FRAGMENTED, INCOMPLETE, AND DISCONTINUOUS: THE FAILURE OF FEDERAL PRIVACY REGULATORY PROPOSALS AND INSTITUTIONS

by ROBERT M. GELLMAN*

TABLE OF CONTENTS

* Chief Counsel, Subcommittee on Information, Justice, Transportation, and Agriculture, House Committee on Government Operations. B.A. 1970, University of Pennsylvania. J.D. 1973, Yale Law School.

The author thanks David Flaherty, Jane Bortnick and Paul Schwartz for their criticism of earlier drafts.

The views expressed in this article are solely those of the author and do not represent the views of the House Committee on Government Operations or its Subcommittees.

I. INTRODUCTION

The protection of individual privacy[1] continues to grow as an important public policy issue around the world.[2] In most western, industrialized countries, data protection laws have been enacted in the past twenty years,[3] and formal data protection authorities have been established in many.[4] Several international organizations have adopted[5] or are in the process of adopting[6] policies on data protection.

---

1. "Data protection," "privacy," "information privacy," and "records privacy" have all been used interchangeably to refer to laws and policies that regulate information about individuals. These terms encompass record keeping practices for personal information including access, correction, use, collection, and retention and disclosure to third parties. The term "data protection" appears to be most in favor today.

2. *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES xxii (1989) ("Concern for the protection of personal privacy in the face of the massive surveillance capacities of governments and corporations is a leading issue in all Western industrialized societies."); *see also* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 3 (1992) ("By the end of the 1980s, the protection of personal data had taken on a momentum of its own as a separate and significant issue of public policy.").

3. *See, e.g.*, A.C. NUGTER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC 18 (1990) ("Generally speaking, most Western countries have now implemented data protection laws." (footnote omitted)).

4. For example, Sweden passed the Data Act of 1973 establishing a Data Inspection Board; West Germany passed the Federal Data Protection Act in 1977 establishing a Data Protection Commissioner; France passed the Law on Informatics, Data Banks, and Freedoms in 1978 establishing a National Commission on Informatics and Freedoms; Canada passed the Privacy Act of 1982 establishing an Office of the Privacy Commissioner; Great Britain passed the Data Protection Act of 1984 establishing a Data Protection Registrar; Australia passed the Privacy Act 1988 establishing a Privacy Commissioner. The first data protection law was passed in 1970 in the German State of Hesse.

For a recent list of the status of data protection laws in countries belonging to the Organization of Economic Co-operation and Development, see BENNETT, *supra* note 2, at 57, Table 1. There are seventeen countries, including the United States, on the list. Legislation was being considered or studied in six other countries. For a summary of data protection laws and proposals in thirty-one countries, see 17 *Privacy Laws & Business* 2-7 (July 1991). *See also Status of Data Protection/Privacy Legislation*, 16 TRANSNAT'L DATA AND COMM. REP. 33 (Jan./Feb. 1993).

5. Organization for Economic Co-operation and Development, *Recommendations of Council Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1981 I.L.M. 422, O.E.C.D. Doc. No. C(80)58 final; Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 1981 I.L.M. 377, Euro. T.S. No. 108 (Jan. 28, 1981). Both of these documents are reprinted in *Data Protection, Computers, and Changing Information Practices, Hearing before the Government Information, Justice, and Agriculture Subcommittee, House Committee on Government Operations*, 101st Cong., 2d Sess. (1990) [hereinafter *1990 House Data Protection Hearing*]; *see also* United Nations, *Guidelines Concerning Personal Data Files*, G.A. Res. 45/95, U.N. Doc. A/RES/45/95 (1990). For a brief discussion of the U.S. response to the adoption of the OECD guidelines, see *infra* notes 179-192 and accompanying text.

6. The European Community is preparing a Council Directive concerning the protection of individuals in relation to the processing of personal data. A first draft of the direc-

These legislative and institutional changes are a response to worldwide concerns about the loss of privacy as a consequence of the computerization of information systems containing personal information. Policy makers in many countries have reacted to fears and uncertainties about the implications of the widespread, long-term collection, maintenance, use, and interconnection of databases containing records about credit and finances, health, criminal history, insurance, employment, social security, tax, and consumption. Some of these records are maintained by governments and, increasingly, more records are maintained by private sector companies. Spiros Simitis, the first of the modern data protection officials, has described the processing of personal data as "a challenge to human rights and the very structure of a democratic society."[7]

Through the early 1970s, the United States was a leader in the development of privacy policy. Professor David Flaherty, a Canadian data protection scholar, has written that the United States invented the concept of a legal right to privacy.[8] A 1976 book by a British privacy expert asserted that the United States was the country with the most highly-developed law of privacy.[9] A recent study[10] (by a Dutch scholar) of privacy statutes of several European countries begins an introductory review of the concept of privacy with a discussion of the famous 1890 article by Brandeis and Warren[11] and of American Professor Alan Westin's seminal 1967 book.[12] The 1972 report of a U.S. Department of Health, Education & Welfare Advisory Committee was one of the earliest and most internationally influential government privacy studies.[13]

---

tive was issued in September 1990. A second draft was issued in October 1992. *See* Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, EUR. PARL. DOC. (COM 422 final-SYN 287) 1 (1992) [hereinafter 1992 Draft EC Data Protection Directive].

7. Spiros Simitis, *New Trends in National and International Data Protection Law*, RECENT DEVELOPMENTS IN DATA PRIVACY LAW 17 (J. Dumortier ed. 1992); *see also* FLAHERTY, *supra* note 2, at 1 ("[I]ndividuals in the Western world are increasingly subject to surveillance through the use of data bases in the public and private sectors, and . . . these developments have negative implications for the quality of life in our societies and for the protection of human rights.").

8. FLAHERTY, *supra* note 2, at 306.

9. PAUL SIEGHART, PRIVACY AND COMPUTERS 11 (1976).

10. NUGTER, *supra* note 3, at 16-17.

11. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 5 HARV. L. REV. 4 (1890). It is difficult, in fact, to find any serious written work on privacy that fails to cite this article.

12. ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

13. U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS viii (1973) [hereinafter HEW REPORT]; *see also infra* notes 58-75 and accompanying text.

The U.S. Privacy Act of 1974[14] was one of the first national data protection laws.[15]

Privacy activities outside the United States accelerated beginning in the mid-1970s In 1977 and 1978 alone, data protection laws were enacted in six countries, including West Germany, France, and Canada.[16] The establishment of formal data protection authorities in other countries institutionalized the government role in privacy matters and fueled the movement toward international cooperation and coordination.[17]

While international interest in data protection accelerated during the 1970s, United States interest peaked at the end of the decade. The election of Ronald Reagan as President marked the end of any significant privacy policy initiatives from the executive branch.[18] This resulted in a divergence between the United States and other western industrialized countries on privacy matters. Although policies and practices in the United States remained relatively static, other nations worked cooperatively and moved in new directions. Colin Bennett observed in his recent study of data protection and public policy in Europe and the United States that *"[w]ith the exception of the United States*, however, in each country there was an immediate awareness of overseas legislation and a keen desire to learn from the experience of others."[19]

The failure of the United States to establish a permanent data protection authority represents the single most important difference in approach to data protection between the United States and most other industrialized countries.[20] In his book, Professor Flaherty was direct in describing the effect: "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."[21] Professor Spiros Simitis,

---

14. Privacy Act of 1974, Pub. L. No. 93-579, § 5(a)(1), 88 Stat. 1896, 1907 (1974).

15. *See* BENNETT, supra note 2, at 57, Table 1. The Swedish Data Act, passed in 1973, is the only earlier law cited.

