A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board

by
ROBERT GELLMAN*

Introduction

The purpose of this paper is to argue that the United States needs a federal privacy agency. The main objective of a privacy agency would be to promote the adoption and implementation throughout the United States of protections for personal privacy and of principles of Fair Information Practices. Other functions would include issuing advisory opinions, conducting investigations, proposing rules and legislation, commenting on governmental and private sector actions affecting privacy, assisting with private sector self-regulatory efforts, and maintaining international continuity. The agency would not have any regulatory powers. The Appendix includes a specific legislative proposal that more fully describes the organization, functions, and membership of the Privacy Protection Board.

The importance of privacy as a public policy concern will be accepted here as a given. Other sources can provide the usual measures of importance, which include:

- the number of state and federal privacy laws enacted in the last few years;
- the number of privacy bills introduced in state legislatures and in Congress;

* Privacy and Information Policy Consultant, Washington, D.C.; former Chief Counsel and Staff Director of the Subcommittee on Information, Justice, Transportation, and Agriculture of the House Committee on Government Operations; B.A., 1970, University of Pennsylvania; J.D., 1973, Yale Law School. I thank Harold Relyea, Paul Schwartz, and Beryl Radin for comments on earlier drafts. Prepared for the Enforcing Privacy Rights Symposium, November 15 & 16, 2002.

- the degree of public concern as expressed in public opinion polls;
- the growth of sincere and other privacy self-regulatory activities;
- the development of public and private institutions dealing with aspects of privacy;
- the number of lawsuits and federal and state investigations into violations of privacy;
- the volume of media coverage of privacy;
- the consequences to individuals from the use and misuse of personal information;
- the ever-increasing amount of personal information maintained by third party record keepers; and
- the vast capabilities of modern information technology, including the Internet, to collect, compile, maintain, and disseminate personal information.[1]

For present purposes, it is sufficient to assert that nearly every institution in the modern world maintains personal data and that nearly every individual is the subject of data files maintained by those institutions. Nowhere is this more true than in the United States, where the collection, maintenance, use, and disclosure of personal information is ubiquitous among private and governmental organizations.

Where personal records exist, privacy issues necessarily follow, even if the issues are ignored at times. Record keepers and record subjects have—or should have—a shared interest in determining the rules governing the collection, maintenance, use, and disclosure of personal data. Both record keepers and record subjects share risks and responsibilities regarding the processing of personal data. A privacy agency would serve the interests of both record keepers and record subjects.

1. The number of popular and scholarly writings that make these points is enormous. Some examples include: DAVID BURNHAM, THE RISE OF THE COMPUTER STATE (1983); ERIK LARSON, THE NAKED CONSUMER (1992); JEFFREY ROTHFEDER, PRIVACY FOR SALE (1992); ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE (2000); SIMSON GARFINKEL, DATABASE NATION (2000); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002). For some interesting metrics on the amount of data collection and the availability of data storage, see Latanya Sweeney, *Information Explosion*, *in* CONFIDENTIALITY, DISCLOSURE, AND DATA ACCESS: THEORY AND PRACTICAL APPLICATIONS FOR STATISTICAL AGENCIES (P. Doyle ed., 2001).

I. Some Reasons for a Privacy Agency

A. All the Other Kids Have One

The history of privacy during the past three decades is, among other things, a history of the international acceptance of Fair Information Practices as core information privacy principles and of the spread of formal institutions to address privacy protection. Many governments around the world enacted data protection[2] laws and established privacy agencies in response to similar concerns about the effects of technology, commercialism, and government on personal privacy.[3] The popularity of data protection institutions is based not on mere fashion but on international recognition of a need to address privacy issues through a formal and dedicated organization, and on a demonstrated record of accomplishment and utility.

Modern data protection laws and data protection agencies began in the State of Hesse in Germany in 1970.[4] Today, each European Union member state has a data protection authority. So do more than a dozen other countries, including Canada, Australia, Hong Kong, Argentina, Thailand, and Monaco. The territories of Guernsey, Isle of Man, and Jersey have data protection authorities, and Canada, Australia, and Germany have provincial privacy authorities.[5] In some cases, these agencies share responsibility for privacy and for open records laws.[6] For the most part, however, responsibilities of the agencies are limited to privacy.

---

2. *Data protection* is used here interchangeably with *privacy* to refer broadly to activities that involve the collection, maintenance, use, and disclosure of personal information. Because it is not the purpose of this Article to explore the boundaries of privacy, this definition is offered as definitive or limiting. Aspects of privacy other than personal information fall within the zone of interest for a privacy agency. Debates over privacy definitions and purposes are well established in privacy literature. *See, e.g.*, Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002); PRISCILLA M. REGAN, LEGISLATING PRIVACY ch. 2 (1995).

3. *See generally* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992).

4. DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 22 (1989).

5. This is not a complete list. The EU Data Protection web page maintains a list of data protection commissioners around the world at http://europa.eu.int/comm/internal_market/en/dataprot/links.htm (last visited Jan. 31, 2003).

6. Leading examples in Canada are the Information and Privacy Commissioner of Ontario, *at* http://www.ipc.on.ca (last visited Feb. 26, 2003), and the British Columbia Office of the Information and Privacy Commissioner, *at* http://www.oipcbc.org (last visited Feb. 26, 2003). The British Data Protection Registrar was recently transformed into the Information Commissioner, *at* http://www.dataprotection.gov.uk (last visited Feb. 26, 2003), when freedom of information functions were added. Data protection offices in some German states also have jurisdiction over access to records.

The European Union ("EU") is the world leader on data protection and on national data protection agencies, which the EU Data Protection Directive calls *supervisory authorities*.[7] The Directive treats supervisory authorities as an essential feature of data protection activities, requiring each EU member state to have a supervisory authority. Most other countries with data protection laws have elected to follow the EU's lead and establish a national privacy office.

The international growth of data protection agencies suggests a broad recognition that the agencies are useful and, perhaps, essential to the conduct of good data protection. A visit to the web pages of many data protection authorities reveals a wealth of useful research, policy analyses, advice, annual reports, and other materials. Some agencies also produce formal opinions, decisions, and interpretations.

It is tempting to jump to the conclusion that the data protection authorities must be useful or they would not have become so established or spread so widely across the globe. That conclusion is almost certainly correct, but it is admittedly hard to apply any metrics in support. Evaluating a national privacy agency is not a simple task, and evaluating many of them is even more challenging. Even the development of criteria for measuring the effectiveness and value of an agency would be controversial. Applying criteria across different governments, cultures, and legal structures makes the task that much more complex.

Academic evaluations of national data protection agencies are scarce. The only multi-national study dates back to 1989. Professor David Flaherty—who later became the Information and Privacy Commissioner for British Columbia—analyzed privacy in five countries, including the United States. Flaherty's conclusion about the importance of data protection agencies to the conduct of data protection is notable:

> Perhaps the most important conclusion of this volume is that it is not enough simply to pass a data protection law in order to control surveillance; an agency charged with implementation is essential to make the law work in practice. A statute by itself is an insufficient countervailing force to the ideological and political pressures for efficiency and monitoring of the population that are at work in Western society.[8]

Flaherty was also realistic about the power that could be exercised by data protection offices. He observed that, "[t]he harsh

7. Council Directive 95/46, art. 28, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281/47), *available at* http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm (last visited Jan. 31, 2003) [hereinafter EU Data Protection Directive].

8. FLAHERTY, *supra* note 4, at 381.

reality is that data protectors run the risk of being only a tiny force of irregulars equipped with pitchforks and hoes waging battle against large technocratic and bureaucratic forces equipped with lasers and nuclear weapons."[9]

Flaherty's assessment suggests that expectations for the accomplishments of data protection authorities should be restrained. Data protection agencies are not exempt from the usual factors that affect the operations of all government agencies. Budgets, statutory limitations, bureaucracy, questionable appointments, timidity, and pragmatism take their toll everywhere. Privacy agencies are not a panacea for privacy problems, but they remain useful contributors for addressing those problems.[10]

Despite the absence of any formal evaluation of data protection agencies, most of the industrialized world has reached the conclusion that a data protection agency can make a useful contribution to the continuing struggle over privacy protections. The number of data protection agencies has steadily increased over the past several decades. No country that established a data protection agency later abolished it.

Not only is a data protection agency almost certainly a good idea on its own, but it may be close to a necessity today. With data protection agencies in so many other countries, the resolution of some international privacy matters comes principally through the cooperation of the national privacy agencies.[11] In essence, with the international critical mass of data protection agencies that now exists, a country without an agency is at a disadvantage.

---

9. *Id.* at 393.

10. Privacy agencies have their critics. Simon Davies, an internationally recognized privacy advocate, objects that privacy officials too often dodge controversy in the name of pragmatism. Simon Davies, *Unprincipled Privacy: Why the Foundations of Data Protection Are Failing Us*, 24 U. NEW S. WALES L.J. 284, 287 (2001), *available at* http://www.austlii.edu.au/au/journals/UNSWLJ/2001/7.html.

> In the face of such criticism, privacy officials (and their biographers) tend to promote success stories, adopting a celebratory tone. While this is understandable, all professions are constantly at risk of sacrificing their responsibilities on the altar of pragmatism, and the area of privacy protection is no exception. Privacy officials all too often abuse the trust placed in them by dodging controversy in an effort to preserve their fiefdoms. As a consequence, governments frequently succeed in using data protection law as a thinly veiled mandate for surveillance.

Id. (footnote omitted).

11. The EU Directive established an advisory Working Party composed of representatives of the national supervisory authorities. EU Data Protection Directive, *supra* note 7, at art. 29. The numerous contributions of the so-called Article 29 Committee can be found at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm (last visited Feb. 26, 2003).

Privacy is one of many policy areas with international dimensions. Over the years, the United States has been represented at international data protection conferences by personnel from the Commerce Department, State Department, Federal Trade Commission, Office of Management and Budget, and others. Continuity of representation by individuals or by agencies has been rare, and the adequacy of U.S. representation has been mediocre, at best.[12]

To some extent, the United States needs a data protection agency because many other countries have agencies and because those countries rely upon their agencies to help resolve international privacy conflicts. Worldwide attention has made privacy a significant concern for businesses operating internationally. The main beneficiary of improved international representation on privacy matters will be the record keepers—the business community—more than American citizens and residents. Better resolution of privacy disputes will benefit global trade and electronic commerce.

The interest in a structural response to privacy is not just international. Flaherty's observation about the continuing need for an agency to address privacy has been borne out by the expansion of institutional responses to privacy matters. National governments have not been the only organizations recognizing the need for privacy institutions.

Federal agencies are increasingly establishing internal organizations to address privacy concerns. The Defense Privacy Board dates back to 1975, when the Privacy Act of 1974 became effective, and it has continued in operation ever since with a principal focus on implementation of the Privacy Act.[13] More recently, the Department of Health and Human Services established a Privacy Advocate in 1996 with a broader portfolio but fewer resources. A few other federal agencies have also established positions or committees to address privacy.

