unions: Hearing Before the Subcomm. on Civil Service on Fed. Labor Union Activities of the House Comm. on Gov't Reform and Oversight, 104th Cong. (1996).

The Administrative Dispute Resolution Act of 1995: Hearing on S. 1224 Before the Subcomm. on Oversight of Gov't Management and D.C. of the Senate Comm. on Gov't Affairs, 104th Cong. (1995).

The Family Privacy Protection Act of 1995: Hearing on H.R. 1271 Before the Senate Comm. on Gov't Affairs, 104th Cong. (1995).

The Family Reinforcement Act: Title IV: Hearing on H.R. 11 Before the Subcomm. on Gov't Mgmt., Info., and Tech. of the House Comm. on Gov't Reform and Oversight, 104th Cong. (1995).

Travel Reform and Savings Act of 1996: Hearing on H.R. 3637 Before the Subcomm. on Gov't Mgmt., Info., and Tech. of the House Comm. on Gov't Reform and Oversight, 104th Cong. (1996).

War Crimes Disclosure Act, Health Information Privacy Protection Act, and Electronic Freedom of Information Improvement Act of 1995: Hearing on H.R. 128 and S. 1090 Before the Subcomm. on Gov't Mgmt., Info., and Tech. of the House Comm. on Gov't Reform and Oversight, 104th Cong. (1996)

Appendix B: Bibliography of Selected Current Secondary Legal Sources Concerning Privacy (1991 – 2001)

Phil Agre & Marc Rotenberg (eds.), Technology and Privacy: The New Landscape (1999).

Ellen Alderman & Caroline Kennedy, *The Right to Privacy* (1995).

Anita L. Allen, Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm, 32 *Conn. L. Rev.* 861 (2000).

James M. Assey & Demetrios A. Eleftheriou, The EU-U.S. Privacy Safe Harbor, 9 *Commlaw Conspectus* 145 (2001).

Ronald Backes, Freedom, Information, Security, 10 *Seton Hall Const' L. J.* 927 (Summer 2000).

David Banisar & Simon Davies, Global Trends in Privacy Protection, 18 *J. Marshall Comp. & Info. L.* 1 (1999).

David Banisar, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments* (2000).

Kalinda Basho, The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?, 88 *Calif. L. Rev.* 1507 (2000).

Joshua S. Bauchner, State Sovereignty and the Globalizing Effects of the Internet, 26 *Brooklyn J. Int'l L.* 689 (2000).

Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (1992).

Colin J. Bennett, Adequate Data Protection by the Year 2000: The Prospects for Privacy in Canada, 11 *International Review of Law Computers & Technology* 79 (1997).

Colin J. Bennet & Rebecca Grant (eds.), *Visions of Privacy: Policy Choices for the Digital Age* (1999).

Stephen R. Bergerson, E-Commerce Privacy and the Black Hole of Cyberspace, 27 *Wm. Mitchell L. Rev.* 1527 (2001).

Lillian R. BeVier, Information about Individuals in the Hands of the Government, 4 *William & Mary Bill Rts. J.* 455 (1995).

Randall P. Bezanson, The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990, 80 *Calif. L. Rev.* 1133 (1992).

Steven A. Bibas, A Contractual Approach to Data Privacy, 17 *Harv. J. L. & Pub. Pol'y* 591 (1994).

Jordan M. Blanke, Safe Harbor and the EU's Directive on Data Protection, 11 *Alb. L. J. Sci. & Tech.* 57 (2000).

Kevin Bloss, Raising or Razing the e-Curtain: The EU Directive on the Protection of Personal Data, 9 *Minn. J. Global Trade* 645 (2000).

Robert G. Boehmer & Todd S. Palmer, The 1992 EC Data Protection: An Examination of Its Implications for U.S. Business and U.S. Privacy Law, 31 *Am. Bus. L. J.* 265 (1993).

Christopher Paul Bogam, The Internet, Information, and the Culture of Regulatory Change, 9 *Commlaw Conspectus* 175 (2001).

Robert T. J. Bond, Internet Regulation—Heavy Handed or Light Touch Approach? A View from A European Union Perspective, 27 *Wm. Mitchell L. Rev.* 1557 (2001).

Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access* (1994).

David Brin, *The Transparent Society: Will Technology Force Us to Choice between Technology and Freedom?* (1998).

Nicole M. Buba, Waging War against Identity Theft: Should the U.S. Borrow from the E.U.'s Battalion, 23 *Suffolk Transnat'l L. Rev.* 633 (2000).

John M. Carroll, *Confidential Information Sources: Public and Private* (1991).

Fred H. Cate, From Conduit to Content: The Emergence of Information Policy and Law, 48 *Fed. Comm. L. J.* 1 (1992).

Fred H. Cate, The National Information Infrastructure: Policymakers and Policymaking, 6 *Stan. L. & Pol'y Rev.* 43 (1994).

Fred H. Cate, D. Annette Fields, and James K. McBain, The Right to Privacy and the Public's Right to Know: The Central Purpose of the Freedom of Information Act, 46 *Admin. L. Rev.* 41 (1994).

Fred H. Cate, Global Information Policymaking and Domestic Law, 1 *Ind. J. Global L. Studies* 467 (1994).

Fred H. Cate, The EU Data Protection Directive, Information Privacy, anf the Public Interest, 80 *Iowa L. Rev.* 431 (1995).

Fred H. Cate, The First Amendment and the National Information Infrastructure, 30 *Wake Forest L. Rev.* 1 (1995).

Fred H. Cate, *Privacy in the Information Age* (1997).

Fred H. Cate, Changing the Face of Privacy Protection in the EU and the U.S., 33 *Ind. L. Rev.* 174 (1999).

Fred H. Cate, Principles of Internet Privacy, 32 *Conn. L. Rev.* 877 (2000).

Francis S. Chlapowski, The Constitutional Protection of Informational Privacy, 71 *Boston U. L. Rev.* 133 (1991).

Marie Clear, Falling into the Gap: The EU's Data Protection Act & Its Impact on U.S. Law & Commerce, 18 *J. Marshall Comp. & Info. L.* 981 (2000).

Joseph P. Cody, Protecting Privacy over the Internet: Has the Time Come to Abandon Self-regulation?, 48 *Cath. U. L. Rev.* 1183 (1999).

Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 *Stan. L. Rev.* 1373 (2000).

Paul Andre Comeau & Andre Ouimet, Freedom of Information and Privacy: Quebec's Innovative Role in North America, 80 *Iowa L. Rev.* 651 (1995).

Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, & the Rise of Technology* (1997).