16. *Id.*

17. A principal purpose of the European Community draft data protection directive is to harmonize national laws and to establish a community standard of privacy protection. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 238 (1992); *see also* EIGHTH REPORT OF THE DATA PROTECTION REGISTRAR (UNITED KINGDOM) 2 (1992) ("The draft [European Community data protection directive] has stimulated greater collaboration between the Data Commissioners of the EC nations.); *supra* notes 5-6 and accompanying text.

18. *See infra* text accompanying notes 176-178.

19. BENNETT, *supra* note 2, at 125 (emphasis supplied).

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

21. FLAHERTY, *supra* note 2, at 305.

Germany's first data protection official, has described the American approach to data protection as "an obviously erratic regulation full of contradictions, characterized by a fortuitous and totally unbalanced choice of its subjects."[22]

It is not the purpose here to make a case for establishing a federal data protection agency in the United States. Others have put forward reasons why such an agency is needed.[23] Proposals to establish a data protection authority in the United States have been regularly offered over twenty years, and continue to be put forward. The failure of the United States to have a data protection authority remains a significant difference with other countries as well as a continuing legislative issue. For example, the European Community proposed directive on data protection requires each member state to designate an independent public authority to supervise the protection of personal data.[24] As a result, the history of federal privacy regulatory actions and proposals continues to be relevant.

This article reviews the legislative and administrative record behind the failure of the United States to create a data protection authority. This task will be accomplished by examining legislative proposals and administrative recommendations for a data protection authority and by evaluating the activities of executive agencies that might be characterized as carrying out functions relating to privacy policy making or international data protection coordination. This history will suggest that (1) the notion of a data protection authority in the United States has been a constant, albeit low-level, issue for twenty years; and (2) administrative privacy activities at the federal level have been fragmented, incomplete, and discontinuous. These activities have never been equivalent to or a substitute for a formal data protection authority.

II. LEGISLATIVE ATTEMPTS TO CREATE A PRIVACY AGENCY

Proposals to establish a permanent federal privacy agency in the United States date back to 1974 when Senator Sam Ervin introduced legislation to establish a five-member Federal Privacy Board. Ervin's Privacy Board would have had privacy responsibilities for records of

22. SIMITIS, *supra* note 7, at 22.

23. *See, e.g.*, FLAHERTY, *supra* note 2, at 382 ("Unless a federal data protection agency is created in the United States, the federal system for articulating privacy interests in a systematic fashion is woefully inadequate."); Schwartz, *supra* note 20, at 1379-84; REIDENBERG, *supra* note 17, at 236-42; M. Rotenberg, *In Support of a Data Protection Board in the United States*, 8 GOV'T INFO. Q. 79 (1991); P. Regan, The Globalization of Privacy: Implications of Recent Changes in Europe, Paper Delivered Before the American Sociological Association (1992); *see also* 137 Cong. Rec. H755 (daily ed. Jan. 29, 1991) (statement of Rep. Wise) (Introduction of the Data Protection Act of 1991, H.R. 685).

24. 1992 Draft EC Data Protection Directive, Art. 30.

federal, state, and local governments as well as the private sector.[25] This legislation, which eventually became the Privacy Act of 1974,[26] also proposed substantive safeguards to personal privacy during the collection, maintenance, and dissemination of information.

As approved by the Senate Committee on Government Operations in 1974, the direct authority of the renamed Privacy Protection Commission would have extended primarily to federal government records. According to the Committee's legislative report, one of the principal reasons for the Commission was "to fill the present vacuum in the administrative process for overseeing establishment of governmental data banks and personal information systems and examining invasions of individual privacy."[27]

As approved by the Committee, the Commission's authority over state governments and the private sector would have been limited. The Commission would have been empowered mostly to study privacy matters affecting state and local governments and the private sector. The Commission would also have been able to "assist agencies and industries in the voluntary development of fair information practices."[28]

The Senate Committee report offered this justification for a privacy protection unit:

> [T]here is an urgent need for a staff of experts somewhere in government which is sensitive both to the privacy interests of citizens and the informational needs of government and which can furnish expert assistance to both the legislative and executive branches. In recent years, controversies over privacy and government data banks have arisen after executive branch decisions have been made. The Commission will serve the important purposes of raising and resolving privacy questions before government plans are put in operation. Agencies need help to incorporate newly-refined concepts of individual liberty into their current procedures without unnecessary disruption and confusion. Congress and the President need help in identifying those areas in which privacy safeguards are most urgently needed and in drafting legislation specifically tailored to those problem areas.[29]

The Senate Committee concluded "with some reluctance" to propose an independent commission. Other locations considered for the

---

25. S. 3418, 93rd Cong., 2d Sess. § 522(a) (1974). Many of the congressional documents from the 93rd Congress were collected and reprinted in SENATE COMM. ON GOV'T. OPERATIONS AND HOUSE COMM. ON GOV'T. OPERATIONS, 94th Cong., 2d Sess. LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S. 3418 (PUBLIC LAW 93-579), (1976).

26. Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified at 5 U.S.C. § 552a & note).

27. SENATE COMM. ON GOV'T. OPERATIONS, PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING, USE AND DISCLOSURE OF INFORMATION, S. Rep. No. 1183, 93rd Cong., 1st Sess. 34 (1974).

28. *Id.* at 23.

29. *Id.* at 24-25.

privacy function but rejected were the General Accounting Office and the Office of Management and Budget.[30]

S. 3418 passed the Senate in November 1974, with the Privacy Protection Commission proposal approved by the Committee intact. The vote was 74-9.[31] An amendment offered by Senator Muskie — and accepted by voice vote — enlarged the mandate of the Commission by authorizing it to prepare model privacy legislation for state and local governments.[32]

A companion bill was reported by the House Committee on Government Operations in 1974 but without a provision establishing a privacy agency.[33] Additional views filed by ten Committee members discussed the failure to create an administrative body for privacy:

> Unlike the Senate bill, H.R. 16373 contains no provision for the establishment of an administrative body to oversee the implementation of this legislation. We recognize the fact that some of our colleagues feel it is wiser to wait and see how Federal agencies respond to privacy legislation before establishing any oversight mechanism. No one, however, wants to repeat the experience of the Freedom of Information Act in holding out rights to individuals but providing them only with the costly and cumbersome mechanism of a judicial remedy. Therefore, we would amend the bill to provide for the establishment of an administrative body to mediate conflicts between agencies and individuals, to investigate complaints, hold hearings, and make findings of fact.
>
> We would be more than naive if we failed to recognize that individual Federal agencies cannot be expected to take an aggressive role in enforcing privacy legislation. Enforcement of the provisions of this bill will be secondary to each agency's legislative mandate and will, of necessity, cause additional expense and administrative inconvenience. Only by providing a separate administrative agency with authority for implementing this legislation and coordinating the privacy programs of the various federal agencies can be we assured of uniform, effective enforcement of the rights guaranteed by this bill.[34]

When H.R. 16373 was considered on the House floor, an amendment was offered by Representative Gilbert Gude to establish a Federal Privacy Commission as an independent agency in the executive branch.[35] The powers proposed for the Commission were "more limited than those provided in other earlier proposals" and were confined to

30. *Id.* at 26.