Perhaps the most interesting federal privacy office is the Office of the Privacy Advocate established by the Internal Revenue Service in 1993.[14] The role of the IRS office is to ensure that the agency

12. For some of the history of the work of other federal agencies on privacy issues, see Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199 (1993) [hereinafter *Privacy Regulatory Proposals*] and Priscilla M. Regan, Perspectives on Privacy: Changing Institutional Roles and Responsibilities (1998) (unpublished paper presented at the Information Privacy Seminar Series, Georgetown Business School).

13. *See* U.S. Dep't of Def., Def. Privacy Off. *at* http://www.defenselink.mil/privacy (last visited Jan. 31, 2003).

14. *See generally* Margaret Ann Irving, *Managing Information Privacy in the Information Age*, 53 ADMIN. L. REV. 659 (2001).

integrates privacy strategies into the agency's business processes. The mandate of the office suggests recognition by IRS management that traditional government responses to privacy are insufficient to address the broader privacy concerns that IRS activities raise and that often are ignored during traditional planning activities to new technology and new ways of doing business.[15] IRS established the office without a legislative requirement.

The first legislative mandate for a privacy officer came in the Homeland Security Act of 2002. The law requires the Secretary of Homeland Security to appoint a senior official in the department to assume primary responsibility for privacy policy.[16] Whether this legislation will start a trend remains to be seen, but it is possible that internal privacy officers may be created in other Cabinet level departments.

California recently established a privacy office.[17] The Office of Privacy Protection is part of the Department of Consumer Affairs. Its mission is to serve as a statewide resource for consumer information and as a source of assistance on identity theft and other privacy issues; to assist law enforcement by providing privacy training and by helping with investigations; to work with businesses to define and encourage sound privacy protection practices; and to report on trends in consumer privacy problems and issues.[18] The California office is too new for an evaluation.[19]

Even corporate America has taken up structural responses to privacy. Some companies have established the position of Chief Privacy Officer ("CPO") to manage privacy issues. It is difficult to estimate the number of CPOs or evaluate their importance to the institutions that created them. However, the voluntary establishment of formal privacy positions in companies suggests some recognition of the continuing

15. The Privacy Act of 1974, the principal law regulating federal government records for privacy, has been recognized as out of date for more than two decades. *See, e.g., Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress: Hearing Before the House Comm. on Gov't Operations*, 98th Cong. (1983); H.R. REP. NO. 98-455 (1983).

16. Homeland Security Act of 2002, Pub. L. No. 107-296, § 222, 116 Stat. 2135, 2155 (2002).

17. CAL. BUS. & PROF. CODE §§ 350–52 (West Supp. 2002), *available at* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=00001-01000&file=350-352. *See also Personal Information and Privacy Protection: Hearing on S.B. 129 before the California Legislature Conference Committee*, 1999–2000 Reg. Sess. (Cal. 2000) (testimony of Robert Gellman recommending creation of a non-regulatory privacy agency).

18. Office of Privacy Protection, *at* http://www.privacy.ca.gov/about.htm (last visited Feb. 26, 2003).

19. Hawaii has had an Office of Information Practices with responsibilities for state open records laws since 1988, *at* http://www.state.hi.us/oip (last visited Feb. 26, 2003). *See* Uniform Information Practices Act, HAW. REV. STAT. § 92 F-11-42 (2001).

importance of privacy management. Whether CPOs will become permanent fixtures remains to be seen.[20]

More CPOs are certain to be established in 2003 in the health care field. The federal privacy rule issued under the Health Insurance Portability and Accountability Act requires every covered entity[21] to designate a privacy official.[22] Small health care offices are likely to have part-time privacy officials, but larger institutions may have full-time offices.

None of the agency or company privacy offices provides an exact parallel to the proposed Privacy Protection Board. However, the establishment of privacy offices is recognition of the growing importance of privacy and the need to manage personal data and organizational responsibility.

B. The United States Estahlishes Agencies All the Time

The United States Government has agencies dedicated to issues and activities of concern to the American public. The larger agencies are familiar, but there are also small agencies that are responsible for postal rates,[23] civil rights,[24] international trade,[25] American battle monuments,[26] marine mammals,[27] migratory birds,[28] and arctic research.[29] Dozens of other small federal agencies, boards, commissions, and committees address other specific issues that were deemed of sufficient importance to warrant the establishment of a permanent federal agency.

Most recently, in the Help America Vote Act of 2002,[30] Congress established the Election Assistance Commission to serve as a national

20. Since 1977, the German national data protection law required private bodies that process personal data and employ at least five (the 2001 amendment changed the number to twenty) permanent employees to have a formal data protection officer. *See* Act to Amend the Federal Data Protection Act and Other Enactments §§ 4f–4g (2001) (F.R.G.), *available at* http://europa.eu.int/comm/internal_market/en/dataprot/law/de18-05-01.pdf.

21. Health care providers, health plans, and clearinghouses are covered entities under the rule. 45 C.F.R. § 160.103 (2002).

22. 45 C.F.R. § 164.530 (2002).

23. Postal Rate Commission, *at* http://prc.gov (last visited Feb. 26, 2003).

24. Commission on Civil Rights, *at* http://www.usccr.gov (last visited Feb. 26, 2003).

25. International Trade Commission, *at* http://www.usitc.gov (last visited Feb. 26, 2003).

26. American Battle Monuments Commission, *at* http://www.abmc.gov (last visited Feb. 26, 2003).

27. Marine Mammal Commission, *at* http://www.mmc.gov (last visited Feb. 26, 2003).

28. Migratory Bird Conservation Commission, *at* http://realty.fws.gov/mbcc.html (last visited Feb. 26, 2003).

29. Arctic Research Commission, *at* http://www.uaa.alaska.edu/enri/arc_web/archome.htm (last visited Feb. 26, 2003).

30. Pub. L. No. 107-252, §§ 201–02, 116 Stat. 1666, 1673 (2002) (codified as amended at 42 U.S.C. §§ 15301–545 (2002)).

clearinghouse and resource for the compilation of information and review of procedures for federal elections. The Commission also has a series of substantive functions.

The point is that when independent agencies help to solve substantive or political problems, Congress does not hesitate to create them. Privacy is a matter of public concern at least to the same degree as many other issues for which federal agencies have been created in the past.

To illustrate the penchant of the federal government to establish institutions, we can look at the relatively new area of critical infrastructure protection. Critical infrastructure protection is a policy and operational response to the explosion in computer interconnectivity that has revolutionized the way that the government, the nation, and much of the world communicate and conduct business.[31] The interconnectivity also poses enormous risks to computer systems and to the critical operations and infrastructures that they support, including telecommunications, power distribution, national defense, law enforcement, and government services.[32]

National attention to the subject of critical infrastructure was spurred by the 1997 report of a presidential commission.[33] In response, President Clinton issued a presidential decision directive calling for actions to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to attacks.[34]

A few years later, the General Accounting Office undertook a review of the government's response. It found that at least fifty federal organizations participate in national or multi-agency critical

31. It is interesting that with all of the attention and money focused on critical infrastructures over the past few years, there is no commonly agreed upon definition of *critical infrastructure*. *See* CONGRESSIONAL RESEARCH SERVICE, CRITICAL INFRASTRUCTURES: WHAT MAKES AN INFRASTRUCTURE CRITICAL? 2 (Aug. 30, 2002) *at* http://www.fas.org/irp/crs/RL31556.pdf (last visited Jan. 31, 2003):

> Over the last few years, a number of documents concerned with critical infrastructure protection have offered general definitions for critical infrastructures and have provided short lists of which infrastructures should be included. None of these lists or definitions would be considered definitive. The criteria for determining what might be a critical infrastructure, and which infrastructures thus qualify, have expanded over time.

Id.

32. *See* U.S. GENERAL ACCOUNTING OFFICE, CRITICAL INFRASTRUCTURE PROTECTION, (GAO-02-474, 2002), *available at* http://www.gao.gov/new.items/d02474.pdf [hereinafter GAO CIP].

33. PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES (1997).

34. Presidential Decision Directive No. NSC-63 (May 22, 1998) *at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (last visited Jan. 31, 2003).

infrastructure protection activities. The fifty organizations include five advisory committees, six organizations in the Executive Office of the President, thirty-eight executive branch organizations, and others.[35] Requested funding for critical infrastructure activities is nearly $4 billion for 2003.[36] So many organizations exist that they are tripping over each other. GAO phrased it more diplomatically: "[R]elationships among all organizations performing similar activities (e.g., policy development or analysis and warning) were not consistently established."[37]

Structural responses to public policy concerns happen routinely. It is not unusual or unprecedented to establish a new agency or independent commission with a focus on a particular set of issues. Privacy is a subject with at least as much broad public interest and concern as other issues that have separate agencies.

C. A U.S. Privacy Agency Has Been Repeatedly Proposed

The argument to this point is that national privacy agencies are increasingly commonplace and useful around the world, that privacy institutions of all stripes have been established in many different types of organizations, and that the establishment of U.S. agencies in response to matters of public concern is routine. It does not necessarily follow from the establishment of so many different privacy institutions that a national agency for privacy is needed.

This section reviews some past proposals for a privacy agency. It is not an entirely new idea. While a privacy agency has never been established, the idea never goes away. Many past reviews of privacy and related issues have concluded that a privacy agency is a good idea.

(1) Proposed Fair Information Practices

The most influential temporary privacy study commission ever convened in the United States was an advisory committee established in 1972 by Eliot Richardson, Secretary of Health, Education and Welfare. The Committee's 1973 report proposed Fair Information Practices as organizing principles for privacy.[38]

35. GAO CIP, *supra* note 32, at 14.

36. *Id.* at 27.

37. *Id.* at 28.

38. SECRETARY'S ADVISORY COMM'N ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973), *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm [hereinafter HEW Report]. *See also infra* the discussion in Part III of Fair Information Practices.

The Committee considered whether to recommend an independent federal agency to regulate the use of automated personal data systems. It is noteworthy that the Committee concluded an agency was the "strongest" mechanism for providing privacy safeguards. The agency might have authority to register or license the operations of automated personal data systems. The Committee rejected the agency idea because it lacked the necessary public support and because regulation or licensing would be complicated and costly.[39] The Committee's preferred choice was enforcement of privacy rights through individual court action.[40] Thirty years later, the notion of licensing and registration of databases has largely passed out of favor in other countries.[41] It remains an open question whether enforcement through private action is a viable strategy.