Rochelle Cooper Dreyfuss, Warren and Brandeis Redux: Finding (More) Privacy Protection In Intellectual Property Lore, 1999 *Stanford Technology Law Review* 8.

Lyombe Eko, Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation, 6 *Comm. L. & Pol'y* 445 (2001).

Rishard A. Epstein, Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism, 52 *Stan. L. Rev.* 1003 (2000).

Amitai Etzioni, A Communitarian Perspective on Privacy, 32 *Conn. L. Rev.* 897 (2000).

William J. Fenrich, Common Law Protection of Individuals' Rights in Personal Information, 65 *Fordham L. Rev.* 951 (1996).

Gregg M. Fishbein & Susan Ellingstad, Internet Privacy: Does the Use of Cookies Give Rise to a Private Cause of Action for Invasion of Privacy in Minnesota?, 27 *Wm. Mitchell L. Rev.* 1609 (2001).

Curtis D. Frye, *Privacy-Enhanced Business: Adapting to the Online Environment* (2001).

Richard T. Ford, Save the Robots: Cyber Profiling and Your So-Called Life, 52 *Stan. L. Rev.* 1573 (2000).

Charles Franklin (ed.), *Business Guide to Privacy and Data Protection Legislation* (1996).

A. Michael Froomkin, The Death of Privacy?, 52 *Stan. L. Rev.* 1461 (2000).

Robert M. Gellman, Fragmented, Incomplete, & Discontinuous: the Failure of Federal Privacy Regulatory Proposals and Institutions, 6 *Software L.J.* 199 (1993).

Robert M. Gellman, Can Privacy Be Regulated Effectively on a National Level?: Thoughts on the Possible Need for International Privacy Rules, 41 *Vill. L. Rev.* 129 (1996).

Michael J. Gerhardt, Privacy, Cyberspace, and Democracy: A Case Study, 32 *Conn. L. Rev.* 907 (2000).

Julia Gladstone, The Impact of E-Commerce on the Law of Nations, 7 *Willamette J. Int'l L. & Dispute Res.* 10 (2000).

Bruce D. Goldstein, Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection, 41 *Emory L. J.* 1185 (1992).

Ken Gormley, One Hundred Years of Privacy, 1992 *Wis. L. Rev.* 1335.

Ken Gormley & Rhonda G. Hartman, Privacy and the States, 63 *Temple L. Rev.* 1279 (1992).

Barry N. Hague & Brian D. Loader, *Digital Democracy: Discourse and Decision Making in the Age of Information* (1999).

James Harvey, Symposium: Privacy in Cyberspace, 61 *Mont. L. Rev.* 285 (2000).

Mike Hatch, The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interests in the 21st Century, 27 *Wm. Mitchell L. Rev.* 1457 (2001).

Michael W. Heydrich, A Brave New World: Complying with the EU's Directive on Personal Privacy through the Power of Contract, 25 *Brooklyn J. Int'l L.* 407 (1999).

Eric Jorstad, The Privacy Paradox, 27 *Wm. Mitchell L. Rev.* 1503 (2001).

M. Ethan Katsh, *Law in a Digital World* (1995).

Michael Kirby, The Impact of Technology on Human Rights, 4 *Privacy Law and Public Reporter* 183 (1998).

Jane E. Kirtley, The EU Data Protection Directive and the First Amendment, 80 *Iowa L. Rev.* 639 (1995).

Jane E. Kirtley, *Is Implementing the EU Data Protection Directive in the United States Irreconcilable with the First Amendment?*, 16 Government Information Quarterly 87 (1999).

Allegra Knopf, Privacy and the Internet: Welcome to the Orwellian World, 11 *J. Law. & Pub. Pol'y* 79 (1999).

Flavio L. Komuves, We've Got Your Number, 16 *J. Marshall J. Comp. & Info. L.* 529 (1998).

Dianne Plunkett Latham, Spam Remedies, 27 *Wm. Mitchell L. Rev.* 1649 (2001).

Marc Lemley, Private Property, 52 *Stan. L. Rev.* 1545 (2000).

Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999).

Lance Liebman, An Institutional Emphasis, 32 *Conn. L. Rev.* 923 (2000).

Kathleen A. Linert, Database Marketing and Personal Privacy in the Information Age, 18 *Suffolk Transnat'l L. Rev.* 687 (1995).

Jessica Litman, Information Privacy/Information Property, 52 *Stan. L. Rev.* 1283 (2000).

James R. Maxiener, Business Information and Personal Data: Some Common-Law Observations about the EU Draft Data Protection Directive, 80 *Iowa L. Rev.* 619 (1995).

James R. Maxeiner, Freedom of Information and the EU Data Directive, 48 *Fed. Comm. L. J.* 93 (1995).

Deckle McLean, *Privacy and Its Invasion* (1995).

Robert J. McGillivray & Stephen C. Lieske, Webjacking, 27 *Wm. Mitchell L. Rev.* 1661 (2001).

Julie J. McMurry, Privacy in the Information Age, 78 *Wash. U. L. Q.* 597 (2000).

Peter Mei, The EC Proposed Data Protection Law, 25 *L. & Pol'y in Internat'l Bus.* 305 (1993).

Patricia Mell, Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness, 11 *Berkeley Tech L. J.* 1 (1996).

James Michael, *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994).

P. Amy Monahan, Deconstructing Information Walls: The Impact of the EU Directive on the Protection of Personal Data, 29 *Law & Pol'y Int'l Bus.* 275 (1998).

Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 *Georgetown L. J.* 2381 (1996).

Jennifer M. Myers, Creating Data Protection Legislation in the U.S.: An examination of Current Legislation in the EU, Spain, and the U.S., 29 *Case W. Res. J. Int'l L.* 109 (1997).

Neil Weinstock Netanel, Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, 88 *Calif. L. Rev.* 395 (2000).

Panel Discussion, The EC Privacy Directive and the Future of U.S. Business in Europe, 80 *Iowa L. Rev.* 669 (1995).

Robert G. Patman, *Universal Human Rights?* (2000).

Elizabeth Paton-Simpson, Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places, 50 *U. Toronto L. J.* 305 (2000).

Allen Frankel Paul, Fred D. Miller, & Jeffery Paul (eds.), *The Right to Privacy* (2000).

Eric D. Paulsrud, The First Amendment on the Internet: Challenges in a New Media, 27 *Wm. Mitchell L. Rev.* 1637 (2001).

Henry H. Perritt, *Law and the Information Superhighway: Privacy, Access, Intellectual Property, Commerce, Liability* (1996).