31. 120 Cong. Rec. 36,917 (1974).

32. *Id.* at 36,897.

33. HOUSE COMM. ON GOV'T. OPERATIONS, PRIVACY ACT OF 1974, H.R. REP. No. 1416, 93d Cong. 2d Sess. 7 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916, 6938.

34. *Id.* at 38-9.

35. 120 Cong. Rec. 36,962 (1974).

serving "as a focus of attention for information and privacy issues" and to being "a watchdog over agencies which are responsible for implementing the provisions of the act."[36] Representative William Moorhead, Chairman of the Government Operations Committee and sponsor of the bill, opposed the Gude amendment. He stated during debate that "if . . . the courts do not do the excellent job they have done under the Freedom of Information Act, then we in Congress can always in the future create a privacy board."[37] The Gude amendment was defeated without a record vote by the House.[38] H.R. 16,373 passed by a vote of 353-1.

The House and Senate bills were reconciled without a formal conference at the conclusion of the 93rd Congress. The opposition of President Ford to the establishment of a separate privacy board or commission was a significant factor in the decision to compromise on the privacy board.[39] The result was a decision to establish a temporary study commission.[40] An analysis of the compromise reprinted in the Congressional Record by Rep. Moorhead included this discussion:

> Under the Senate bill the Privacy Protection Commission was directed to develop model guidelines and conduct certain oversight of the implementation of this Act to Federal agencies. Since the compromise amendment would change the scope of authority of the commission, it was felt there remained a need for an agency within the government to develop guidelines and regulations for agencies to use in complementing the provisions of the Act and to provide continuing assistance in and oversight of the implementation of the provisions of this Act by the agencies.
>
> This function has been assigned to the Office of Management and Budget.[41]

The Privacy Act of 1974 became law on December 31, 1975. The substantive provisions of the Act became effective on September 27,

---

36. *Id.* at 36,964 (statement of Rep. Gilbert Gude).

37. *Id.*

38. *Id.* at 36,965.

39. *See* FLAHERTY, *supra* note 2, at 311-312.

40. 120 Cong. Rec. 40,409 (1974) (statement of Sen. Ervin). The temporary study commission was the Privacy Protection Study Commission. See *infra* text accompanying notes 101-116 for a discussion of the work of the PPSC.

41. 120 Cong. Rec. at 40,883 (1974). James H. Davidson, former Counsel to the Senate Government Operations Subcommittee on Intergovernmental Relations, testified in 1983 that the selection of OMB "was a compromise forced by the reluctance of the Congress to establish an agency with ongoing responsibility for implementing the act and an unwillingness to give the job to the Justice Department after examining its dismal record of implementing the Freedom of Information Act." *Oversight of the Privacy Act of 1974: Hearings Before a Subcomm. of the House Comm. on Gov't. Operations*, 98th Cong., 1st Sess. 43 (1983) (statement of James H. Davidson, Counsel to the Senate Government Operations Subcommittee on Intergovernmental Relations).

1975.[42]

The consideration of the privacy board issue during the debate on this bill represented the legislative high-water mark of the privacy agency concept.[43] Legislation to create a privacy agency has been introduced repeatedly since 1977, but no action was taken. In the 95th Congress, Representative Ed Koch — a member of the Privacy Protection Study Commission[44] — introduced a bill to establish a Federal Information and Privacy Board and to implement the other recommendations of the Commission.[45] Representative Silvio Conte introduced the Comprehensive Right to Privacy Act which included the establishment of a Federal Privacy Board.[46]

In the 98th Congress, Representative Glenn English, then chairman of the Subcommittee on Government Information, Justice, and Agriculture, introduced legislation to establish a Privacy Protection Commission.[47] In the 99th and 100th Congress, Representative English reintroduced similar bills to establish a Data Protection Board.[48] A modified proposal for a Data Protection Board was introduced by Representative Bob Wise in the 101st[49] and 102nd Congress.[50]

In 1992, the House Committee on Government Operations adopted a report recommending the establishment of a temporary advisory commission to address a privacy issue.[51] This proposed commission was to consider the ethical, legal, and social implications of the Human Genome Project. Many of the Committee's concerns related to the prospect

---

42. Privacy Act of 1974, Pub. L. No. 93-579, § 8, 88 Stat. 1907 (1974).

43. In his book on data protection, Professor David Flaherty called the absence of a federal privacy protection commission "largely a matter of accident or at least of an historic compromise." FLAHERTY, *supra* note 2, at 310. Professor Flaherty's book also contains a detailed account of Senator Ervin's privacy commission proposal. *Id.* at 310-14.

44. See *infra* text accompanying notes 101-116 for a discussion of the report of the Commission.

45. H.R. 9986, 95th Cong., 1st Sess. (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., 1st Sess. (1979).

46. H.R. 285, 95th Cong., 1st Sess. (1977).

47. H.R. 3743, 98th Cong., 2d Sess. (1983).

48. H.R. 1721, 99th Cong., 1st Sess. (1985); H.R. 638, 100th Cong., 2d Sess. (1987).

49. H.R. 3669, 101st Cong., 1st Sess. (1989). A hearing that considered, among other issues, H.R. 3669 was held in 1990. *1990 House Data Protection Hearings.*

50. H.R. 685, 102d Cong., 1st Sess. (1991). The bill was discussed at data protection oversight hearings in 1991. *See Domestic and International Data Protection Issues: Hearings before the Gov't. Information, Justice, and Agriculture Subcomm. of the House Comm. on Gov't. Operations*, 101st Cong., 2d Sess. (1990) [hereinafter *1991 House Data Protection Hearings*].

51. HOUSE COMM. ON GOV'T. OPEARATIONS, DESIGNING GENETIC INFORMATION POLICY: THE NEED FOR AN INDEPENDENT POLICY REVIEW OF THE ETHICAL, LEGAL, AND SOCIAL IMPLICATIONS OF THE HUMAN GENOME PROJECT, H.R. REP. NO. 478, 102d Cong., 2d Sess. (1992) [hereinafter 1992 HOUSE GENETIC INFORMATION REPORT].

of the availability of identifiable genetic information about individuals. The report discusses the need to establish ground rules for the collection, maintenance, disclosure, and use of genetic information.[52] These are traditional privacy policy concerns.