(2) Privacy Act of 1974

When Congress enacted the Privacy Act of 1974, the establishment of a privacy agency was actively considered.[42] The bill that passed the Senate included a proposal for a Privacy Protection Commission with a primary mission to oversee federal record keeping activities. The Commission would have been empowered to study privacy matters affecting state and local governments and the private sector. In addition, the Commission would have been able to assist agencies and industries in the voluntary development of fair information practices. A proposal to establish a federal privacy commission as an independent agency was offered in the House, but the amendment was defeated without a recorded vote. The compromise between the House and Senate positions resulted in the creation of a temporary study commission.[43]

(3) Privacy Protection Study Commission

The Privacy Protection Study Commission ("PPSC"), established as a temporary organization in the Privacy Act of 1974, issued its report in 1977.[44] Although better funded and staffed than the 1973 HEW Advisory Committee, the PPSC has had little long-term

39. *Id.* at 42–43. At the time of the Advisory Committee's report, no other country had yet established a formal data protection authority.

40. *Id.* at 44.

41. *See, e.g.*, Gellman, *supra* note 12, at n.71.

42. The history of consideration of a privacy agency during debates on the Privacy Act of 1974 is set out in Gellman, *supra* note 12, at 203, and much of the discussion about proposals for privacy agencies is excerpted from that article.

43. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, 1907 (1974) (codified as amended in scattered sections of 5 U.S.C.).

44. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977).

significance. Although its recommendations received some attention from Congress in the late 1970s, the PPSC's work is mostly forgotten today.

The first of the PPSC's 177 recommendations was that the President and Congress establish a federal entity such as a Federal Privacy Board or other independent unit. The Board would have been charged with four general functions:

> 1) to monitor and evaluate the implementation of any statutes and regulations enacted pursuant to the Commission's recommendations and to have the authority to formally participate in federal administrative proceedings that are relevant to the protection of personal privacy;
>
> 2) to research, study, and investigate areas of privacy concern;
>
> 3) to issue binding interpretative rules for use by federal agencies in implementing the Privacy Act of 1974; and
>
> 4) to advise the President, Congress, government agencies, and states regarding the privacy implications of proposed federal or state statutes or regulations.[45]

(4) Commission on Federal Paperwork

The Commission on Federal Paperwork was established by Congress in 1975 to make recommendations to eliminate needless paperwork while assuring that the Federal Government has the information necessary to meet the mandate of law and operate effectively.[46] The Commission issued thirty-six reports and 770 recommendations on major program areas and government processes.[47] One report specifically addressed privacy and confidentiality issues.[48]

Among other privacy recommendations, the Commission proposed creation of a new federal agency to centralize and coordinate existing information management functions within the executive branch with particular focus on developing and recommending policies and standards on information disclosure, confidentiality, and safeguarding the security of information collected or maintained by federal agencies.[49] The recommendation was based in part on the Commission's conclusions about widespread

45. *Id.* at 37.

46. Act of Dec. 27, 1974, Pub. L. No. 93-556, 88 Stat. 1789 (1974) (establishing a commission on federal paperwork).

47. *Id. See also Privacy and Confidentiality Report and Final Recommendations of the Commission on Federal Paperwork: Hearing before a Subcommittee of the House Committee on Government Operations*, 95th Cong. 53 (1977).

48. COMM'N ON FEDERAL PAPERWORK, CONFIDENTIALITY AND PRIVACY (1977).

49. *Id.* at 150.

noncompliance with the Privacy Act of 1974. The Commission also found that judicial review has not been a meaningful remedy.[50]

(5) Other Legislative Proposals

Legislative proposals for a privacy agency have been introduced from time to time. In the 95th Congress, Representative Ed Koch—a member of the Privacy Protection Study Commission—introduced a bill to establish a Federal Information and Privacy Board and to implement the other recommendations of the Commission.[51] Representative Silvio Conte introduced the Comprehensive Right to Privacy Act, which included the establishment of a Federal Privacy Board.[52]

In the 98th Congress, Representative Glenn English, chairman of the Subcommittee on Government Information, Justice, and Agriculture, introduced legislation to establish a Privacy Protection Commission.[53] In the 99th and 100th Congress, Representative English reintroduced similar bills to establish a Data Protection Board.[54] Representative Bob Wise introduced a somewhat modified proposal for a Data Protection Board in the 101st[55] and 102nd Congress.[56]

The only active legislative attempt to create a permanent privacy agency in recent years came in 1994 when Senator Paul Simon offered an amendment establishing a Privacy Protection Commission[57] to a bill amending the Fair Credit Reporting Act.[58] There was only a brief debate on the Senate floor. The floor manager of the bill opposed the amendment largely on jurisdictional grounds.[59] The amendment was tabled by a vote of 77 to 21.[60]

50. *Id.* at 147.

51. H.R. 9986, 95th Cong. (1977). This bill was reintroduced in the following Congress by Representative Barry Goldwater, Jr., the second congressional appointee to the Privacy Protection Study Commission. H.R. 350, 96th Cong. (1979).

52. H.R. 285, 95th Cong. (1977).

53. Privacy Protection Act of 1984, H.R. 3743, 98th Cong. (1983).

54. Data Protection Act of 1985, H.R. 1721, 99th Cong. (1985); Data Protection Act of 1987, H.R. 638, 100th Cong. (1987).

55. Data Protection Act of 1989, H.R. 3669, 101st Cong. (1989). A hearing that considered, among other issues, H.R. 3669, was held in 1990.

56. Data Protection Act of 1991, H.R. 685, 102d Cong. (1991). The bill was discussed at data protection oversight hearings in 1991. *See Domestic and International Data Protection Issues: Hearings Before the Government Information, Justice, and Agriculture Subcomm. of the House Comm. on Gov't Operations,* 102d Cong. (1991).

57. 140 CONG. REC. S5129-31 (1994).

58. *See* Consumer Reporting Reform Act of 1994 need cite; 140 CONG. REC. S5129 (1994).

59. *Id.* at S5132 (statement of Sen. Bryan).

60. *Id.* at S5133.

In 2000, Congress considered a proposal to establish a temporary Commission for the Comprehensive Study of Privacy Protection. The bill reached the House floor, where it attracted a majority. However, the bill failed to pass because the procedure used to bring the bill to a vote required a two-thirds majority.[61] By 2000, privacy had become so politicized that some members of Congress viewed the notion of a study commission as an excuse not to consider substantive privacy legislation.[62]

A temporary study commission and a permanent privacy agency are significantly different institutions. A temporary commission cannot perform most of the functions proposed for a privacy agency. For example, the 1977 report of the temporary Privacy Protection Study Commission was long-since forgotten by the time that privacy became a major public policy issue in the 1990s. That report failed to anticipate many technological and marketplace developments.

(6) Information Infrastructure Task Force & Information Policy Committee

During the Clinton Administration's second term, an Information Infrastructure Task Force operated as a cabinet level group chaired by the Secretary of Commerce. An Information Policy Committee chaired by the Administrator of the Office of Information and Regulatory Affairs in the Office of Management and Budget examined several policy options, including the creation of a privacy entity.[63] The discussion paper considered the advantages and disadvantages of an independent regulatory agency. In the end, the Committee did not endorse any of the options. The issue became moot when a privacy counselor was established in the Office of Management and Budget in March 1999. However, the OMB privacy counselor position was abolished when the Bush Administration took office in January 2001.[64]

(7) Conclusion

A privacy agency is an idea that never developed enough support for serious consideration. During the 1980s and most of the 1990s, the business community was largely opposed to federal privacy

61. Privacy Comm'n Act, H.R. 4049, 106th Cong. (2000). The House voted on the bill on October 2, 2000. 146 CONG. REC. H8588-89 (2000).

62. *See, e.g.*, 146 CONG. REC. H8564 (2000) (remarks of Rep. Henry Waxman).

63. INFORMATION POLICY COMMITTEE, NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE (1997), *available at* http://www.iitf.nist.gov/ipc/privacy.html.

64. *See* Patrick Thibodeau, *Bush Makes Key Privacy Decision*, COMPUTERWORLD, Apr. 16, 2001, at 1, *available at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,59647,00.html.

legislation of any type. When privacy received more congressional attention in the last half of the 1990s, actions focused on more substantive privacy legislation. While the political prospects for privacy agency legislation remain, at best, mixed, the increased private and governmental interest in organizational responses to privacy make a privacy agency ripe for reconsideration. The past opposition of the business community to privacy legislation is no longer monolithic, and privacy matters have increased in importance in the political and commercial marketplaces. A privacy agency, especially a non-regulatory agency, is likely to be viewed today in a more positive light, even by some past opponents.

III. Model for a Privacy Agency

Perhaps the best model for a privacy agency is the Civil Rights Commission that Congress established in the Civil Rights Act of 1957.[65] Some parallels between privacy and civil rights can be identified, but it is not the similarities that make the Civil Rights Commission a model for a privacy agency. The features of the Civil Rights Commission that are most relevant are its independence, fact-finding functions, limited powers, and the highly controversial subject of its mandate.

The President appoints the members of the Commission, who must be confirmed by the Senate. The Commission's functions are to investigate complaints of civil rights violations, study, collect information, make appraisals of the law and policies of the federal government, serve as a national clearinghouse, and prepare public service announcements.[66] The Commission may also hold hearings and issue subpoenas.[67] The Commission also reports annually to the President and to Congress.[68] The Commission has no authority to regulate anyone or to enforce any law.

An independent evaluation of the Civil Rights Commission's early years (1957–1963) contrasted the agency's limited powers with the importance of its issues:

> In comparison with these relatively weak and legalistic provisions, the importance of the Commission lay in its future potentialities. Empowered to assemble authentic and documented information, to be incorporated in the public record, this new Federal agency would be able to build up an unassailable factual record of the

65. 42 U.S.C. § 1975 (1994).

66. *Id.* § 1975c. Some of the Commission's functions date back to its original legislation, Civil Rights Act of 1957, Pub. L. No. 85-315, 71 Stat. 635 (1957). Other functions were added by the Civil Rights Act of 1964, Public Law 88-352, 78 Stat. 251 (1964).

67. 42 U.S.C. § 1975d(f).

68. *Id.* § 1975c(c).

> status of civil rights throughout the country. From this base, it could then point the way toward more effective policies, on the part of both the Executive and Congress, than anything contemplated in the existing halfway [civil rights legislation].[69]

A statement in support of the Commission from Attorney General Herbert Brownell pointed out the need for a guide to a fundamental issue of the day. "Investigations and hearings will bring into sharper focus the area of responsibility of the Federal Government and of the States under our constitutional system. Through greater public understanding, therefore, the Commission may chart a court of progress to guide us in these years ahead."[70]

A full evaluation of the Civil Rights Commission is far beyond this paper. A study of the Commission's early years concluded by noting the Commission's effectiveness in influencing congressional and executive actions:

> For some eight years, [the Commission] had conducted far-flung investigations into every phase of legal discrimination and issued a series of reports with specific recommendations for both congressional and executive action to remedy the infringements of equal rights so carefully documented by the staff's findings. In very considerable part as a result of these findings and recommendations, Congress passed the Civil Rights Acts of 1960 and 1964, and the Voting Rights Act of 1965, while the Executive Branch initiated a broad program to eliminate discrimination in governmental agencies and Federally controlled programs of aid and assistance to the states.[71]

A statement made in 1963 by a one-time staff director of the Commission made a similar point about the Commission's effectiveness despite its lack of enforcement authority:

> Though the Commission is a fact-finding agency alone and has no powers of enforcement, it will, I believe, be seen by history as a major and dynamic force for the realization of civil rights in America. It has done things that no group or other agency could do. It established national goals, conceived legislation, criticized inaction, uncovered and exposed denials of equality in many fields and places, prodded the Congress, nagged the Executive, and aided the Courts. Above all, it has lacerated, sensitized, and perhaps even recreated the national conscience.[72]

---

69. FOSTER RHEA DULLES, THE CIVIL RIGHTS COMMISSION: 1957–1965 at 2–3 (1968).

70. *Id.* at 11–12 (citing H.R. 291, 85th Cong. (1957)). It may be noteworthy that proposals for a Civil Rights Commission had circulated for years without success. Congress created the Commission only after President Eisenhower included the proposal in his 1956 State of the Union message. *Id.* at 11.