Sandra Byrd Petersen, Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?, 48 *Fed. Comm. L. J.* 163 (1995).

David G. Post, What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace, 52 *Stan. L. Rev.* 1439 (2000).

Judith Beth Prowda, A Lawyer's Ramble Down the Information Superhighway: Privacy and Security of Data, 64 *Fordham L. Rev.* 697 (1995).

David Rameden, When the Database is Wrong, 100 *Com. L.J.* 390 (1995).
Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (1995).

Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 *Fed. Comm. L. J.* 195 (1992).

Joel R. Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 *Iowa L. Rev.* 497 (1995).

Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Texas Law Review 553 (1998).

Joel R. Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 *Stan. L. Rev.* 1315 (2000).

Robert A Reilly, Conceptual Foundations of Privacy, 6 *Rich. J.L. & Tech.* 6 (1999).

Paul Rose, A Market Response to the EU Directive on Privacy, 4 *UCLA J. Int'l L. & For. Aff.* 445 (1999/2000).

Michael P. Roch, Filling the Void of Data Protection in the U.S.: Following the European Example, 12 *Comp. & High Tech L. J.* 71 (1996).

Jeffery Rothfeder, *Privacy for Sale: How Computerization Has Made Everyone's Life an Open Secret* (1992).

Seth Safer, Between Big Brother and the Bottom Line: Privacy in Cyberspace, 5 *Va. J. L. & Tech* 6 (2000).

Pamela Samuelson, Privacy as Intellectual Property?, 52 *Stan. L. Rev.* 1125 (2000).

Paul M. Schwartz, Data Processing & Government Administration: Failure of the American Legal Response to the Computer, 43 *Hastings L.J.* 1321 (1992).

Paul M. Schwartz, European Data Protection Law and Restrictions on International Data Flows, 80 *Iowa L. Rev.* 471 (1995).

Paul M. Schwartz, Privacy and Participation: Personal Information and Public sector Regulation in the United States, 80 *Iowa L. Rev.* 553 (1995).

Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (1996).

Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 *Vand. L. Rev.* 1607 (1999).

Paul M. Schwartz, Internet Privacy and the State, 32 *Conn. L. Rev.* 815 (2000).
Paul M. Schwartz, Charting a Privacy Research Agenda: Responses, Agreements, and Reflections, 32 *Conn. L. Rev.* 929 (2000).

Paul M. Schwartz, Free Speech v. Information Policy, 52 *Stan. L. Rev.* 1559 (2000).

Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, 2000 *Wis. L. Rev.* 743.

Gregory Shaffer, Globalization and Social Protection: The Impact of the EU and International Rules in Ratcheting Up U.S. Privacy Standards, 25 *Yale J. Int'l L.* 1 (2000).

Anna E. Shimanek, Do You Want Milk with These Cookies: Complying with Safe Harbor Privacy Principles, 26 *Iowa J. Corp. L.* 455 (2000)

Scott Shorr, Personal Information Contracts: How to Protect Privacy with Violating the First Amendment, 80 *Cornell L. Rev.* 1756 (1995).

Spiros Simitis, From Market to the Polis: The EU Directive on the Protection of Personal Data, 80 *Iowa L. Rev.* 445 (1995).

Solveig Singleton, Reviving a First Amendment Absolutism for the Internet, 3 *Tex. Rev. Law & Pol.* 279 (1999).

Solveig Singleton, Privacy Versus the First Amendment: A Skeptical Approach, 11 *Fordham I. P., Media, & Ent. L.J.* 97 (2000).

Eric J. Sinrod & Barak D. Jolish, Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace, 1999 *Stan. Tech. L. Rev.* 1 (1999)

Jeff H. Smith, *Managing Privacy: Information Technology and Corporate America* (1994).

Rodney A. Smolla, *Free Speech in an Open Society* (1993).

David L. Sobel, The Process that John Doe is Due: Addressing the Legal Challenge to Internet Anonymity, 5 *Va. J. L. & Tech* 3 (2000).

Jeff Sovern, Opting In, Opting Out, or no Options at all: The Fight for Control of Personal Information, 74 *Wash. L. Rev*. 1033 (1999).

Jeff Sovern, Protecting Privacy with Deceptive Trade Practices Legislation, 69 *Fordham L. Rev*. 1305 (2001).

Shaun A. Sparks, The Direct Marketing Model and Virtual Identity, 18 *Dick. J. Int'l L.* 517 (2000).

James T. Sunosky, Privacy Online: A Primer on the EU's Directive and the United States' Safe Harbor Privacy Principles, 9 *Currents Int'l Trade L. J.* 80 (2000).

Robert E. Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (2000).

Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (1998).

Domingo R. Tan, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the U.S. and the EU, 21 *Loy. L.A. Int'l & Comp. L.J.* 661 (2001).

Douglas Thomas and Brian D. Loader, *Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age* (2000).

R. Craig Tollier, Filling the Black Hole of Cyberspace: Legal Protections for Online Privacy, 1 *Vand. J. Ent. L. & Prac.* 66 (1999).

George B. Trubow, The European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans-Border Data Flow, 13 *Nw. J. Int'l L. & Bus.* 159 (1992).

George B. Trubow, Protecting Informational Privacy in the Information Society, 10 *Ill. L. Rev.* 521 (1994).

Richard C. Turkington, Legacy of the Warren and Brandeis article: The Emerging Unencumbered Constitutional Right to Informational Privacy, 10 *N. Ill. U. L. Rev.* 479 (1990).

Richard C. Turkington & Anita L Allen, *Privacy Law* (1999).

Hillary Victor, Big Brother is at Your Backdoor, 18 *J. Marshall Comp. & Info. L.* 825 (2000).

Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You, 52 *Stan. L. Rev.* 1049 (2000).

Jonathan Weinberg, Hardware-Based ID, Rights Management, and Trusted Systems, 52 *Stan. L. Rev.* 1251 (2000).

Diane Zimmerman, Information as Speech, Information as Goods: Some thoughts on Marketplaces and the Bill of Rights, 33 *Wm. & Mary L. Rev.* 665 (1992).

Rachel K. Zimmerman, The Way the Cookies Crumble: Internet Privacy and Data Protection in the 21st Century, 4 *NYU J. Legis & Pub. Pol'y* 439 (2000/2001).

Jonathan Zittrain, Rejoinder—Privicating Privacy, 52 *Stan. L. Rev.* 1595 (2000).