The Committee recommended that the two cabinet departments[53] sponsoring the Human Genome Project establish the advisory commission administratively. If a satisfactory commission is not established "in a timely fashion," then the Committee recommended that legislation be enacted.[54]

This proposed advisory commission shares only some of the characteristics of proposed data protection agencies. The two principal differences are the temporary nature of the genetic advisory commission and the narrow subject matter jurisdiction. Although the proposal cannot be read to suggest that there is congressional support for a permanent privacy entity, it does illustrate that there is continuing bipartisan[55] support in Congress for studies of privacy matters.[56]

III. HISTORY OF TEMPORARY FEDERAL PRIVACY STUDY ORGANIZATIONS

Over the past twenty years, general privacy policy issues at the federal level have been addressed intermittently through a variety of agencies, commissions, and study committees. Some of these efforts centered largely on privacy policy issues; others considered privacy as a significant part of broader policy initiatives. One common characteristic of these efforts is that they were temporary. Another common characteristic is that three of the four study organizations recognized the need for a permanent entity in the federal government with responsibility for privacy issues.

A short description of significant privacy policy study efforts follows. However, no attempt has been made to discuss every report or entity that ever touched upon a privacy issue.[57] The focus here is on

---

52. *Id.* at 13.

53. Department of Health and Human Services and Department of Energy.

54. 1992 HOUSE GENETIC INFORMATION REPORT, at 5.

55. The Government Operations Committee report was adopted without dissent. The Committee's recommendations were supported by the House Appropriations Committee. *See* H.R. REP. NO. 708, 102d Cong., 2d Sess. 87 (1992) *available in* WESTLAW, Legislative History Library, 1992 WL 193621.

56. In 1978, Congress created the President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research. 42 U.S.C. § 300v (1988). This temporary Commission's tasks include privacy of human subject research and confidentiality of records. This was one of five major tasks. The Commission's work on confidentiality of medical records is discussed in *Summing Up*, a March 1983 report by the Commission. *See also* 1992 HOUSE GENETIC INFORMATION REPORT, *supra* note 51, at 39-41.

57. Reports on privacy matters not discussed in this article include: DOMESTIC COUN-

reviews that dealt with privacy implications of federal or private sector record keeping practices rather than on general studies that touched on privacy as a secondary concern or in a narrow subject-area context.

A. SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (DEPARTMENT OF HEALTH, EDUCATION, & WELFARE, 1972-1973)

The Advisory Committee on Automated Personal Data Systems was established in 1972 by Health, Education, and Welfare Secretary Elliot Richardson in response to the growing public and private use of automated data systems containing information about individuals. Richardson was concerned that automated personal data systems presented a serious potential for harmful consequences, including infringement of basic liberties.[58]

The Advisory Committee was asked to analyze and make recommendations about the harmful consequences from using automated personal data systems; safeguards that may protect against those consequences; measures that might afford redress; and policy and practices relating to the issuance and use of Social Security numbers.[59] The Committee's report was issued in July 1973.

Willis H. Ware from the RAND Corporation served as Chairman of the Committee. Other members of the Committee came from a variety of backgrounds, including state legislatures and governments, academia, and the private sector. The scope of the Committee's work included both the public and private sectors, and the recommendations addressed both public and private records. However, it appears that the Committee was principally concerned with government records and did not focus much attention on the effect of its recommendations on private record keepers.[60]

CIL COMMITTEE ON THE RIGHT OF PRIVACY AND THE COUNCIL OF STATE GOVERNMENTS, PRIVACY, A PUBLIC CONCERN: A RESOURCE DOCUMENT (1975); WESTIN, COMPUTERS, HEALTH RECORDS, AND CITIZEN RIGHTS (1976) (National Bureau of Standards Monograph 157); REPORT OF THE NATIONAL COMMISSION FOR REVIEW OF FEDERAL AND STATE WIRETAPPING LAWS (1976) (established under title III of the Omnibus Crime and Safe Streets Act); NATIONAL BUREAU OF STANDARDS, ACCESSING INDIVIDUAL RECORDS FROM PERSONAL DATA FILES USING NON-UNIQUE IDENTIFIERS (1977) (Special Publication 500-2); REPORT OF THE PRESIDENT'S COMMISSION FOR THE STUDY OF ETHICAL PROBLEMS IN MEDICINE AND BIOMEDICAL AND BEHAVIORAL RESEARCH (1983); OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985); OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC RECORD SYSTEMS AND INDIVIDUAL PRIVACY (1986).

58. HEW REPORT, *supra* note 13.

59. *Id.* at ix.

60. The Advisory Committee recommended a few changes to the Fair Credit Reporting Act. *Id.* at 66-71. No action was taken on these recommendations. The Committee also reviewed the mailing list industry, but concluded that if the "control of mailing list is

The central contribution of the HEW Advisory Committee was the development of a code of fair information practices[61] for automated personal data systems.[62] The fair information practice code included these elements:

- The code should define "fair information practice" as adherence to specified safeguard requirements.
- The code should prohibit violation of any safeguard requirement as an "unfair information practice".
- The code should provide that an unfair information practice be subject to both civil and criminal penalties.
- The code should provide for injunctions to prevent violations of any safeguard requirement.
- The code should give individuals the right to bring suit to recover actual, liquidated, and punitive damages as well as attorney fees and litigation costs.[63]

The key part of the proposed fair information practice code was the safeguard requirements. The safeguards fell in three broad categories:

First, the general requirements covered transfer of data; maintenance of administrative and security controls; and standards for data accuracy, completeness, timeliness, and pertinence.[64]

Second, the public notice requirements were intended to prevent the maintenance of secret records by mandating annual publication of a complete description of each system of records. The Committee also

---

to be undertaken by law, it should be done by legislation that is directed specifically to that purpose." *Id.* at 73. The report includes no detailed discussion of records maintained by other major private sector record keepers, such as banks, insurance companies, and employers.

61. The same basic principles that formed the HEW Committee's code of fair information practices were also put forward at the same time in Great Britain in the *Report of the Committee on Privacy* (1972), known more popularly as the "Younger Committee." According to one privacy scholar, it is impossible to judge which committee came first or how the work of one committee may have influenced the other. *See* BENNETT, *supra* note 2, at 99.

62. The Advisory Committee made a major distinction between the use of personal information for administrative purposes and for statistical and research purposes. The report also singles out systems of records that maintain personal information solely for statistical or research use. The Committee's interest in these uses of personal information is not surprising given HEW's statistical and research functions. In general, the Committee recommended that statistical and research records be maintained in accordance with the proposed code of fair information practices. It also recommended additional notices to record subjects, segregation of statistical and research records from administrative use, and statutory protection against compulsory disclosure. HEW REPORT, *supra* note 13, at 78-106.

Based in part on the recommendations of the Advisory Committee, the Privacy Act of 1974 included a few special provisions for statistical records. *See* 5 U.S.C. § 552a(a)(6), (b)(5), (k)(4) (1988). There is no general privacy law for statistical records.