71. *Id.* at 257.

72. *Id.* at 258 (quoting speech of Berl Berhard).

The recent history of the Civil Rights Commission reveals significant fighting between liberals and conservatives and between Republicans and Democrats. Civil rights issues have always been controversial, but more recent disputes centered on partisan issues, personalities, and appointments. That was not always true.[73] Controversy over the Commission increased with actions taken and appointments made by President Ronald Reagan in the early 1980s, and continued during the Clinton and Bush Administrations.[74] The more recent record of the Commission is not the part of its history that should be considered as a model for a privacy agency. The recent controversies may be a partial reflection of the changed views on civil rights and on the role of the Commission after decades of activity and evolution.

The Civil Rights Commission shows that a government agency can serve a useful purpose in highly visible and contentious public policy disputes without having either regulatory or enforcement authority. If a privacy board could accomplish some of what the Civil Rights Commission did during in its early years, the contribution would be important. No existing American institution plays the role of fact finder, investigator, policy resource, and opinion leader for privacy.

IV. Features of a Privacy Agency

The draft legislation identifies five mandatory functions for the Privacy Protection Board, along with a larger set of permissive activities. Most mandatory functions involve the preparation of Privacy Act of 1974[75] guidelines and other materials for use by agencies and the public. The Board would also be required to make legislative recommendations for revising the Privacy Act. These activities would result in valuable and needed materials. The Privacy Act itself is woefully out of date, and no existing institution in

73. *See* Editorial, *Sins of the Commission*, WASH. POST, Feb. 11, 2002, at A24, *available at* http://www.washingtonpost.com/wp-dyn/articles/A55482-2002Feb10.html:

> It wasn't always this way—and needn't be so now. When the commission was established during the Eisenhower administration, it used its investigative powers to shed light on systemic civil rights problems, and it spoke with great moral authority. That authority began breaking down during the 1970s, and the decline hastened during the Reagan administration, which sought to turn the commission's ideological direction around and make it a voice for conservative policies. The result was a pitched ideological battle.

Id.

74. *See, e.g.*, Darryl Fears, *A Deepening Divide on U.S. Civil Rights Panel; Controversy Over Appointment Highlights Historical Disagreements Over Commission's Role*, WASH. POST, Dec. 18, 2001, at A3.

75. 5 U.S.C. § 552a (2000).

government or outside of government has the interest to undertake the difficult task of modernizing what is now an ancient privacy law.[76] All mandatory activities would be useful, but none justifies a permanent privacy agency.

A. Functions: The Importance of Fair Information Practices

The most important mission for a Privacy Protection Board would be to promote the adoption and implementation of Fair Information Practices ("FIPs") in the United States. The reference to FIPs is not casual. FIPs are the most widely recognized international principles in information privacy. FIPs are especially significant because they form the basis of most privacy laws around the world.[77] Even most U.S. privacy laws reflect FIPs to some extent, although rarely with any overt awareness on the part of Congress. The international policy convergence around FIPs 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.[78]

FIPs are an American invention. They were a major contribution of the 1973 HEW Advisory Committee.[79] According to

76. *See* Robert Gellman, *Anyone Out There Up to Fixing the Privacy Act?*, GOV'T COMPUTER NEWS, Aug. 9, 1999, at 22 (suggesting that the Computer Science and Telecommunications Board at the National Research Council be given an assignment to propose revisions to the Act).

77. BENNETT, *supra* note 3, at 6. *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 (last visited Feb. 26, 2003).

78. BENNETT, *supra* note 3, at 95–96.

79. HEW Report, *supra* note 38, at 41. 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;

Committee Chairman Willis Ware, the name "Code of Fair Information Practices" was inspired by the "Code of Fair Labor Practices."[80]

Privacy scholar David Flaherty wrote that the FIPs Code "greatly influenced the Privacy Act and subsequent data protection legislation in other countries."[81] European privacy laws starting in the early 1970s used the FIPs concepts included in the U.S. Privacy Act of 1974.[82]

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.[83] The Organization for Economic Cooperation and Development ("OECD") issued its own privacy guidelines around the same time.[84] Both documents

---

> 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 him; [and]
>
> 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.

Id. at 41.

80. Willis Ware, An Account of the HEW Advisory Committee (RAND Document P-7846, 1993).

81. FLAHERTY, *supra* note 4, at 306. Colin Bennett called the Committee's report "surprisingly coherent and influential." BENNETT, *supra* note 3, at 70.

82. *See* FLAHERTY, *supra* note 4, at 21, 107.

83. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, 20 I.L.M. 317 (entered into force Oct. 1, 1985), *available at* http://conventions.coe.int/treaty/en/treaties/html/108.htm.

84. Org. for Econ. Cooperation and Dev., Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Oct. 1, 1980, 20 I.L.M. 422, *available at* http://www.oecd.org/EN/document/0,,EN-document-43-1-no-24-10255-43,00.html.

The OECD Guidelines include these Fair Information Practices:

> *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

relied upon FIPs as the central organizing principles. These two documents spurred greater international recognition of FIPs as core privacy policies during the 1980s.[85] The international organizations expanded upon and revised the original statement of FIPs from the HEW Advisory Committee seven years earlier.

An academic study[86] by Professor Colin Bennett of the development of privacy policy suggested five major reasons for the international convergence around FIPs. The first reason is the spread of computer technology. Privacy was a concern before the computer, but the data protection movement did not take hold before computer use became widespread. Second, countries study the experiences of others and emulate the solutions found elsewhere. Third, an international policy community with shared interests and some domestic influence spread common ideas and responses. Fourth, privacy work undertaken by international organizations pressured other governments to conform to international policies. Finally, actions taken by one country can prompt other countries to adopt a conforming policy.

The OECD statement of FIPs was embraced by the United States, a member of the OECD. During the Reagan Administration,

---

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 (*i*) within a reasonable time; (*ii*) at a charge, if any, that is not excessive; (*iii*) in a reasonable manner; and (*iv*) in a form that is readily intelligible to him; (c) to be given reasons if a request made under sub-paragraphs (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.

Id. at 424–25.

85. *See* BENNETT, *supra* note 3, at 130–40.

86. *Id.* at ch. 4.

the National Telecommunications and Information Administration ("NTIA") at the Department of Commerce actively supported the OECD Guidelines and urged corporations to comply voluntarily with them.[87] NTIA's support was part of an effort to show a serious commitment to privacy through voluntary action rather than legislation.[88] 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 questioned, and the effect of the endorsements was unclear at the time.[89] The corporate endorsements have long since been forgotten.

Regardless, the early expression 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. Nor are the Guidelines irrelevant in the Internet era. At a 1998 meeting of OECD Ministers, the United States joined with others to reaffirm the objectives of the Guidelines for the collection and handling of personal data in any medium, including global networks.[90] However, some critics believe that the OECD Guidelines are out of date or in need of some revision.[91]

In the United States, restatements of FIPs without all internationally recognized elements are found more frequently.[92] The

87. *See Report on OECD Guidelines Program: Hearings Before A Subcomm. of the Comm. on Gov't Operations,* 97th Cong., *reprinted in* INT'L TELECOM. & INFO. POL'Y 27–58 (1981) (memorandum from Bernard J. Wunder, Jr., Assistant Sec'y for Commerce & Info., Dep't of Commerce).

88. *See* WILLIAM J. ANDERSON, U.S. GEN. ACCOUNTING OFFICE, PRIVACY POLICY ACTIVITIES OF THE NAT'L TELECOMMUNICATIONS AND INFO. ADMIN., 4 (GGD-84-93, 1984).

89. *See Privacy Regulatory Proposals*, *supra* note 12, at 227–33.

90. OECD Ministerial Conference, Conference Conclusions (1998), www.anu.edu.au/mail-archives/link/link981010208.html.

91. *See, e.g.*, Roger Clarke, Beyond the OECD Guidelines: Privacy Protection for the 21st Century (2000), http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html (last visited Feb. 26, 2003). In 1999, Mr. Justice Michael Kirby of the High Court of Australia—the former chair of the OECD Committee that developed the 1980 Privacy Guidelines—suggested that some updating of the Guidelines might be needed in light of advances in technology. See his remarks at the International Conference on Privacy and Personal Data Protection (1999), http://www.pco.org.hk/english/infocentre/conference.html. Kirby concluded, however, that the OECD "framework of privacy principles . . . has been extraordinarily successful and remarkably enduring." *Id. See also* Ann Cavoukian, A Report to the 22nd International Conference of Data Protection Commissioners: Should the OECD Guidelines Apply to Personal Data Online? (2000), http://www.ipc.on.ca/scripts/index_.asp?action=31&p_ID=11425&N_ID=1&PT_ID=98&U_ID=0 (last visited Feb. 26, 2003).

92. Restatements in other countries are also found. It is much more likely, however, that other countries will adopt a policy close to the OECD principles. In Canada, for example, the Canadian Standards Association ("CSA") developed a privacy code as a National Standard of Canada in 1996. MODEL CODE FOR THE PROTECTION OF

use of FIPs as a label for privacy policies is slowly increasing in the United States, and this suggests that international standards are seeping into American consciousness. However, American versions of FIPs are often significantly bowdlerized, with modifications or omissions to provisions that the business community views as inconvenient.

An example of an abbreviated version of FIPs comes from the Federal Trade Commission.[93] In 2000, the Commission recommended that consumer-oriented commercial web sites 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, a significantly weaker provision.