Appendix C: State Privacy Office Interview Script

Contact Information

1. Appropriate privacy office information, activities, and enabling laws
2. Contacts related to privacy activities
3. Privacy statement on the state homepage

Structure

1. How long has office been in operation, and where is it located organizationally in the government? To whom or what does the privacy office or commission report?
2. Is there a formal head of a privacy office, how appointed, term of service?
   Have there been any temporary commissions or offices dealing with privacy issues in the last 10 years?
3. What degree of independence does the office have or are there direct linkages to the governor's office, the attorney general, or the legislature?
4. What is the staff size and budget of the privacy office or commission?
5. Does the privacy office has responsibilities or is organized to deal with other areas beyond privacy, e.g., Freedom Of Information?
6. Does the privacy office or commission have any type of advisory group? If yes, how is the advisory group organized?

Laws and Regulations

1. What is the enabling law (or regulation) that created the privacy office or commission and what specific responsibilities, activities, and power have been ascribed to the office or commission?
2. Does the enabling law (if there is one) rely on FIPS concepts?
3. What are the current and most important privacy laws that have been enacted by the state and to what degree to they describe the activities, responsibilities, and power of the privacy office or commission – to the extent they affect structure and activities of state government?
4. Is there language directly in the state constitution about privacy responsibilities?

Activities/Functions

1. What are the functions and responsibilities of the privacy office or commission?
2. Do privacy officers believe they are listened to by others in government, are they consulted prior to legislation being passed, or are they basically ignored?
3. Do they receive privacy complaints and what actions can be taken if they do?
4. What kind of formal and informal relationships of review and giving advice has the privacy office or commission?
5. Does the privacy office offer training, education, or other types of support to other state agencies?
6. Enforcement powers of the privacy office
   - Issue orders
   - Hold hearings
   - Conduct investigations
   - Issue subpoenas
   - Regulate the private sector
   - Petition judicial review/actions
   - Refer cases for prosecution
   - Report to governor or legislature
   - Other

Publications

1. Are there any reports, studies, investigations, or commission reports available that describe state government privacy activities in that particular state?
2. Does the privacy office issue an annual report and to whom or what is it distributed to?
3. Are there any reports by "watch" groups or public citizen type groups on state government privacy, privacy structure, courts, or commissions in this particular state?

Lessons for Federal Privacy Offices/Efforts

a. Are there any structures/activities being done in this state that have applications at the Federal level, or to the private sector?
b. Has the privacy office had any "big successes" or "major disappointments?"
c. Is there a model of structures/activities/enforcement that can be generalized to other situations? How would this model be described?

Appendix D: Selected International Policy & Data Protection Agencies and Laws

Australia

The Office of the Federal Privacy Commissioner: http://www.privacy.gov.au.

The Privacy Act, as amended, at http://www.privacy.gov.au/news/pab.html/#6.

Canada

The Office of the Privacy Commissioner of Canada: http://www.privcom.gc.ca.

The Privacy Act, as amended, at http://www.privcom.gc.ca/legislation/02_07_01_e.asp.

The Personal Information Protection and Electronic Documents Act, at http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

The Czech Republic

The Office for Personal Data Protection: http://www.uoou.cz/eng/index.php3.

Act No. 101 of April 4, 2000 on the Protection of Personal Data and on Amendments to Some Related Acts, as amended, at http://www.uoou.cz/eng/101_2000.php3.

France

The National Data Processing and Liberties Commission: http://www.cnil.fr.

The Act on Data Processing, Data Files, and Individual Liberties, as amended, is available in French at http://www.cnil.fr/textes/index.htm. An unofficial English version is at http://ccweb.in2p3.fr/secur/legal/a78-17-text-local.html#renv.

Germany

The Federal Data Protection Commissioner**:** http://www.bfd.bund.de.

The *Federal Data Protection Act of 1990*, as amended, at http://bfd.bund.de/information/bdsg_eng.html.

Hong Kong

The Privacy Commissioner's Office: http://www.pco.org.hk.

The Personal Data (Privacy) Ordinance, as amended, at http://www.pco.org.hk/english/ordinance/ordfull.html.

Hungary

The Parliamentary Commissioner for Data Protection and Freedom of Information: http://www.obh.hu/adatved/indexek/index.htm.

The Data Protection and Freedom of Information Law of 1992, as amended, at http://www.obh.hu/adatved/indexek/index.htm.

Ireland

Office of the Data Protection Commissioner: http://www.dataprivacy.ie.

Data Protection Act, as amended, at http://www.dataprivacy.ie/6ai.htm.

Italy

The Italian Data Protection Commission: http://astra.garanteprivacy.it/garante/HomePageNs.

The Processing of Personal Data Act.

The Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data, at http://astra.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG=2.

The Act Enabling the Government in the Field of the Protection of Individuals and Other Subjects with regard to the Processing of Personal Data, at http://astra.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG=2.

Netherlands

The Dutch Data Protection Commission: http://www.registratiekamer.nl.

The Personal Data Protection Act, as amended, at http://www.registratiekamer.nl/bis/top-1-11.htm.

New Zealand

The Office of the Privacy Commissioner: http://www.privacy.org.nz.

The Privacy Commissioner Act of 1991.

The Privacy Act 1993, as amended, at http://www.privacy.org.nz/slegisf.html.

Poland

The Bureau of the Inspector General for the Protection of Personal Data: http://www.giodo.gov.pl/English/english.htm.

The *Act on Personal Data Protection of August 29, 1997*, at http://www.giodo.gov.pl/English/english.htm.

Portugal

The National Data Protection Commission, at http://www.cnpd.pt.

The Law for the Protection of Personal Data with Regard to Automatic Processing (1991).

The Act on the Protection of Personal Data, as amended, at http://www.cnpd.pt.

United Kingdom

Office of the Information Commissioner**:** http://www.dataprotection.gov.uk.

Freedom of Information Act 2000.

Data Protection Act of 1998, Ch. 29, as amended, at http://wood.ccta.gov.uk/dpr/dpdoc.ns.

Appendix E: GAO Reports Involving Privacy Issues

Elections: Voting Assistance to Military and Overseas Citizens Should Be Improved, GAO-01-1026 (Sept. 28, 2001), at http://www.gao.gov/new.items/d011026.pdf.

Financial Privacy: Too Soon to Assess the Privacy Provisions in the Gramm-Leach-Bliley Act Of 1999, GAO-01-617 (May 3, 2001), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d01617.pdf.

Internet Privacy: Implementation of Federal Guidance for Agency Use of "Cookies", GAO-01-424 (Apr. 27, 2001), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d01424.pdf.

Medical Privacy Regulation: Questions Remain about Implementing the New Consent Requirement, GAO-01-584 (Apr. 6, 2001), athttp://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=gao&docid=f:d01584.pdf.

VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist, GAO-01-550T (Apr. 4, 2001), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d01550t.pdf.

Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information, GAO-01-126SP (Apr. 1, 2001), at http://www.gao.gov/new.items/d01126sp.pdf.

Information Security: IRS Electronic Filing Systems, GAO-01-306 (Feb. 16, 2001), at http://www.gao.gov/new.items/d01306.pdf.

Health Privacy: Regulation Enhances Protection of Patient Records but Raises Practical Concerns, GAO-01-387T (Feb. 8, 2001), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d01387t.pdf.

Medicare Home Health Care: OASIS Data Use, Cost, and Privacy Implications, GAO-01-205 (Jan. 30, 2001), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d01205.pdf.

The Challenge of Data Sharing: Results of a GAO-Sponsored Symposium on Benefit and Loan Programs, GAO-01-67 (Oct. 20, 2000), at http://www.gao.gov/new.items/d0167.pdf.

Internet Privacy: Federal Agency Use of Cookies, GAO-01-147R (Oct. 20, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d01147r.pdf.

Financial Management: Significant Weaknesses in Corps of Engineers' Computer Controls, GAO-01-89 (Oct. 11, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d0189.txt.

Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles, GAO-01-113T (Oct. 11, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d01113t.pdf.

Benefit and Loan Programs: Improved Data Sharing Could Enhance Program Integrity, HEHS-00-119 (Sept. 13, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he00119.pdf.

Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles, AIMD-00-296R (Sept. 11, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ai00296r.pdf.

Medicare: HCFA Could Do More to Identify and Collect Overpayments, HEHS/AIMD-00-304 (Sept. 7, 2000), at http://www.gao.gov/new.items/h100304.pdf.

Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy, GGD-00-191 (Sept. 5, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:gg00191.pdf.

Social Security Numbers: Subcommittee Questions Concerning the Use of the Number for Purposes Not Related to Social Security, HEHS/AIMD-00-253R (July 7, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:h100253r.pdf.

Social Security: Government and Other Uses of the Social Security Number Are Widespread, T-HEHS-00-120 (May 18, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he00120t.pdf.

On-Line Trading: Better Investor Protection Information Needed on Brokers' Websites, GGD-00-43 (May 9, 2000), at http://www.gao.gov/new.items/gg00043.pdf.

Social Security: Use of the Social Security Number Is Widespread, T-HEHS-00-111 (May 9, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he00111t.pdf.

Privacy Standards: Issues in HHS' Proposed Rule on Confidentiality of Personal Health Information, T-HEHS-00-106 (Apr. 26, 2000), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he00106t.pdf.

Office of Management and Budget: Future Challenges to Management, T-GGD/AIMD-00-141 (Apr. 7, 2000), at http://www.gao.gov/new.items/g100141t.pdf.

Military Dependents: Services Provide Limited Confidentiality in Family Abuse Cases, NSIAD-00-127 (Apr. 5, 2000), at http://www.gao.gov/new.items/ns00127.pdf.

Gun Control: Implementation of the National Instant Criminal Background Check System, GGD/AIMD-00-64 (Feb. 29, 2000), at http://www.gao.gov/new.items/g100064.pdf.

District Of Columbia: The District Has Not Adequately Planned for and Managed Its New Personnel and Payroll System, AIMD-00-19 (Dec. 17, 1999), at http://www.gao.gov/archive/2000/ai00019.pdf.

Medicaid and Special Education: Coordination of Services for Children with Disabilities Is Evolving, HEHS-00-20 (Dec. 10, 1999), at http://www.gao.gov/archive/2000/he00020.pdf.

Survey Methodology: An Innovative Technique for Estimating Sensitive Survey Items, GGD-00-30 (Nov. 1, 1999), at http://www.gao.gov/archive/2000/gg00030.pdf.

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences, AIMD-00-1 (Oct. 1, 1999), at http://www.gao.gov/archive/2000/ai00001.pdf.

Taxpayer Confidentiality, Federal, State, and Local Agencies Receiving Taxpayer Information, GGD-99-164; B-282749 (Aug. 30, 1999), at http://www.gao.gov/archive/1999/gg99164.pdf.

Information Security: The Proposed Computer Security Enhancement Act of 1999, T-AIMD-99-302 (Aug. 30, 1999), at http://www.gao.gov/archive/1999/ai99302t.pdf.

Physician Performance: Report Cards under Development but Challenges Remain, HEHS-99-178 (Aug. 30, 1999), at http://www.gao.gov/archive/1999/he99178.pdf.

U.S. Postal Service: Status of Efforts to Protect Privacy of Address Changes, GGD-99-102 (July 30, 1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:gg99102.pdf.

Medicare: HCFA Needs to Better Protect Beneficiaries Confidential Health Information, T-HEHS-99-172 (July 20, 1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he99172t.pdf.

Medicare: Improvements Needed to Enhance Protection of Confidential Health Information, HEHS-99-140 (July 20, 1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he99140.pdf.

Military Housing: Status of the Services' Implementation of the Current Barracks Design Standard, NSIAD-99-52 (Apr. 24, 1999), at http://www.gao.gov/archive/1999/ns99052.pdf.

Gender Issues: Medical Support for Female Soldiers Deployed to Bosnia, NSIAD-99-58 (Mar. 10, 1999), at http://www.gao.gov/archive/1999/ns99058.pdf.

Medical Records Privacy: Access Needed for Health Research but Oversight of Privacy Protections Is Limited, HEHS-99-55 (Feb. 24, 1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he99055.pdf.

Medical Records Privacy: Uses and Oversight of Patient Information in Research, T-HEHS-99-70 (Feb. 24, 1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he99070t.pdf.

Social Security: Government and Commercial Use of the Social Security Number Is Widespread, HEHS-99-28 (Feb. 16, 1999), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he99028.pdf.

VA Health Care for Women: Progress Made in Providing Services to Women Veterans, HEHS-99-38 (Jan. 29, 1999), at http://www.gao.gov/archive/1999/he99038.pdf.

Child Support Enforcement: Information on Federal and State Databases, AIMD-99-42R (Dec. 31, 1998), at http://161.203.16.4/paprpdf2/161520.pdf.

Certificated Expenditures: FY 1996 Presidential and Vice Presidential Certificated Expenditures and Related Matters, AIMD-99-26 (Oct. 29, 1998), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ai99026.pdf.

Gender Issues: Information on DOD's Assignment Policy and Direct Ground Combat Definition, NSIAD-99-7 (Oct. 19, 1998), at http://www.gao.gov/archive/1999/ns99007.pdf.