63. HEW REPORT, *supra* note 13, at 50.

64. *Id.* at 53-57.

recommended advance publication for new systems with an opportunity for public comment.[65]

Third, the safeguards included specific protections for the rights of individual data subjects. These included providing notice of legal rights to individuals asked to provide data; right of access to records; opportunity to contest the accuracy of data; and notice of uses of the data and the identity of recipients.[66]

Privacy scholar David Flaherty observed that this fair information practices code "greatly influenced the Privacy Act and subsequent data protection legislation in other countries."[67] Even a cursory review of the Advisory Committee's report and the Privacy Act of 1974 shows a striking similarity in content and organization.[68] Many of the Committee's proposals were enacted almost verbatim in the Privacy Act of 1974.[69]

The Advisory Committee considered a variety of mechanisms for protecting against the adverse effects of automated personal data systems. The notion of a public ombudsman to monitor automated personal data systems, to identify problems, and to investigate complaints was rejected because it was not well understood or widely accepted in America.[70]

The Committee also considered a "centralized, independent Federal agency to regulate the use of all automated personal data systems." This was identified in its report as the "strongest" mechanism for providing privacy safeguards. Such an agency might have authority to register or license the operations of automated personal data systems. This suggestion was rejected by the Advisory Committee because it lacked the necessary public support and because regulation or licensing would

---

65. *Id.* at 57-58.

66. *Id.* at 59-64.

67. FLAHERTY, *supra* note 2, at 310. Colin Bennett described the Committee's report as "surprisingly coherent and influential." BENNETT, *supra* note 2, at 70.

68. Both the House and Senate Committees that reported the legislation that became the Privacy Act of 1974 cited the HEW Advisory Committee's report. *See* SENATE COMM. ON GOV'T. OPERATIONS, PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING, USE AND DISCLOSURE OF INFORMATION, S. REP. NO. 1183, 93rd Cong., 1st Sess. 161-163 (1974) (report to accompany S. 3418); HOUSE COMM. ON GOV'T. OPERATIONS, PRIVACY ACT OF 1974, H.R. REP. NO. 1416, 93rd Cong., 2d Sess. 7 (1974) (report to accompany H.R. 16,373) *reprinted in* 1974 U.S.C.C.A.N. 6916.

69. The Committee's contributions extended beyond its report to the Secretary. The Committee's Chairman, Willis Ware, was appointed in 1975 to serve as Vice Chairman of the Privacy Protection Study Commission established by the Privacy Act of 1974. Carole Parsons who served as Associate Executive Director of the Committee was Executive Director of the Privacy Protection Study Commission.

70. HEW REPORT, *supra* note 13, at 42.

be complicated and costly.[71] The Committee's choice of enforcement of privacy rights through individual court action was chosen in part to "create no obstacles to further development, adaptation, and application of a technology that, we all agree, has brought a variety of benefits to a wide range of people and institutions in modern society."[72]

The report does not discuss any of the alternatives that fall between an ombudsman and a regulatory body.[73] However, the Committee did see the need for an official in the Office of the Secretary of HEW to provide guidance and assistance within the Department. This official was to be a "combination advisor, monitor, and catalyst" and was to assure that personal data systems are operated in accordance with recommended privacy safeguards.[74] Otherwise, the Committee generally concluded that institutions should be held legally responsible for unfair information practices and should be liable to damages through legal action.[75]

B. DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY (WHITE HOUSE 1974-77)

On February 23, 1974, President Richard Nixon announced the establishment of a Domestic Council Committee on the Right of Privacy.[76] The President's action followed his 1974 State of the Union

---

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

The Committee's conclusions regarding licensing were prophetic. Professor Flaherty found that the licensing of information systems "increases paperwork, costs, and bureaucratic burden." He reported that Sweden and Norway revised their laws to reduce these pressures because they could not cope in a meaningful way with the avalanche of paper. FLAHERTY, *supra* note 2, at 395; *see also* BENNETT, *supra* note 2, at 161-165. The British registration system also proved to require a large bureaucracy that used most of the resources of the Data Registrar's Office. *Id.* at 189.

72. HEW REPORT, *supra* note 13, at 43.

73. In a footnote, the Committee indicated that it did not intend "to discourage the development of regulation in specific, limited areas of application of computer-based record-keeping systems," such as where particular institutions or societal functions (e.g., public utilities, common carriers, insurance companies and hospitals) are already subject to regulation. *Id.*, n.12.

74. *Id.* at 142. There are some similarities between later proposals for a non-regulatory data protection authority and the Committee's proposed "combination advisor, monitor, and catalyst." *See, e.g.*, H.R. 685, 102d Cong., 1st Sess. (1991).

75. HEW REPORT, *supra* note 13, at 42-44. The Privacy Act of 1974 largely adopted the model put forward by the HEW Committee for enforcement of privacy rights by individuals through lawsuits. The extent to which this type of enforcement is effective is beyond the scope of this paper. However, Ronald Plesser, General Counsel to the Privacy Protection Study Commission, testified in 1983 that "[t]he Privacy Act, to a large extent, is unenforceable by an individual." *Oversight of the Privacy Act of 1974: Hearings Before a Subcommittee of the House Comm. on Gov't. Operations*, 98th Cong., 1st Sess. 240 (1983).

76. OFFICE OF THE WHITE HOUSE PRESS SECRETARY, FACT SHEET: THE PRESIDENT'S

Address in which he said that "the time has come . . . for a major initiative to define the nature and extent of the basic rights of privacy and to erect new safeguards to ensure that those rights are respected."[77]

The Domestic Council Privacy Committee was chaired initially by Vice President Gerald Ford. Nelson Rockefeller later served as chairman when he became Vice President. Members included six Cabinet Secretaries and the directors of four other federal offices. There were 19 specific areas which the Committee was asked to address including:

- Trafficking in records containing identifiable personal information by third parties in government and private industry;
- Relevance and adequacy of consent to disclose personal information;
- Need for a code of fair record keeping practices for both the public and private sectors;
- Need for new organizations or methods to assure that privacy concerns are reflected and accommodated in government and private programs;
- Lessening the amount of information that is acquired and collected;
- Increasing the individual's ability to find out what information about him is collected and how it is used;
- How can government and private industry adopt meaningful ways to enforce general principles and broad safeguards regarding privacy, and adopt legal, administrative, and voluntary remedies.[78]

The major product of the President's privacy committee was a report entitled *National Information Policy*.[79] The report's focus was much broader than privacy. Information policy was described as "the policies which govern the way information affects our society"[80] and includes "information communications, information technology, information economics, information privacy, information systems, information confidentiality, information science, information networks, and information management."[81]

The Domestic Council Committee found that a key question was "how to structure the policy making process so that the country can begin to develop a national information policy that is comprehensive, sufficiently sensitive to the new technology, and responsive to the

---

ADDRESS ON THE AMERICAN RIGHT OF PRIVACY (February 23, 1974) (Box 84, Gerald R. Ford Vice Presidential Papers, Gerald R. Ford Library) [hereinafter NIXON PRIVACY ADDRESS].

77. President's 1974 State of the Union Address, 25 PUB. PAPERS 47, 52 (Jan. 30, 1974).

78. NIXON PRIVACY ADDRESS, *supra* note 76, at 2-5.

79. DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY, NATIONAL INFORMATION POLICY: REPORT TO THE PRESIDENT OF THE UNITED STATES (1976); *see also* Douglas W. Metz, *Federal Leadership in Privacy Protection*, 61 A.B.A. J. 825 (1975).