The FTC statement of FIPs does not address the *collection limitation* or *data quality* principle. The *accountability* principle is not mentioned, but it is part of the FTC's proposal by implication since the Commission would enforce the legislation, 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,[94] a 1998 law that the FTC enforces, addresses all traditional elements of

PERSONAL INFORMATION CAN/CSA Q830-96 (Can. Standards Ass'n), *available at* http://www.qmi.com/registration/privacy/default.asp?load=content&language=English. The starting point for the CSA effort was the OECD Privacy Guidelines. In 2000, Canada then enacted a private sector privacy law that directly incorporated the CSA Model Code into law. Personal Information Protection and Electronic Documents Act, R.S.C., ch. 5 (2000) (Can.), *available at* http://www.privcom.gc.ca/legislation/02_06_01_e.asp. The Canadian law was found by the European Commission to meet EU standards for data protection laws. Commission Regulation 2002/2 of 20 December 2001 on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act, *available at* http://europa.eu.int/eur-lex/en/dat/2002/l_002/l_00220020104en00130016.pdf. The acceptance of the Canadian law by the EU shows how different formulations of FIPs can still meet international standards. 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).

93. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

94. 15 U.S.C. §§ 6501–06 (2000).

FIPs in some manner. However, the Commission did not recommend that all FIPs elements be included in proposed legislation applying to a broader set of web site operators and data subjects. Nor did the Commission explain why it did not support enactment for all Internet users of the FIPs applicable to children. The Commission's formulation of FIPs was similar to versions from parts of the American business community.[95]

The FTC's endorsement of a diluted version of FIPs is one reason that the Commission is not a good candidate to serve a larger role in privacy policy. The Commission's privacy vision is too limited. In addition, the Commission does not have jurisdiction over many private sector, non-profit, and governmental record keepers.

The purpose of this discussion of FIPs is to show that a congressional statement about the value of FIPs in establishing privacy rules would be valuable and essential. The Privacy Protection Board needs to have some legislative policy direction to guide its work. The draft bill deliberately lists only the titles of the OECD FIPs principles and does not reproduce the content. One reason for the limited reference is political. The full OECD statement of FIPs would be too much of a lightning rod in the current environment to expect that it could survive the congressional process. Failure to recognize all elements of FIPs might, however, lead privacy advocates and other national privacy agencies to view the Privacy Protection Board as too crippled to be useful.

Another reason has to do with the nature of FIPs. Translating FIPs into privacy laws or policies is complex and judgmental because the FIPs principles are not self-implementing. For any type of records or record keeper, application of FIPs depends on many 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. A common reliance on FIPs does not avoid all problems or conflicts and does not answer all privacy policy questions. 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.

Protecting privacy nearly always requires a balance. 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

95. Some in the business community would find even the FTC's limited version of FIPs to be too strong. *See, e.g.*, the privacy protection practices of The Direct Marketing Association, http://www.the-dma.org/privacy.shtml (last visited Feb. 26, 2003). The DMA's privacy policy is basically *notice* and *opt-out*. *Id.* Most FIPs elements are missing.

accommodating other important social, political, or economic ends."[96] These other goals include national security, law enforcement, economy and efficiency, and public health. FIPs provide a framework for making sure that the balancing includes essential elements of privacy. The application of the same principles will not always result in the same outcome. The tradeoffs between privacy and other values depend greatly on the context.

This diversity is needed in setting a broad policy direction for a privacy agency. Congress is not likely to agree on many details because there is no consensus in the United States on those details. However, Congress could well agree on broadly stated general principles, with the express understanding that those principles can be applied in different ways. Consensus is possible, but only at higher levels of generality. Part of the work of the Privacy Protection Board would be translating FIPs into practice and helping record keepers and record subjects address the implementation specifics.

Another reason for starting from international principles is to bring the United States more into conformity with the rest of the world. Even if American acceptance of international principles is only skin deep, it will help to lessen differences between the privacy regimes in the United States and other countries. A formal legislative recognition of FIPs will be a valuable step.

B. No Regulatory Authority

The Privacy Protection Board would have no regulatory powers. There are several reasons for proposing a non-regulatory agency.

First, as the history of the Civil Rights Commission demonstrates, it is possible for a non-regulatory agency to contribute to a national response to a contentious policy issue. The answer to all privacy problems is not necessarily additional regulation. At least some of the laws and regulations adopted to date have not produced results that make record keepers or record subjects happy.[97] Indeed,

96. Charles D. Raab, *From Balancing to Steering: New Directions for Data Protection*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 68, 68 (Colin J. Bennett & Rebecca Grant eds., 1999) (footnote omitted).

97. Perhaps the best example is the Gramm-Leach-Bliley Act. *See* 15 U.S.C. § 6801 (2000). Janger & Schwartz say that GLB "has managed to disappoint both industry leaders and privacy advocates alike." Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230 (2002). For complaints from organizations representing consumers, *see, e.g.*, *An Examination of Existing Federal Statutes Addressing Information Privacy: Hearing Before The House Comm. on Energy & Commerce*, 107th Cong. (2001) (testimony of Ed Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group), *available at* http://energycommerce.house.gov/107/hearings/04032001Hearing154/Mierzwinski242.htm; Mark Hochhauser, Ph.D., Lost in the Fine Print: Readability of Financial Privacy Notices, *at* http://privacyrights.org/ar/GLB-Reading.htm (last visited

it is hard to point to a fully successful privacy legislative or regulatory initiative. The shortcomings of current regulatory efforts suggest a reason to explore alternative approaches to addressing privacy issues.

Second, the task of regulating all activities in the United States that affect privacy would be overwhelming. Every institution that maintains personal data, including all government agencies, private businesses and non-profit organizations, might be the target of regulation. Even a mildly comprehensive attempt to regulate personal data processing activities could take decades. The politics of comprehensive privacy regulation would be impossible to manage, and the administration of broad rules would require enormous resources. Omnibus privacy legislation of the type found in Europe and elsewhere around the world is not likely to succeed in America, in part because of American demands for detailed regulatory instruments.

Third, some existing agencies already conduct limited regulation of activities affecting privacy. The Federal Trade Commission oversees the Fair Credit Reporting Act,[98] the Gramm-Leach-Bliley Act,[99] and the Children's Online Privacy Protection Act.[100] The Federal Communications Commission has responsibilities under the Telephone Consumer Protection Act.[101] The Department of Education enforces the Family Educational Rights and Privacy Act.[102] Whether any of these agencies is doing a good job is an open question. All have many other responsibilities, and their interest in privacy enforcement has waxed and waned over the years. However, trying to transfer all of these enforcement and oversight functions to a new agency would be a political impossibility.

Fourth, a Privacy Protection Board would be more effective supplementing rather than replacing existing regulators. The Board's permissive functions would include receiving complaints, participating in agency proceedings, and petitioning agencies to take action on matters affecting privacy rights and interests. The Board could use its limited resources to encourage other agencies to do a

Feb. 26, 2003). While consumer groups find GLB too weak, financial institutions tend to think that the law strikes the right balance. However, the lack of federal preemption of state laws in GLB draws objections. *See, e.g., Financial Privacy and Consumer Protection: Hearing Before The Senate Comm. on Banking, Hous., & Urban Affairs*, 107th Cong. (2002) (testimony of John Dugan, Financial Services Coordinating Council), *available at* http://banking.senate.gov/02_09hrg/091902/dugan.htm.

98. 15 U.S.C. § 1681s (2000).

99. 15 U.S.C. §§ 6804–05 (2000). Numerous other federal agencies share in regulatory and enforcement activities under the law. *Id.*

100. 15 U.S.C. § 6505 (2000).

101. 47 U.S.C. § 227 (2000).

102. 20 U.S.C. § 1232g (2000).

better job with their ongoing responsibilities, particularly their enforcement responsibilities.

C. Independence

The most important feature of the proposed Privacy Protection Board is independence. The Board would be an independent agency in the executive branch, with its members appointed by the President, and confirmed by the Senate. The President would designate the Chairman. Members would serve fixed term appointments, with the possibility of reappointment to a single additional term. The Board would be an independent agency just like the Federal Trade Commission, Federal Communications Commission, and Securities and Exchange Commission. Members of the Privacy Protection Board would have the ability, by virtue of fixed term appointments, to speak their minds on matters relating to privacy. Like members of other comparable independent agencies, they would not be subject to removal from office for disagreeing with the President.

The principal reason for independence is simple. Only an independent agency can criticize the policies and practices of the executive branch. Whether the government or the private sector presents the greatest threat to privacy is an interesting subject for debate. However, it is undisputed that many routine government functions can have drastic effects on the privacy rights and interests of individuals. The federal government maintains enormous volumes of personal information for its own operations. The federal government would be a major subject of inquiry for a privacy agency, along with the private sector.

Any privacy policy or oversight function assigned to an agency within the executive branch and subject to the direct control of the President cannot be independent. For example, the Privacy Counselor who served at the Office of Management and Budget from 1999–2001 appeared to make a significant contribution to the setting of policy in the Clinton Administration.[103] Despite the limited resources available to the Privacy Counselor (there were only two other staff positions in his immediate office), the Counselor played an important role on privacy issues related to health, financial, and Internet privacy policy and legislation. In addition, the Counselor

103. In an unpublished paper, the Clinton Administration's privacy counselor argues with some persuasion that a privacy official located at OMB is valuably involved in coordinating privacy policy across multiple issues and multiple agencies. *See* Peter P. Swire, The Administration Response to the Challenges of Protecting Privacy (Jan. 8, 2000) (unpublished draft), http://www.peterswire.net/STANF7.doc. Swire also argues that a political appointee, rather than a civil servant, can be more effective. *Id.* at 35.

worked on international privacy efforts as well as a variety of other legislative, regulatory, and administrative matters.

However, the Privacy Counselor was not an independent voice. The Privacy Counselor was located in the Office of Information and Regulatory Affairs[104] at OMB under the supervision of several levels of OMB management. He had no ability to publicly question, criticize, or object to decisions announced by the administration. Once the Clinton Administration established policy, the Privacy Counselor was obliged to publicly support that policy. No matter how effective an internal voice may be, it is not the equivalent of an independent, external one.

A privacy office located in another agency would be subject to the same limitations. Consider how a privacy office established in the Department of Commerce might function.[105] Disputes between the privacy office and the Bureau of the Census (another component of the Commerce Department) would almost certainly be resolved by the Secretary of Commerce. A privacy officer within a department would not have the ability to appeal beyond the Secretary. Disputes between a privacy policy office at the Commerce Department and government offices in other departments would be more likely to be resolved outside the Department, probably by OMB. In either case, a privacy office might not be able to raise questions publicly, hold hearings, solicit comments, or conduct investigations, and the office would certainly not be able to speak publicly without the approval of its political overseers at the Commerce Department.

A Privacy Protection Board would not be the exclusive privacy office for the executive branch. A privacy policy function can, and perhaps should, be included within any administration. Many government activities affect privacy, and an administration is obliged to take positions on privacy legislation proposed by Congress and on international privacy matters. The coordination of privacy policy within the executive branch is just as important as the coordination of policies on communications, securities regulation, trade regulation, and other issue areas assigned to independent regulatory agencies.

The importance of independence in data protection agencies is well-established in the EU and elsewhere around the world. A prefatory recital to the EU Data Protection Directive states expressly that "complete independence" is an "essential component" of the

104. *Id.* at 20.

105. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998). The authors recommended that a privacy office be established in the Department of Commerce, rejecting OMB or other parts of the Executive Office of the President as a home. *Id.* at 185–86. Swire later became the privacy counselor at OMB. Swire, *supra* note 103, at 1.

protection of individual privacy.[106] The substantive provisions of the Directive require each Member State to have an independent supervisory authority that must be consulted when administrative activities will affect the processing of personal data.[107] The authority must have power to investigate, to intervene, and to engage in legal proceedings. The EU standards for supervisory authorities have influenced the establishment of most privacy agencies in other countries.

Professor Flaherty's review of international privacy activities also emphasized the importance of independence in the operations of data protection offices:

> [D]ata protection agencies exercise a degree of independence in the performance of their tasks that is relatively unusual among governmental institutions. Observers and practitioners agree that data protection agencies require as much independence as is constitutionally possible, subject to the most appropriate type of governmental, legislative, administrative, or judicial review, since independence must be balanced with some form of accountability.[108]

Independence is vital for a privacy agency's governmental oversight activities. However, that does not mean that the agency should only have governmental responsibilities. Independence may not be as crucial for an agency's review of private sector privacy activities, but the agency can and should play a role with respect to the private sector. No existing agency has a broad mandate to oversee private sector self-regulatory privacy activities.

D. Private Sector Responsibilities

Even though the proposed privacy agency would not have any regulatory authority over the private sector, it could and should have the ability to support and encourage the adoption and implementation of FIPs by private sector organizations, including both for profit and non-profit institutions. The draft proposal allows the Privacy Protection Board to "comment on or assist in the development or implementation of policies designed to provide for the protection of personal information maintained by private sector record keepers." Under this authority, the Board could informally approve a self-regulatory privacy code at the request of the proponent. The Board could also comment upon codes adopted without its approval.

In Europe, where legislation establishes mandatory privacy standards, codes of conduct "contribute to the proper

106. Council Directive 95/46, recital 62, 1995 O.J. (L 281) 31, *available at* http://elj.warwick.ac.uk/jilt/dp/material/directiv.htm.

107. *Id.* at art. 28.

108. FLAHERTY, *supra* note 4, at 391 (footnote omitted).

implementation"[109] of national laws. The Netherlands offers a partial model. The Netherlands data protection law gives the data protection authority a formal role in approving private sector codes of conduct. Under the Dutch law, an organization applies to the College Bescherming Persoonsgegevens (Dutch Data Protection Authority) seeking a declaration that a sectoral code of conduct properly reflects the legal requirements for the processing of personal data. The law requires that requests for approval must come from a representative organization, that the sector be precisely defined, and that any dispute procedures be independent.[110]

Despite the lack of privacy legislation covering most personal data processing activities in the United States, industry or company codes are increasingly common. However, the quality of those codes is highly variable. One reason is that codes are typically drafted by the industry without any outside participation or comment. No existing institution serves as a proxy for data subjects. Occasionally, a privacy advocacy group will comment, positively or negatively, on a private sector policy. The Federal Trade Commission has also commented from time to time on industry codes.[111] State attorneys general also provide some review of industry privacy activities, and the states have regularly been more effective in producing meaningful change than the FTC.[112] However, systematic review of most private sector privacy policies is rare.

Several organizations have been established to give seals of approval to corporate privacy policies for web sites. TRUSTe[113] and

109. Council Directive 95/46, *supra* note 106, at art. 27(1).

110. Personal Data Protection Act, No. 92 at art. 25 (1999) (Neth.) (Session 1999–2000 Nr. 92), *available at* http://www.cbpweb.nl/english/en_pdpa.htm. The EU Data Protection Directive encourages the use of industry codes of conduct. *See* Council Directive 95/46 at art. 27.

111. The Children's Online Privacy Protection Act encourages a safe harbor procedure as an incentive for self-regulation, and the FTC must approve requests for safe harbor treatment. 15 U.S.C. § 6503 (2000).

112. An interesting comparison of the effectiveness of the review of private sector privacy policies can be taken from recent events involving Amazon.com. In 2000, Amazon announced a change in its privacy policy. Two organizations asked the FTC to investigate the changes, alleging that Amazon deceived consumers in representations about its privacy policy. The FTC reviewed the matter and did not act. Two years later, several state attorneys general pressured Amazon.com to revise the same privacy policy. *See* Troy Wolverton, *Amazon to Revamp Privacy Policy*, CNET NEWS.COM (Sept. 25, 2002), *at* http://news.com.com/2100-1017-959571.html. State attorneys general have often produced better results for consumers on privacy matters than the FTC. *See, e.g.*, Professor Joel Reidenberg, The Toysmart Bankruptcy, Paper Presented at the 23rd International Conference of Data Protection Commissioners (Sept. 24, 2001), http://reidenberg.home.sprynet.com/Toysmart.pdf (last visited Feb. 26, 2003). *See also* Robert Gellman, *States Are Trumping FTC on Privacy*, DM NEWS, Oct. 7, 2002, at 12.

113. *See* http://truste.org (last visited Feb. 26, 2003).

BBBOnline[114] are two examples. These seal programs rely mostly on disclosure of privacy policies and a procedure for resolution of complaints. Substantive standards are weak. The credibility of the programs has suffered because financial support for the privacy seal organization comes from the corporate seal holders. TRUSTe in particular has been the subject of a constant series of attacks for not acting against companies believed to have violated TRUSTe's rules.[115] The seal programs do not have sufficient independence to be able to serve a broader role. The programs also have had limited success in attracting participants.

A federal Privacy Protection Board would offer record keepers adopting privacy policies both a source of expertise and independent approval. By operating under a statutory mandate to encourage the adoption and implementation of FIPs, the Board could measure privacy codes against general standards. Approval of a privacy policy or self-regulatory code by the Privacy Protection Board would offer a significant degree of assurance that the policy or code should be accepted by data subjects as providing an adequate degree of privacy protection.

Imagine that a trade association decides to develop a self-regulatory code for privacy. Under today's pattern, the association develops the code through closed industry deliberations and announces its adoption with a glowing press statement about the great privacy advances it has voluntarily adopted. The lack of tension undercuts the credibility of self-regulation. This pattern has produced a series of industry self-regulatory actions ranging from indifferent to worthless.

However, consider the same scenario with a privacy agency willing and able to measure the self-regulatory code against a fair information practice yardstick. No industry is likely to take the chance that its self-regulatory code will be undercut by criticism from a privacy agency. To forestall criticism, the industry would likely ask the privacy agency for a blessing. The resulting discussion and negotiations will lead to a stronger and more complete set of privacy rules. Much can be accomplished without the need for legislation or regulation.

A privacy agency would benefit both consumers and industry. The advantage for consumers is more honest and balanced self-regulatory codes of practice. The advantage for business is the ability

114. *See* http://bbbonline.org (last visited Feb. 26, 2003).

115. *See, e.g.*, Paul Boutin, *Just How Trusty Is Truste?*, WIRED NEWS, Apr. 9, 2002, *at* http://www.wired.com/news/exec/0,1370,51624,00.html; Alex Lash, *No More Hand-Holding*, THE INDUSTRY STANDARD, Nov. 12, 1999, *available at* http://www.thestandard.com/article/display/0,1902,7648,00.html.

to adopt privacy rules with the support and assistance of an institution charged with protecting privacy. Today, businesses face criticism over privacy actions no matter what they do. No existing consumer or privacy institution has the standing or resources to negotiate over privacy on behalf of the public. A privacy agency can perform that function with credibility, and it can defend the results of the process. The result would be enhanced self-regulation with greater credibility. No institution would be obliged to bring its privacy rules to the Board for approval. However, the credibility of an unapproved code would be diminished, and the risk of negative comments from the Board would discourage the adoption of weak privacy codes. An agency can also seek to make sure that a code is working as promised, and this would contribute to the maintenance of a level playing field among competing companies.

E. International Activities

The proposed legislation would give the Privacy Protection Board the ability to play a role in international privacy matters. The Board could assist in coordination of U.S. privacy laws, policies, and practices with laws, policies, and practices of foreign governments. It could also accept inquiries and complaints from foreign governments.

The Board would not be empowered to represent the United States formally on international privacy matters. Official representation would continue to belong to the President and to agencies that the President controls directly. The Board could participate in lower level international cooperative efforts, and the Board could provide continuity in international relations that has been missing to date. A stable U.S. presence at international privacy conferences and discussions would be welcomed, and it is likely that differences between the United States and other nations over privacy could be more easily resolved as a result.

In addition, the Board could solve a potential problem with the Safe Harbor Agreement between the Department of Commerce and the European Commission. The Agreement was finalized in 2000 to address data protection barriers to the transfer of personal data from EU Member States to the United States. The EU Data Protection Directive prohibits the transfer of personal data to non-EU nations that do not meet the European "adequacy" standard for privacy protection.[116] The Safe Harbor Agreement allows a U.S. company to certify to compliance with the Agreement's standards. The EU accepts the certification and allows personal data to be sent to that

116. Council Directive 95/46, *supra* note 106, at art. 25(1).

company in the United States despite the absence of adequate privacy laws.[117]

An essential element of the Safe Harbor Agreement is enforcement by the Federal Trade Commission against Safe Harbor companies that do not comply with their promise to comply with the standards in the Agreement. The FTC claims jurisdiction under section 5 of the FTC Act prohibiting unfair or deceptive acts or practices. Under the FTC's view of its law, a company's failure to comply with a promise to meet Safe Harbor standards would be actionable as an unfair or deceptive practice.[118] The FTC promised to give priority to complaints regarding privacy violations by Safe Harbor companies.[119]

However, it is not entirely clear that the FTC's jurisdiction extends to protecting foreign consumers. Professor Joel Reidenberg reviewed the legislative and judicial history of section 5 of the FTC Act and concluded that the FTC's assertion of jurisdiction over the Safe Harbor process "is a radical departure from the stated legislative purposes of the statute and in direct opposition to the Supreme Court's restrictive interpretation of section 5 authority."[120] Without the possibility of FTC enforcement, the entire Safe Harbor process would be in danger of collapse.

The Privacy Protection Board could take over some of the enforcement role in international privacy arrangements under the provision allowing it to accept and investigate inquiries and complaints from foreign governments with respect to privacy rights and interests. The Board would not need the full range of enforcement powers that the FTC exercises. It would only need to find facts. Once the Board determined that a Safe Harbor company violated its agreement to comply with the Safe Harbor principles, enforcement would come from the EU by cutting off the flow of personal data to the offending company. The Board would not have to enforce its findings. The FTC could still play a role when appropriate by pursuing other remedies if needed.

---

117. The Department of Commerce's Safe Harbor web site can be found at http://www.export.gov/safeharbor. As of the beginning of February 2003, fewer than 300 companies have agreed to enter the Safe Harbor. *See* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Feb. 26, 2003).