Social Security Administration: Subcommittee Questions Concerning Information Technology Challenges Facing the Commissioner, AIMD-98-235R (July 10, 1998), at http://161.203.16.4/paprpdf2/160834.pdf.

Money Laundering: Regulatory Oversight of Offshore Private Banking Activities, GGD-98-154 (June 29, 1998), at http://www.gao.gov/archive/1998/gg98154.pdf.

Occupational Safety and Health: Efforts to Obtain Establishment-Specific Data on Injuries and Illnesses, HEHS-98-122 (May 22, 1998), at http://www.gao.gov/archive/1998/he98122.pdf.

Women Veterans' Health Care: VA Efforts to Respond to the Challenge of Providing Sexual Trauma Counseling, HEHS-98-177R (May 21, 1998), at http://161.203.16.4/paprpdf2/160523.pdf.

Identity Fraud: Information on Prevalence, Cost, and Internet Impact Is Limited, GGD-98-100BR (May 1, 1998), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:gg98100b.pdf.

Social Security Administration: Information on Monitoring 800 Number Telephone Calls, HEHS-98-56R; B278085 (Dec. 8, 1997), at http://161.203.16.4/paprpdf1/159635.pdf.

The White House: Status Review of the Executive Residence, T-OGC/AIMD-98-12 (Nov. 6, 1997), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:c198012t.pdf.

Social Security Administration: Responses to Subcommittee Questions about the On-Line PEBES Service, AIMD-97-121R (June 20, 1997), at http://161.203.16.4/paprpdf1/158905.pdf.

Supplemental Security Income: Timely Data Could Prevent Millions In Overpayments to Nursing Home Residents, HEHS-97-62 (June 03, 1997), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he97062.pdf.

U.S. Postal Service: Information about Restrictions on Mailbox Access, GGD-97-85 (May 30, 1997), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:gg97085.pdf.

Internet Census and Use Estimates, GGD-97-102R (May 12, 1997), at http://161.203.16.4/paprpdf1/158649.pdf.

Social Security Administration: Internet Access to Personal Earnings and Benefits Information, T-AIMD/HEHS-97-123 (May 6, 1997), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ai97123t.pdf.

Statistical Agencies: Consolidation and Quality Issues, T-GGD-97-78 (Apr. 8, 1997), at http://www.gao.gov/archive/1997/gg97078t.pdf.

Aviation Security: Urgent Issues Need To Be Addressed, T-RCED/NSIAD-96-251 (Sept. 11, 1996), at http://www.gao.gov/archive/1996/rc96251t.pdf.

Privatization Of OPM's Investigations Service, GGD-96-97R (Aug. 22, 1996), at http://161.203.16.4/paprpdf1/157355.pdf.

U.S. Postal Service: Improved Oversight Needed To Protect Privacy of Address Changes, GGD-96-119 (Aug. 13, 1996), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:gg96119.pdf.

Statistical Agencies: A Comparison of the U.S. and Canadian Statistical Systems, GGD-96-142 (Aug. 1, 1996), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:gg96142.pdf.

Consumer Health Informatics: Emerging Issues, AIMD-96-86 (July 26, 1996), at http://www.gao.gov/archive/1996/ai96086.pdf.

Concessions Contracting: Governmentwide Rates of Return, GGD-96-86 (Apr. 29, 1996), at http://www.gao.gov/archive/1996/gg96086.pdf.

Money Laundering: U.S. Efforts to Combat Money Laundering Overseas, T-GGD-96-84 (Feb. 28, 1996), at http://www.gao.gov/archive/1996/gg96084t.pdf.

Medicare: Modern Management Strategies Needed to Curb Program Exploitation, T-HEHS-95-183 (June 15, 1995), at http://161.203.16.4/t2pbat1/154471.pdf.

Department of Energy: Procedures Lacking to Protect Computerized Data, AIMD-95-118 (June 5, 1995), at http://161.203.16.4/t2pbat1/154627.pdf.

Governmentwide Initiatives: Critical Issues Facing the Post-FTS 2000 Program, T-AIMD-95-108 (Mar. 21, 1995), at http://161.203.16.4/t2pbat1/153782.pdf.

Information Integrity: Using Technology to Determine Eligibility to Work and Receive Benefits, T-AIMD-95-99 (Mar. 7, 1995), at http://161.203.16.4/t2pbat1/153670.pdf.

Information Superhighway: An Overview of Technology Challenges, AIMD-95-23 (Jan. 23, 1995), at http://www.gao.gov/archive/1995/ai95023.pdf.

Information Superhighway: Issues Affecting Development, RCED-94-285 (Sept. 30, 1994), at http://161.203.16.4/t2pbat2/152628.pdf.

Bureau of the Census: Legislative Proposal to Share Address List Data Has Benefits and Risks, T-GGD-94-184 (July 21, 1994), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:tgg94184.txt.

Records Management: Inadequate Controls over Various Agencies' Political Appointee Files, NSIAD-94-155 (July 13, 1994), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ns94155.txt.

Records Management: Retrieval of State Department's Political Appointee Files, NSIAD-94-187 (July 13, 1994), at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ns94187.txt.

Smart Highways: Challenges Facing DOT's Intelligent Vehicle Highway Systems Program, T-RCED-94-253 (June 29, 1994), at http://161.203.16.4/t2pbat3/151999.pdf.

Health Care: Benefits and Barriers to Automated Medical Records, T-AIMD-94-117 (May 6, 1994), at http://161.203.16.4/t2pbat3/151828.pdf.
HUD Information Resources: Strategic Focus and Improved Management Controls Needed, AIMD-94-34 (Apr. 14, 1994), at http://161.203.16.4/t2pbat3/151342.pdf.

VA Health Care for Women: In Need of Continued VA Attention, T-HEHS-94-114 (Apr. 9, 1994), at http://161.203.16.4/t2pbat4/150981.pdf.

Federal Lands: Public Land Access, T-RCED-94-72 (Nov. 09, 1993), at http://161.203.16.4/t2pbat5/150287.pdf.

Communications Privacy: Federal Policy and Actions, OSI-94-2 (Nov. 4, 1993), at http://161.203.16.4/t2pbat5/150236.pdf.

Automating Medical Information, AIMD-94-47R (Oct. 22, 1993), at http://161.203.16.4/t2pbat5/150152.pdf.

Computer Matching: Quality of Decisions and Supporting Analyses Little Affected by 1988 Act, PEMD-94-2 (Oct. 18, 1993), at http://161.203.16.4/t2pbat4/150416.pdf.