80. *Id.* at xi.

81. *Id.* at xii.

implications of the Information Age."[82] Given the breadth of this inquiry, it may not be surprising that the principal recommendations were structural rather than substantive.

The report begins with a statement of the problem, including a discussion of the role of the government in shaping information policy. The report found that the responses of both the Congress and the Executive Branch to information policy problems were ad hoc and piecemeal.[83] Institutional mechanisms which could have helped were "beleaguered by constant proposals for their abolition, by inadequate resources and by limited authority."[84] This conclusion applies across the entire front of information policy issues, including privacy, telecommunications, computer technology, intellectual property rights, and other matters.

Some of the specific privacy areas discussed in the report were standards for the federal collection of personal data, federal use and sharing of personal data, Social Security numbers and universal identifiers, data havens, restrictions on the use and transfer of personal information in the private sector, and the free flow of information across national boundaries.

As a first step toward structuring the policy making process, the Domestic Council Privacy Committee recommended the establishment of a permanent policy organization within the Executive Office of the President to provide coordination and to articulate a rational framework for a national information policy.[85] This was the major recommendation in the report. The new organization would serve as the President's principal advisor on matters of information policy, provide leadership for the executive branch, provide a structural framework for the resolution of competing interests and the balancing of competing values, establish priorities for information policy issues, and provide a focal point for problems.[86]

Among the reasons offered for this recommendation was the need for an organizational structure with high visibility and adequate authority that could prevent information concerns from being compromised and traded away for other concerns at the agency level below the range of public visibility.[87] The Committee also recommended the creation of

82. *Id.* at 183-184.

83. *Id.* at 12, 14.

84. *Id.* at 14.

85. *Id.* at 184.

86. *Id.* at 191-92.

87. *Id.* at 186. The Committee rejected as premature a recommendation for the establishment of a Department of Communications. The Committee also rejected the notion of an independent agency for policy coordination of information and communications issues because it would dilute the authority of the President. *Id.* at 187-88.

an inter-agency council on information policy and an advisory committee for non-governmental people.[88]

C. COMMISSION ON FEDERAL PAPERWORK (1975-1977)

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.[89] Representative Frank Horton (R-NY) was appointed as Chairman of the Commission.

The Commission issued thirty-six separate reports and 770 recommendations on major program areas and government processes.[90] The report,[91] which specifically addressed confidentiality and privacy issues, was prepared in response to a statutory direction for recommendations that would "guarantee appropriate standards of confidentiality for information held by private citizens or the Federal Government, and the release thereof."[92]

The Paperwork Commission's principal confidentiality and privacy findings included:

> • Federal laws treating confidentiality and disclosure of information are inconsistent at best and chaotic at worst.
>
> • Existing federal standards on the confidentiality and disclosure of information collected and maintained by federal agencies or by others administering federally supported programs are imprecise and confusing.
>
> • Compliance machinery for enforcing federal information laws is inadequate. Available sanctions are infrequently used, remedies are not always appropriate . . . and organizational responsibility is fragmented.[93]

The Commission's twelve confidentiality and privacy recommendations were aimed at encouraging the maximum utilization of federal information within a framework guaranteeing appropriate standards of

---

88. *Id.* at 197-198.

89. Pub. L. No. 93-556, 88 Stat. 1789 (1974).

90. *See also Privacy and Confidentiality Report and Final Recommendations of the Commission on Federal Paperwork: Hearing before a Subcomm. of the House Comm. on Government Operations,* 95th Cong., 1st Sess. (1977).

91. COMMISSION ON FEDERAL PAPERWORK, CONFIDENTIALITY AND PRIVACY (1977) [hereinafter PAPERWORK REPORT].

92. Pub. L. No. 93-556, § 3(b)(3), 88 Stat. 1790. The law establishing the Commission expressly also called for study of "the ways in which policies and practices relating to the maintenance of confidentiality of information impact upon Federal information activities." Pub. L. No. 93-556, 88 Stat. 1789, § 3(a)(6).

93. PAPERWORK REPORT, *supra* note 91, at 6-7.

confidentiality.[94] Some recommendations called for action by the President and by agencies. Suggested legislation included a new Fair Information Practices Act and a series of amendments to the Privacy Act of 1974.[95]

The Commission also recommended the creation of a new federal agency to centralize and coordinate existing information management functions within the executive branch and 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.[96] The new agency was to be composed of persons with knowledge and expertise in such fields as law, civil rights and liberties, records management, and computer technology.[97]

This recommendation was based in part on the Commission's conclusions about noncompliance with the Privacy Act. The Act was found to be confusing, in need of revision, and difficult to implement. The Commission found that the "overall guidance and advice which OMB has attempted to furnish have plainly been inadequate."[98] The Commission also found that judicial review has not been a meaningful remedy and suggested that this is unlikely to change until the Act is amended.[99]

The Commission concluded that legislation establishing the proposed new organization should authorize it to provide advice and guidance to other executive branch agencies, monitor compliance with information management laws, receive and mediate citizen complaints, and issue standards and regulations. The Commission noted that an agency with quasi-judicial authority could be more effective in enforcing compliance with law but that it might not be equipped to perform the functions of policy development, coordination, and direction. The Commission suggested that Congress could consider granting the agency additional enforcement powers in the future.[100]

D. Privacy Protection Study Commission (1975-77)

The Privacy Act of 1974 established the Privacy Protection Study Commission (PPSC) as a temporary study commission. The creation of the PPSC was part of a compromise between the Senate, which sup-

94. *Id.* at 8.

95. *See generally id.* at 139-175.

96. *Id.* at 150.

97. *Id.* at 148.

98. *Id.* at 147.

99. *Id.*; *see also supra* note 75. None of the Paperwork Commission's recommendations for amendments to the Privacy Act of 1974 has been enacted.

100. *Id.* at 150.

ported the creation of a permanent federal privacy agency, and the House, which was opposed to a privacy agency.[101] The PPSC had seven members; three appointed by the President of the United States, two by the President of the Senate, and two by the Speaker of the House.[102]

Of all of the privacy studies undertaken in the last twenty years, the PPSC had the broadest mandate to review privacy matters in the federal government, state governments, and the private sector.[103] The Privacy Act of 1974 assigned two general tasks to the Commission:

> (1) to make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information; and
>
> (2) to recommend to the President and the Congress the extent, if any, to which the requirements and principles of the Privacy Act should be applied to the information practices of those organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and to report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.[104]

In addition, the PPSC was directed to study several specific issues, including use of universal identifiers, mailing lists, use of Internal Revenue Service data, and the adequacy of provisions of the Privacy Act itself.[105] The legislation expressly authorized the PPSC to consider personal information activities relating to medical, insurance, education, employment, credit, banking, and other records.[106] The PPSC was also authorized to hold hearings, conduct inspections, and issue subpoenas to

---

101. *See supra* text accompanying notes 25-41.