118. Letter from Robert Pitofsky, Chairman, Federal Trade Commission, to John Mogg, Director, DG XV, European Commission, ¶ 3 (July 14, 2000), *available at* http://www.export.gov/safeharbor/FTCLETTERFINAL.htm.

119. *Id.* at ¶ 6.

120. *Implications for the U.S. Privacy Debate: Hearing on the EU Data Protection Initiative Before the Subcomm. on Commerce, Trade & Consumer Prot. of the House Comm.on Energy & Commerce*, 107th Cong. (2001) (testimony of Joel R. Reidenberg, Professor of Law, Fordham Univ. Sch. of Law), *available at* http://reidenberg.home.sprynet.com/Reidenberg_Testimony_03-08-01.htm.

F. Federal Government Privacy Management and Oversight

The proposed legislation assigns the Privacy Protection Board responsibilities regarding federal agency activities under the Privacy Act of 1974. These include developing privacy guidelines for federal agencies; issuing advisory opinions regarding the Act; investigating compliance with the Act; filing comments on proposals to create or amend Privacy Act systems of records or rules; and commenting on actions of federal agencies that affect privacy. The Board would be required to develop several different types of guides and guidelines. The authority to advise, investigate, and comment would be permissive. No agency would be required to comply with the advice or recommendations of the Board.

No existing federal agency has the authority and interest to oversee Privacy Act operations. The Privacy Act of 1974 assigned the Office of Management and Budget responsibility for developing guidelines and regulations and for providing continuing assistance to and oversight of agency implementation of the Act.[121] Except for the brief period during the Clinton Administration when OMB had a Privacy Counselor, OMB has paid little attention to its Privacy Act responsibilities during the last twenty-five years.[122] Even during the Privacy Counselor's tenure, the Privacy Act was a relatively minor focus of attention. While OMB has the power to direct other agencies to do a better job of Privacy Act compliance, OMB does not have the interest to engage in meaningful oversight.

The proposed Privacy Protection Board would be able to carry out the responsibilities that OMB has ignored in the past. The Board would not have direct authority to order agencies to take actions because of concern that an independent agency could not constitutionally issue orders to an agency subject to direct presidential control. The Board could review agency Privacy Act activities and could work cooperatively with OMB to improve government-wide compliance with the Act.

Conclusion

Professor Spiros Simitis, Germany's first data protection official described the American approach to data protection as "an obviously erratic regulation full of contradictions, characterized by a fortuitous

121. 5 U.S.C. § 552a(v) (2000).

122. H.R. REP. NO. 98-455, at 34–35 (1983); U.S. GEN. ACCOUNTING OFFICE, PRIVACY ACT: FEDERAL AGENCIES' IMPLEMENTATION CAN BE IMPROVED (GGD-86-107, 1986). *See, e.g.*, OFFICE OF TECH. ASSESSMENT, 99TH CONG., FEDERAL GOV'T INFO. TECH.: ELEC. RECORD SYS. AND INDIVIDUAL PRIVACY (1986); *Privacy Regulatory Proposals*, *supra* note 12, at 221–26.

and totally unbalanced choice of its subjects."[123] Simitis wrote those words in 1992, but the situation has really not changed.

The American approach to privacy is, in many ways, a reflection of the American approach to law and public policy when there is no clear consensus about the right thing to do or how to do it. We lurch back and forth between disjointed and inconsistent responses. We apply last year's response to next year's technology, and we find that the result does not work well. We do nothing when something is needed, and when we do something, it often does not work. We pass legislation to protect the privacy of one type of record while allowing virtually identical records to remain unregulated.[124]

We rarely confront privacy issues squarely or comprehensively. We do little to educate the American public or corporate record keepers about the real stakes in the privacy arena or about the limitations of what can be achieved in the modern world. We obscure questions about who bears the cost of protecting privacy.[125] As a result, expectations are often unrealistic, and solutions rarely match the expectations or the political rhetoric.

Addressing privacy is especially hard because the borders of privacy can be impossible to define with any precision. It is difficult to cleanly distinguish between types of records. A health record in one context becomes a financial or Internet record in another. For example, when a co-payment of a health insurance claim is made by a patient to a physician through an online transfer of funds, are the resulting records subject to rules for health records, banking records, insurance records, or Internet records? Similarly, it is difficult to draw a clean line between sectors because traditional sectoral lines blur, and the same personal data may be used for multiple purposes by a company with numerous lines of unrelated business.

It is also difficult or impossible to identify real borders, whether between states or nations.[126] Internet transactions can take place with

123. Spiros Simitis, *New Trends in National and International Data Protection Law*, *in* RECENT DEVELOPMENTS IN DATA PRIVACY LAW 22 (J. Dumortier ed., 1992).

124. For example, the Cable Communications Policy Act provides some privacy protections for personal information collected by cable television operators, but others who provide similar services through direct broadcast satellite or in other ways are not subject to the same rules. 47 U.S.C. § 551 (2000). The Video Privacy Protection Act protects privacy and First Amendment interests by limiting the use and disclosure of video rental records. 18 U.S.C. § 2710 (2000). No law protects similar interests in book or magazine purchase records.

125. *See* Robert Gellman, Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete (2002), *at* http://www.epic.org/reports/dmfprivacy.html (last visited Feb. 26, 2003).

126. *See* 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).

neither the merchant nor the customer knowing in which legal jurisdiction the other resides. Merchants are often located in multiple jurisdictions, and they may be unable to determine which privacy laws apply to which transactions. Small differences in data processing methodology can make a large difference to jurisdictional determinations.[127] The confusion can be seen in U.S. privacy laws, which sometimes share jurisdiction between state and federal governments,[128] and which sometimes ignore international implications.[129]

We cannot always clearly distinguish an online activity from an offline activity. When an online order results in physical delivery of a product, should the resulting records be subject to the rules for online or offline records? It can even be difficult to distinguish clearly or fairly between opt-in and opt-out regimes for regulating personal data uses.[130] The difficulty of making these distinctions will not disappear soon. A permanent privacy agency with expertise will help. However, an agency will not be a magic bullet that will make the problems disappear immediately or permanently.

One of the major political shortcomings with a privacy agency—and especially a non-regulatory agency—is that it offers a procedural or institutional response to a substantive problem. It is hard to explain why a small bureaucracy without any direct regulatory authority will help a voter who has a credit record replete with errors; a victim of identity theft; an individual who hates spam and telemarketers; a person who doesn't want his personal data sold to profilers by government; a Netizen who doesn't want her email read by government agents without sufficient cause; or a pedestrian,

127. *See, e.g.*, WORKING PARTY ON THE PROT. OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, WORKING DOCUMENT DETERMINING THE INTERNATIONAL APPLICATION OF EU DATA PROTECTION LAW TO PERSONAL DATA PROCESSING ON THE INTERNET BY NON-EU BASED WEB SITES (2002). The Working Party is established by Article 29 of the EU Data Protection Directive. *See* http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp56_en.pdf (last visited Feb. 26, 2003).

128. The health privacy rule promulgated under the authority of the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d–22 (2002), allows state laws that are more stringent than and not contrary to the federal rule to remain in effect. 45 C.F.R. § 160.203 (2002). *See also* the Gramm-Leach-Bliley Act. 15 U.S.C. § 6807 (2000).

129. The Children's Online Privacy Protection Aet applies to web sites outside the United States. 15 U.S.C. §§ 6501–06 (2000). The international application of this law was somewhat surprising in light of U.S. objections to the international application of EU data protection laws.

130. *See, e.g.*, Ari Schwartz & Paula J. Bruening, Center for Democracy and Technology, On Consent, Choice, and Check Boxes: Sorting Out the Opt-In v. Opt-Out Debate (undated), *at* http://www.cdt.org/publications/optin-optout.shtml (last visited Feb. 26, 2003).

driver, or traveler who does not want to be subjected to surveillance by cameras in the airport, on the highway, or in a store.

Others are unhappy with an agency because they are afraid that it will not facilitate their favored response to privacy. Some object because a privacy agency is not a law or regulation, and the creation of an agency will offer those who oppose laws and regulations a new reason for opposition. Others see a privacy agency as the camel's nose under the tent, with the camel in this case being more legislation and regulation. Some fear a privacy agency because it could make the self-regulatory process more honest and rigorous, and companies will be less able to adopt policies that have little or no substance. Some disapprove because the agency offers no remedies to individuals whose privacy has been violated. Others express concern that an independent agency will not have enough influence to affect federal government activities. Still others will oppose a privacy agency unless it guarantees federal preemption of state laws, class action lawsuits, a stronger role for consent in disclosures of health information, an exemption for their activity, or some other specific objective. Some will dissent because they do not want to perpetuate privacy as a public policy concern, hoping that privacy will eventually go away. Finally, some raise objections on grounds of cost, although a small agency with a hundred employees would cost less than $15 million annually.

These objections miss the point. A privacy agency will not guarantee any particular outcome. Everyone on all sides of the issue will take an equal chance that his or her preferred response to privacy will be encouraged by a Privacy Protection Board.

The most likely role for a privacy agency will be to serve as a catalyst. A Privacy Protection Board will help to achieve the responses to privacy that we are likely to achieve in its absence, but the Board will do so more quickly, more efficiently, and more consistently. If we choose legislation and regulation, the Privacy Protection Board will make that solution work better. If we choose self-regulation, the Board will make self-regulation work better. Even if we do nothing, the Board will contribute by conducting studies, doing oversight, encouraging more cooperation among all relevant parties, and keeping governmental and private sector record keepers honest. Under any scenario, the Board will contribute to a better understanding of privacy, information and other technologies, and public concerns.

Admittedly, there is a risk that a privacy agency may not achieve these results. A Privacy Protection Board could be populated with too many pro-privacy zealots or too many privacy detractors to develop credibility. Members of the Board could be lazy, cynical, out of touch, uncreative, indifferent, or undiplomatic. These are some

characteristics of the American approach to privacy seen in the last two decades. The greater risk is that we will continue stumbling down the crooked path we are on, and that we will never find a coherent way to make sense out of the conflicting demands for use and for protection of personal data. We have little to lose by proceeding with a privacy agency.

The failure of the United States to have a national privacy agency is, perhaps, the single most important difference in approach to data protection between the United States and most other industrialized countries.[131] Professor David Flaherty was direct in describing the effect of this difference. "The United States carries out data protection differently than other countries, and on the whole does it less well, because of the lack of an oversight agency."[132]

Since Flaherty wrote those words in 1989, the rest of the world has moved toward the European Union's model of data protection. More countries have data protection authorities that operate with a significant degree of independence. Data protection agencies in other countries have not become unreasonable or irresistible bureaucracies. Most of these agencies make useful contributions to the difficult privacy issues that every nation faces. An American Privacy Protection Board will do the same.

The time has come to establish an American Privacy Protection Board.

131. Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1383 (1992) ("The United States is almost alone among Western nations in its failure to create an institution with [data protection] expertise.").