Drug Use Measurement: Strengths, Limitations, And Recommendations For Improvement, T-PEMD-94-4 (Oct. 5, 1993), at http://161.203.16.4/t2pbat5/150124.pdf.

Medicare Physician Payment: Geographic Adjusters Appropriate but Could Be Improved with New Data, HRD-93-93 (July 20, 1993), at http://161.203.16.4/t2pbat5/149506.pdf.

GSA's Computer Security Guidance, AIMD-93-7R (July 19, 1993), at http://161.203.16.4/d45t15/149787.pdf.

Tax Administration: Information Returns Can Improve Reporting of Forgiven Debts, GGD-93-42 (Feb. 17, 1993), at http://161.203.16.4/d37t11/148753.pdf.

Tax Administration: Status of Tax Systems Modernization, Tax Delinquencies, and the Tax Gap, T-GGD-93-4 (Feb. 3, 1993), at http://161.203.16.4/d42t14/148492.pdf.

Geological Survey: Computer Security, IMTEC-93-10R (Dec. 14, 1992), at http://161.203.16.4/d36t11/148127.pdf.

Tax Systems Modernization: Concerns over Security and Privacy Elements of the Systems Architecture, IMTEC-92-63 (Sept. 21, 1992), at http://161.203.16.4/d35t11/147870.pdf.

Health Insurance: More Resources Needed To Combat Fraud and Abuse, T-HRD-92-49 (July 28, 1992), at http://161.203.16.4/t2pbat6/147229.pdf.

VA Health Care for Women: Despite Progress, Improvements Needed, T-HRD-92-33 (July 2, 1992), at http://161.203.16.4/t2pbat6/147022.pdf.

Census Reform: Major Expansion in Use of Administrative Records for 2000 Is Doubtful, T-GGD-92-54 (June 26, 1992), at http://161.203.16.4/t2pbat6/146958.pdf.

VA Health Care for Women: despite Progress, Improvements Needed, T-HRD-92-42 (June 19, 1992), at http://161.203.16.4/t2pbat6/146956.pdf.

Tax Systems Modernization: Update on Critical Issues Facing IRS, T-IMTEC-92-18 (May 13, 1992), at http://161.203.16.4/d38t12/146691.pdf.

Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse, HRD-92-69 (May 7, 1992), at http://161.203.16.4/t2pbat6/146547.pdf.

Federal Lands: Reasons for and Effects of Inadequate Public Access, RCED-92-116BR (Apr. 14, 1992), at http://161.203.16.4/d32t10/146394.pdf.

Tax Systems Modernization: Progress Mixed in Addressing Critical Success Factors, T-IMTEC-92-13 (Apr. 02, 1992), at http://161.203.16.4/t2pbat6/146314.pdf.

Tax Systems Modernization: Factors Critical to Success, T-IMTEC-92-10 (Mar. 10, 1992), at http://161.203.16.4/t2pbat6/146093.pdf.

VA Health Care for Women: Despite Progress, Improvements Needed, HRD-92-23 (Jan. 23, 1992), at http://161.203.16.4/d31t10/145766.pdf.

Internal Revenue Service: Status of IRS' Efforts to Deal with Integrity and Ethics Issues, GGD-92-16 (Dec. 31, 1991), at http://161.203.16.4/d31t10/145528.pdf.

Tax System Modernization: Issues Facing IRS, T-IMTEC-91-18 (July 9, 1991), at http://161.203.16.4/d48t13/144304.pdf.

Tax System Modernization: An Assessment of IRS' Design Master Plan, IMTEC-91-53BR (June 25, 1991), at http://161.203.16.4/d20t9/144208.pdf.

Tax System Modernization: Attention to Critical Issues Can Bring Success, T-IMTEC-91-8 (June 25, 1991), at http://161.203.16.4/d48t13/144295.pdf.

Peer Review: Compliance with The Privacy Act and Federal Advisory Committee Act, GGD-91-8 (Apr. 17, 1991), at http://161.203.16.4/t2pbat8/143644.pdf.

Computer Matching Act: Many States Did Not Comply with 30-Day Notice or Data-Verification Provisions, HRD-91-39; B242262 (Feb. 8, 1991), at http://161.203.16.4/d21t9/143136.pdf.

Medical ADP Systems: Automated Medical Records Hold Promise to Improve Patient Care, IMTEC-91-5 (Jan. 22, 1991), at http://161.203.16.4/t2pbat8/143217.pdf.

Nuclear Waste: Quality Assurance Auditors Need Access to Employee Records, RCED-91-7 (Jan. 18, 1991), at http://161.203.16.4/t2pbat8/143177.pdf.

Computers And Privacy How the Government Obtains, Verifies, Uses, and Protects Personal Data, IMTEC-90-70BR; B-239819 (Aug. 3, 1990), at http://161.203.16.4/d23t8/142109.pdf.

Energy Management: DOE Controls over Contractors' Use of FTS Are Inadequate, RCED-90-184 (July 17, 1990), at http://161.203.16.4/d23t8/142021.pdf.

Computer Matching: Need for Guidelines on Data Collection and Analysis, HRD-90-30 (Apr. 17, 1990), at http://161.203.16.4/d24t8/141142.pdf.

Telecommunications Privacy GSA's Planned FTS 2000 Telephone Record Controls Appear Reasonable, IMTEC-89-6; B-130441 (Dec. 23, 1988), at http://161.203.16.4/d15t6/137745.pdf.

FBI Voice Privacy Update on Program Direction, IMTEC-88-39; B-226295 (Aug. 30, 1988), at http://161.203.16.4/d17t6/136935.pdf.

Medicare: Issues Concerning The Health Choice Demonstration Project, HRD-88-69 (July 20, 1988), at http://161.203.16.4/d16t6/136617.pdf.

Veterans' Pensions: Verifying Income with Tax Data Can Identify Significant Payment Problems, HRD-88-24 (Mar. 16, 1988), at http://161.203.16.4/d34t11/135485.pdf.

FBI Voice Privacy: Cost, Status, and Future Direction, IMTEC-87-4S (Mar. 8, 1988), at http://161.203.16.4/d34t11/135357.pdf.

Privacy Act Privacy Act System Notices, GGD-88-15BR; B223140 (Nov. 30, 1987), at http://161.203.16.4/d29t5/134673.pdf.

Welfare: Summary of Administrative Problems Discussed in Past GAO Reports, HRD-88-29BR (Nov. 27, 1987), at http://161.203.16.4/d16t6/135929.pdf.

Veterans' Benefits: Improving the Integrity of VA's Unemployability Compensation Program, HRD-87-62 (Sept. 21, 1987).