102. Privacy Act of 1974, Pub. L. No. 93-579, § 5(a)(1), 88 Stat. 1907, (1974).

103. The PPSC did not address two major privacy issues that only began to emerge as the Commission completed its work. Computer matching began in 1977 with Project Match at the Department of Health, Education, and Welfare. *See generally* COMM. ON GOV'T. OPERATIONS, COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988, H.R. REP. NO. 802, 100th Cong., 2d Sess. (1988) (report to accompany H.R. 4699); Kirchner, *Privacy: A History of Computer Matching in Federal Government*, COMPUTERWORLD (Dec. 14, 1981), *reprinted in* OVERSIGHT OF THE PRIVACY ACT OF 1974: HEARINGS BEFORE A SUBCOMM. OF THE HOUSE COMM. ON GOV'T. OPERATIONS, 98th Cong., 1st Sess. at appendix 2 (1983).

A second major privacy issue that also grew to prominence in the mid-1970s was the flow of personal information across national borders. This general subject was originally known as "transborder data flow" and is today usually referred under the rubric of "data protection." For one of the earliest congressional discussions of international information issues, see COMM. ON GOV'T. OPERATIONS, INTERNATIONAL INFORMATION FLOW: FORGING A NEW FRAMEWORK, H.R. REP. NO. 1535, 96th Cong., 2d Sess. (1980).

104. Privacy Act of 1974, Pub. L. No. 93-579, § 5(b), 88 Stat. 1907 (1974).

105. *Id.* § 5(c).

106. *Id.* § 5(c)(2)(A).

carry out its functions.[107]

The PPSC issued a report[108] in 1977 and went out of existence. The PPSC report found five systemic features of personal data record keeping in America:

> First, while an organization makes and keeps records about individuals to facilitate relationships with them, it also makes and keeps records about individuals for other purposes, such as documenting the record-keeping organization's own actions and making it possible for other organizations — government agencies, for example, to monitor the actions of individuals.
>
> Second, there is an accelerating trend, most obvious in the credit and financial areas, toward the accumulation in records of more and more personal details about an individual.
>
> Third, more and more records about an individual are collected, maintained, and disclosed by organizations with which the individual has no direct relationship but whose records help to shape his life.
>
> Fourth, most record-keeping organizations consult the records of other organizations to verify the information they obtain from an individual and thus pay as much or more attention to what other organizations report about him than they pay attention to what he reports about himself; and
>
> Fifth, neither law nor technology now gives an individual the tools he needs to protect his legitimate interests in the records organizations keep about him.[109]

The first of the PPSC's 177 recommendations was that the President and the Congress establish a federal entity such as a Federal Privacy Board or other independent unit. The Board would be 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;
> 4) to advise the President, Congress, government agencies, and states regarding the privacy implications of proposed federal or state statutes or regulations.[110]

---

107. *Id.* § 5(e)(1).

108. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter PPSC REPORT]. In addition to the main report, the Commission issued five separate appendices. The titles were: PRIVACY LAW IN THE STATES, THE CITIZEN AS TAXPAYER, EMPLOYMENT RECORDS, THE PRIVACY ACT OF 1974: AN ASSESSMENT, and TECHNOLOGY AND PRIVACY.

109. PPSC REPORT, *supra* note 108, at 8.

110. *Id.* at 37.

In support of its recommendation for a Federal Privacy Board, the PPSC wrote about the difficulty of interpreting the law and establishing an appropriate uniform policy:

> [I]n all areas of the public sector the Commission has studied, the need for a mechanism to interpret both law and policy is clear. The difficulty of deciding which disclosures of records about individuals are routine within the meaning of the Privacy Act often raises conflicts of interest or interpretation between two or more Federal agencies. Similarly, . . .Federal agencies often need an efficient means of arriving at common solutions to their common privacy protection problems . . . . State agencies frequently complain about being subjected to multiple, and sometimes incompatible, record-keeping rules as a consequence of participating in programs funded by different Federal agencies or by different components within a single agency. There must also be a way of bringing private-sector recommendations for voluntary action to the attention of all the relevant organizations.[111]

The Commission indicated that the Federal Privacy Board should only have enforcement authority in connection with the implementation of the Privacy Act of 1974 by federal agencies. Responsibilities for other privacy matters would be limited to oversight, including the ability to participate in the proceedings of other agencies involving privacy matters.[112]

The recommendations of the PPSC were based on three objectives for an effective privacy protection policy:

> • to create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return (to minimize intrusiveness);
>
> • to open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it (to maximize fairness); and
>
> • to create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual (to create legitimate, enforceable expectations of confidentiality).[113]

The creation of a Federal Privacy Board was one way of imple-

111. *Id.* at 36.

112. *Id.* at 37. The Privacy Protection Study Commission's recommendation for a privacy board was also discussed at several congressional hearings. *See Final Report of the Privacy Protection Study Commission: Joint Hearing before the Senate Comm. on Gov. Affairs and a Subcomm. of the House Comm. on Gov't. Operations*, 95th Cong., 1st Sess. 8-10 (1977); *Privacy and Confidentiality Report and Final Recommendations of the Commission on Federal Paperwork: Hearing before a Subcomm. of the House Comm. on Gov't. Operations*, 95th Cong., 1st Sess. (1977); *Right to Privacy Proposals of the Privacy Protection Study Commission: Hearings on H.R. 10076 before a Subcomm. of the House Comm. on Gov't. Operations*, 95th Cong., 2d Sess. (1978).

113. PPSC REPORT, *supra* note 108, at 14-15.

menting these objectives. The PPSC also recommended a combination of voluntary compliance and statutory mechanisms to protect privacy. Voluntary compliance was suggested for the mailing list industry and for employment and personnel records.[114] In most other areas — such as credit, banking, insurance, health, and research — the PPSC recommended statutory protections.[115]

The Commission saw the Federal Privacy Board as part of a combination of compliance alternatives that will be capable of responding to the dynamic character of record keeping practices for personal data. The Board was to serve as a focal point to keep privacy concerns in perspective and to respond to new privacy problems.[116]

IV. EXECUTIVE BRANCH AGENCIES AND INITIATIVES ON PRIVACY

There are three federal agencies that have had direct general[117] or international privacy policy responsibilities for significant parts of the last two decades: the Office of Management and Budget in the Executive Office of the President; the National Telecommunications and Information Administration at the Department of Commerce; and the Bureau of International Communications and Information Policy at the Department of State.[118] Privacy represents only a small fraction of the work of these agencies. A brief review of their privacy policy activities

114. PPSC Chairman David Linowes recently testified that new remedies were needed to protect individuals. *See 1991 House Data Protection Hearings, supra* note 50, 84.

115. PPSC REPORT, *supra* note 108, at 29-35.

116. *Id.* at 35-36.

117. The Office of Federal Register in the National Archives and Records has the responsibility to compile and publish a federal agency system of records notices and rules under the Privacy Act of 1974. 5 U.S.C. § 552a(f) (1988). This is a general privacy responsibility which other countries have been assigned to data protection offices. The assignment of this responsibility to the Office of Federal Register is a direct consequence of the Privacy Act's requirement that all system's of records notices be initially published in the Federal Register. 5 U.S.C. § 552a(e)(4) (1988). Since the function is ministerial and the Office exercises no substantive control or oversight over other agencies, no further discussion is warranted.