132. FLAHERTY, *supra* note 4, at 305.

Appendix: Draft Privacy Protection Board Legislation

A bill to establish a Privacy Protection Board, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Section 1. Short Title.

This Act may be cited as the "Privacy Protection Board Act."

Section 2. Privacy Protection Board.

(a) Establishment of Board.

(1) There is established as an independent agency of the executive branch of the Government the Privacy Protection Board.

(b)(1) The Board shall be composed of 5 members who shall be appointed by the President, by and with the advice and consent of the Senate, from among members of the public at large who are well qualified for service on the Board by reason of their knowledge and expertise in any of the following areas: civil rights and liberties, law, social sciences, information policy, communications, technology, business, and state and local government. Not more than 3 of the members of the Board shall be adherents of the same political party.

(2) One member of the Board shall be designated Chairman by the President.

(3) The Chairman shall preside at all meetings of the Board, but the Chairman may designate another member as an acting Chairman who may preside in the absence of the Chairman. A quorum for the transaction of business shall consist of at least 3 members present, except that one member may conduct hearings and take testimony if authorized by the Board. Each member of the Board, including the Chairman, shall have equal responsibility and authority in all decisions and actions of the Board, shall have full access to all information relating to the performance of the duties and responsibilities of the Board, and shall have one vote. Action of the Board shall be determined by a majority vote of the members present. The Chairman (or Acting Chairman) shall see to the faithful execution of the policies and decisions of the Board, and shall report thereon to the Board from time to time or as the Board may direct.

(4) Members of the Board shall serve for terms of 5 years, except that a member may continue to serve until a successor takes office. Members shall be eligible for reappointment for a single additional term. Vacancies in the membership of the Board shall be filled in the same manner in which the original appointment was made.

(5) Vacancies in the membership of the Board, as long as there are 3 members in office, shall not impair the power of the Board to execute the functions and powers of the Board.

(6) The members of the Board shall not engage in any other employment during their tenure as members of the Board.

(7)(A) Whenever the Board submits any budget estimate or request to the President or Office of Management and Budget, it shall concurrently transmit a copy of that request to the Congress.

(B) Whenever the Board submits any legislative recommendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No officer or agency of the United States shall have any authority to require the Board to submit its legislative recommendations, testimony, or comments on legislation, to any office or agency of the United States for approval, comments, or review, prior to the submission of the recommendations, testimony, or comments to the Congress.

(c) Personnel of the Board.

(1)(A) The Board shall appoint an Executive Director and a General Counsel who shall perform such duties as the Board may determine. The appointments may be made without regard to the provisions of Title 5 of the United States Code.

(B) The Executive Director and the General Counsel shall each be paid at a rate not to exceed the rate of basic pay for level V of the Executive Schedule.

(2) The Board is authorized to appoint and fix the compensation of not more than 100 officers and employees (or the full-time equivalent thereof), and to prescribe their functions and duties.

(3) The Board may obtain the services of experts and consultants in accordance with the provisions of Section 3109 of Title 5 of the United States Code.

(d) Functions of the Board.

(1) The Board shall:

(A) promote the adoption and implementation throughout the United States of protections for personal privacy and of principles of Fair Information Practices, including the principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability;

(B) develop model guidelines, regulations, and routine uses for use by federal agencies in implementing the provisions of Section 552a of Title 5 of the United States Code;

(C) develop guidelines for use by federal, state, and local agencies in implementation the provisions of Section 7 of the Privacy Act, Public Law 93-579;

(D) publish on a regular basis on the Internet and, as appropriate:

(i) a guide to the Privacy Act of 1974 (5 U.S.C. § 552a) for use by record managers;

(ii) a guide to the Privacy Act of 1974 (5 U.S.C. § 552a), the Freedom of Information Act (5 U.S.C. § 552), and other laws relating to privacy of federal agency records, for use by record subjects;

(iii) a guide to federal, state, and other relevant privacy laws for use by records subjects and by record managers; and

(iv) a compilation of agency system of record notices, including an index and other finding aids.

(E)(i) not later than two years after its first meeting, make detailed recommendations to the Congress for amending the Privacy Act of 1974, for improving coordination between the Privacy Act of 1974 and the Freedom of Information Act; and

(ii) from time to time, make recommendations to the Congress and to the states for passage of or amendments to laws affecting privacy.

(2) The Board may:

(A) issue advisory opinions with respect to Section 552a of Title 5 of the United States Code, at the request of a federal agency, a data integrity board of an agency, a court, the Congress, or any person;

(B) investigate compliance with Section 552a of Title 5 of the United States Code, and report on any violation of any provision thereof (or of any regulation promulgated under the section) to an agency, the President, the Attorney General, or to the Congress;

(C) file comments with the Office of Management and Budget and with any agency on any proposal (i) to amend Section 552a of Title 5 of the United States Code, or any regulation promulgated under the section; (ii) to create or modify a system of records; (iii) to establish or change an exemption for a system of records; or (iv) to establish or alter routine uses of a system of records;

(D) request an agency to stay (i) the establishment or revision of a system of records, (ii) a routine use, (iii) an exemption, or (iv) a regulation promulgated under Section 552a of Title 5 of the United States Code;

(E) review federal, state, and local laws, executive orders, regulations, directives, and judicial decisions and report on the extent to which they are consistent with privacy rights and standards and with fair information practices;

(F) at the request of a state or local government or federal agency, provide assistance on matters relating to privacy;

(G) comment on the implications for privacy of proposed federal, state, or local statutes, regulations, or procedures;

(H) propose legislation on privacy;

(I) accept and investigate complaints about violations of privacy rights and interests;

(J) participate in any formal or informal federal administrative proceeding or process where, in the judgment of the Board, the action being considered would have a material effect on privacy, either as a result of direct government action or as a result of government regulation of others;

(K) petition a federal agency to take action on matter affecting privacy rights and interests;

(L) comment on any action or proposal of any federal, state, or local action, activity, or plan that affects privacy rights and interests; and

(M) comment on any action, proposal, or legislation of any foreign country or international organization that affects privacy rights and interests;

(3) In addition, the Board may:

(A) conduct, assist, or support research, studies, public opinion polls, and investigations on the collection, maintenance, use, or dissemination of personal information; the implications for privacy rights and interests of computer, network, communications, surveillance, and other technologies; and any other matter relating to privacy rights and interests;

(B) comment on or assist in the development or implementation of policies designed to provide for the protection of personal information maintained by private sector record keepers, including for profit and non profit organizations;

(C) assist United States companies and organizations doing business abroad to respond to foreign privacy laws and agencies;

(D) assist in the coordination of United States privacy laws, policies, and practices with the data protection laws, policies, and practices of foreign countries;

(E) accept and investigate inquiries and complaints from foreign governments with respect to privacy rights and interests;

(F) cooperate and consult with privacy agencies of foreign government; and

(G) sponsor and support conferences and meetings on privacy rights and interests.

(e) Confidentiality of Information.

(1) Each department, agency, and instrumentality of the executive branch of the Government, including each independent agency, shall furnish to the Board, upon request made by the Chairman, any data, reports, and other information as the Board deems necessary to carry out its functions under this Act.

(2) In carrying out its functions and exercising its powers under this Act, the Board may accept from any federal agency or other person any identifiable personal data if the data is necessary to carry out its powers and functions. In any case in which the Board accepts any information, it shall provide appropriate safeguards to insure that the confidentiality of the information is maintained and that upon completion of the purpose for which the information is required, the information is destroyed or returned to the agency or person from which it is obtained, as appropriate.

(3) The Board shall maintain the same level of confidentiality for a record made available under this section as is required of the head of the agency from which it is obtained. Officers and employees of the Board are subject to the same statutory penalties for unauthorized disclosure or use as officers or employees of the agency from which the information is obtained.

(f) Powers of the Board.

(1)(A) The Board may, in carrying out its functions under this Act, conduct inspections, sit and act at times and places, hold hearings, take testimony, require by subpoena the attendance of witnesses and the production of books, records, papers, correspondence, and documents, administer oaths, have printing and binding done, and make expenditures as the Board deems advisable. A subpoena shall be issued only upon an affirmative vote of a majority of all members of the Board. Subpoenas shall be issued under the signature of the Chairman or any member of the Board designated by the Board and shall be served by any person designated by the Chairman or any designated member. Any member of the Board may administer oaths or affirmations to witnesses appearing before the Board.

(B) In case of disobedience to a subpoena issued under subparagraph (A) of this subsection, the Board may invoke the aid of any district court of the United States in requiring compliance with the subpoena. Any district court of the United States within the jurisdiction where the person is found or transacts business may, in case of contumacy or refusal to obey a subpoena issued by the Board, issue an order requiring the person to appear and testify, to produce books, record, papers, correspondence, and documents. Any failure to obey the order of the court shall be punished by the court as a contempt thereof.

(C) Appearances by the Board under this Act shall be in its own name. The Board shall be represented by attorneys designated by it.

(2) The Board may delegate any of its functions to officers and employees of the Board as the Board may designate and may

authorize successive redelegations of the functions as it may deem desirable.

(3) In order to carry out the provisions of this Act, the Board may:

(A) adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

(B) enter into contracts or other arrangements with any state or local government, any agency or department of the United States, or with any person, firm, association, or corporation, and the contract, other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to Section 3709 of the Revised Statutes (41 U.S.C. § 5)

(C) make advance, progress, and other payments as the Board considers necessary under this Act without regard to the provisions of 31 U.S.C. §§ 3324(a), (b);

(D) establish advisory committees in accordance with the Federal Advisory Committee Act;

(E) accept unconditional gifts or donations of services, money, or property, real, personal, or mixed, tangible or intangible;

(F) use, with their consent, the services, equipment, personnel, and facilities of federal and other agencies with or without reimbursement, and on a similar basis cooperate with other public and private agencies and instrumentalities in the use of services, equipment, and facilities. Each department and agency of the federal government shall cooperate fully with the Board in making its services, equipment, personnel, and facilities available to the Board; and

(G) take any other action as may be necessary to carry out the provisions of this Act.

(g) Reports and Information.

(1) The Board shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this Act.

(2) The Board shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public, organizations that maintain personal information, or others of privacy rights, interests, and responsibilities.

Section 3. Conforming Amendments

(a) Conforming Amendment to the Privacy Act of 1974.— Section 552a of Title 5 of the United States Code, is amended:

(1) by striking "or" at the end of subsection (b)(11), by striking the period at the end of subsection (b)(12) and inserting in lieu thereof: "; or", and by inserting after the subsection the following:

"(13) to the Privacy Protection Board."

(2) by inserting "the Privacy Protection Board," after "of the Senate," in subsection (r).

(b) Conforming Amendment to Executive Schedule.—Section 5314 of Title 5 of the United States Code, is amended by adding at the end thereof the following new paragraph:

"Members, Privacy Protection Board (5)."

Section 4. Authorization of Appropriations

There are authorized to be appropriated such sums as may be necessary to carry out this Act.