Counterterrorism: Role of Interpol and the U.S. National Central Bureau, GGD-87-93BR; B-226943 (June 25, 1987), at http://161.203.16.4/d29t5/133875.pdf.

Welfare Eligibility: Deficit Reduction Act Income Verification Issues, HRD-87-79FS; B-226802 (May 26, 1987), at http://161.203.16.4/d28t5/133177.pdf.

FBI Voice Privacy: Cost, Status, and Future Direction, IMTEC-87-4 (Feb. 27, 1987), at http://161.203.16.4/t2pbat22/132564.pdf.

Privacy Act: Federal Agencies' Implementation Can Be Improved, GGD-86-107; B-223140 (Aug. 22, 1986), at http://161.203.16.4/d4t4/130974.pdf.

Social Security: Quality of Services Generally Rated High by Clients Sampled, HRD-86-8 (Jan. 30, 1986), at http://161.203.16.4/d12t3/128999.pdf.

Department Of Defense: DOD's Training Program for Polygraph Examiners, NSIAD-86-33BR (Dec. 31, 1985), at http://161.203.16.4/d12t3/128749.pdf.

Current Issues in U.S. Participation in the Multilateral Trading System, NSIAD-85-118 (Sept. 23, 1985), at http://161.203.16.4/d11t3/127972.pdf.

A Central Wage File for Use by Federal Agencies: Benefits and Concerns, HRD-85-31 (May 21, 1985), at http://161.203.16.4/d9t2/127201.pdf.

Eligibility Verification and Privacy in Federal Benefit Programs: A Delicate Balance, HRD-85-22 (Mar. 1, 1985), at http://161.203.16.4/d10t2/126333.pdf.

GAO Observations on the Use of Tax Return Information for Verification in Entitlement Programs, HRD-84-72 (June 5, 1984), at http://161.203.16.4/d6t1/124423.pdf.

State Field Offices Are Not Protecting Social Security Beneficiary Information from Potential Abuse and/or Misuse Report, HRD-81-151 (Dec. 30, 1981).

Solving Social Security Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed, HRD-82-19 (Dec. 10, 1981), at http://161.203.16.4/d41t14/117253.pdf.

Increasing Use Of Data Telecommunications Calls for Stronger Protection and Improved Economies, LCD-81-1 (Nov. 12, 1980).

Disclosure and Summons Provisions of 1976 Tax Reform Act - An Analysis of Proposed Legislative Changes, GGD-80-76 (June 17, 1980), at http://161.203.16.4/d46t13/112579.pdf.

Federal Agencies' Initial Problems with the Right to Financial Privacy Act of 1978, GGD-80-64 (May 29, 1980).

Inadequate Contract Administration on Housing Renovation Project at Malmstrom Air Force Base, PSAD-80-32 (Mar. 11, 1980).

Unresolved Issues Impede Federal Debt Collection Efforts - A Status Report, CD-80-1 (Jan. 15, 1980)

A Technical Guide to Assessing and Preparing Economic Impact Analysis of Regulatory Legislation, PAD-81-03 (Jan. 1, 1980).

After Six Years, Legal Obstacles Continue to Restrict Government Use of the Standard Statistical Establishment List, GGD-79-17; B-78395 (May 25, 1979).

Disclosure and Summons Provisions of 1976 Tax Reform Act - Privacy Gains with Unknown Law Enforcement Effects, GGD-78-110; B137762 (Mar. 12, 1979).

A Framework for Balancing Privacy and Accountability Needs in Evaluations of Social Research, PAD-79-33 (Mar. 1, 1979).

Automated Systems Security, Federal Agencies Should Strengthen Safeguards over Personal and Other Sensitive Data, LCD-78-123; B-130441, B-115369, B-173761 (Jan. 23, 1979).

What Are the Capabilities of the Selective Service System? FPCD-79-4 (Dec. 14, 1978).

Privacy Act of 1974 Has Little Impact on Federal Contractors, LCD-78-124 (Nov. 27, 1978).

Impact of the Freedom of Information and Privacy Acts on Law Enforcement Agencies, GGD-78-108 (Nov. 15, 1978).

Fundamental Changes Needed to Improve the Independence and Efficiency of the Military Justice System, FPCD-78-16 (Oct. 31, 1978).

The Impact of the Privacy Act of 1974 on Federal Contractors, 107246 (Sept. 18, 1978).

VA's New Computer System Has Potential to Protect Privacy of Individuals Claiming Benefits, HRD-78-135 (July 17, 1978).

Data on Privacy Act and Freedom of Information Act Provided by Federal Law Enforcement Agencies, LCD-78-119 (June 16, 1978).

Agencies' Implementation of and Compliance with the Privacy Act Can Be Improved, LCD-78-115; B-130441 (June 6, 1978).

Status of Office of Education's National Direct Student Loan Funds at Selected Postsecondary Education Institutions, HRD-78-94 May 2, 1978).

Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment, LCD-76-102 (Apr. 28, 1978).

Federal Bureau of Investigation's Handling and Responsiveness to Freedom of Information Act and Privacy Act Requests, 105692 (Apr. 10, 1978).

Office of Telecommunications Policy's Contract for a Publication on Intercepting Electronic Communications, LCD-78-110 (Apr. 10, 1978).

Timeliness and Completeness of FBI Responses to Requests under Freedom of Information and Privacy Acts Have Improved, GGD-78-51 (Apr. 10, 1978).

Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment, LCD-76-102; B-146864 (Apr. 2, 1978).

Privacy Implications of IRS' Proposed Tax Administration System, GGD-78-46 (Mar. 22, 1978).

An Analysis of IRS' Proposed Tax Administration System: Lessons for the Future, GGD-78-43 (Mar. 1, 1978).

FBI Taking Actions to Comply Fully with the Privacy Act, GGD-77-93 (Dec. 26, 1977).

Cooperative Actions Result in More Economical Computer Acquisition and Improved Security at the New Orleans Computer Center, LCD-77-118 (Dec. 23, 1977).

Privacy Issues And Supplemental Security Income Benefits, HRD-77-110 (Nov. 15, 1977).

Lawsuits Against The Government Relating To A Bill To Amend The Privacy Act Of 1974 Department Of Justice, GGD-77-21; B-130441 (May 6, 1977).

Safeguarding Taxpayer Information: An Evaluation Of The Proposed Computerized Tax Administration System, LCD-76-115; B-115369 (Jan. 17, 1977).

National Security Agency's Compliance with the Privacy Act of 1974, LCD-77-103 (Nov. 11, 1976).