118. Beginning in 1989, the U.S. Office of Consumer Affairs in the Department of Health and Human Services appears to have adopted privacy as an issue. The Office was established in 1971 by Executive Order 11,583. 36 Fed. Reg. 3509 (1971). There is nothing in the Executive Order assigning specific privacy responsibilities to the Office, and there is no evidence of any general privacy-related activities prior to 1989. For example, the Office had no role in the Carter Administration Privacy Initiative. The privacy effort coincided with the appointment of Dr. Bonnie Guiton as Director of the Office of Consumer Affairs and Special Adviser to the President for Consumer Affairs. Representatives of the Office have participated in meetings and hearings on privacy, but the scope of the Office's authority, jurisdiction, and continuing interest for privacy issues is uncertain.

Other agencies, such as the United States Trade Representative, have become involved from time to time in international discussions and negotiations on data protection

will demonstrate that none has managed to sustain an interest in or commitment to privacy policy work for more than a short period. None of the agencies has the mission or capability to serve as a general privacy policy agency.

Agency[119] or program[120] specific privacy activities are not within the scope of this review.

A. OFFICE OF MANAGEMENT AND BUDGET (1975-PRESENT)

The Privacy Act of 1974 established privacy and record management rules for federal agency records containing personal information about individuals.[121] While each federal agency is responsible for fulfilling the requirements of the Act[122], the law 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.[123] OMB was given this general su-

---

issues. This is part of the agency's general international functions and does not represent the exercise of direct policy responsibility for data protection.

119. Only one federal agency has a major internal privacy office. For a discussion of the Defense Privacy Board, see COMM. ON GOV'T. OPERATIONS, WHO CARES ABOUT PRIVACY? OVERSIGHT OF THE PRIVACY ACT OF 1974 BY THE OFFICE OF MANAGEMENT AND BUDGET AND BY THE CONGRESS, H.R. REP. NO. 455, 98th Cong., 1st Sess. 34-35 (1983) [hereinafter 1983 OVERSIGHT REPORT]. Other agencies generally have assigned Privacy Act responsibilities to relatively low-level staff. *See* FLAHERTY, *supra* note 2, at 328-337.

120. For example, the Family Educational and Privacy Rights Act, which establishes rules for the maintenance, use, and disclosure of student records maintained by educational institutions receiving federal funds, is administered by the Department of Education. *See* 20 U.S.C. § 1232g (1988). Similarly, the Fair Credit Reporting Act, which establishes information rules for credit reporting agencies, is administered by the Federal Trade Commission. *See* 15 U.S.C. § 1681 et seq. (1988). Not all laws that can be characterized as privacy laws have oversight agencies. *See, e.g.*, the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1988), which is enforced through criminal penalties.

121. 5 U.S.C. § 552a (1988). The Act does not normally apply to records maintained by entities other than federal agencies. The Act can be applied to government contractors who maintain personal records to accomplish an agency function. 5 U.S.C. § 552a(m) (1988).

122. Office of Management and Budget, Management of Federal Information Resources *reprinted in* 50 Fed. Reg. 52,738 (1985) at Appendix I, § 3a (Circular No. A-130).

Some commentators characterize data protection laws as "first generation" or "second generation". One describes second generation legislation as characterized by a trend to simplification, a greater amount of differentiation for different sectors, a trend in favor of self-regulation, and the increased use of informal and civil sanctions. *See* NUGTER, *supra* note 3, at 19. The U.S. Privacy Act of 1974, which does establish a uniform set of rules for most federal records, would be recognized as a first generation law. *See also* Simitis, *supra*, note 7, at 22.

123. This requirement was originally included in section six of the Privacy Act of 1974, a part of the Act that was uncodified. *See* Pub. L. No. 93-579, 88 Stat. 1907 (1974). This section was repealed by the Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, § 6(c), 102 Stat. 2506 (1988), and reenacted as part of the codified portion of

pervisory role as part of the 1974 compromise over the need for a privacy agency.[124] OMB also has responsibility to review agency proposals to establish or alter a Privacy Act system of records[125] and to submit a consolidated report on the administration of the Act.[126]

The Paperwork Reduction Act of 1980[127] slightly broadened the privacy role of OMB. That Act centralized the information functions of OMB in the newly created Office of Information and Regulatory Affairs. Privacy functions were defined to include developing and implementing policies on information disclosure and confidentiality; providing agencies with advice about information security; and monitoring compliance with the Privacy Act.[128]

A 1983 report by the Committee on Government Operations reviewed in detail the record of OMB Privacy Act oversight.[129] In general, the Committee found that OMB was not especially interested in the Privacy Act and was not effective in an oversight capacity. Some specific findings were:

> • Interest in the Privacy Act at the Office of Management and Budget has diminished steadily since 1975. Each successive Administration has shown less concern about Privacy Act oversight.
>
> • OMB issued extensive Privacy Act guidelines contemporaneous with the effective date of the Act in 1975. Since 1975, however, OMB has not actively pursued its responsibility to revise and update Privacy Act guidance. With the exception of computer matching guidelines, OMB has issued no guidance reflective of experience with the law, problems encountered by agencies, or court decisions. OMB does respond to questions and problems brought to its attention by agencies.
>
> • OMB's Privacy Act oversight is reactive to changes in Privacy Act systems of records proposed by agencies. In the absence of a proposal for change, OMB does not conduct any active supervision or review of agency Privacy Act regulations or activities. OMB does not monitor agency compliance with its computer matching guidelines.[130]

---

the Privacy Act. *See* 5 U.S.C. § 552a(v) (1988). The 1988 amendment also expressly requires OMB to provide notice and opportunity for public comment for its guidelines and regulations.

124. *See supra* note 41 and accompanying text.

125. 5 U.S.C. § 552a(r) (1988). Minor changes were made in 1988 to the content of the system of records notices and to the scope of the advance reporting requirement. For an explanation, see HOUSE COMM. ON GOV'T. OPERATIONS, COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988, H.R. REP. NO. 802, 100th Cong., 2d Sess. 37 (1988) (report to accompany H.R. 4699).

126. As originally enacted, a report was due annually from OMB. As amended by the Computer Matching and Privacy Protection Act of 1988, the report is now due biennially. *See* 5 U.S.C. § 552a(s) (1988).

127. 44 U.S.C. § 3501 et seq. (1988).

128. 44 U.S.C. § 3504(f) (1988).

129. 1983 OVERSIGHT REPORT, *supra* note 119.

130. *Id.* at 35-36.

These findings were based in part on assessments of OMB's Privacy Act activities made by the Privacy Protection Study Commission, the Commission on Federal Paperwork, and veteran privacy observers such as Ronald Plesser, former General Counsel to the Privacy Protection Study Commission; James Davidson, former Counsel to the Senate subcommittee that drafted the Privacy Act; John Shattuck, National Legislative Director of the American Civil Liberties Union; and privacy scholar David Flaherty.[131] There was universal agreement that OMB did little with its Privacy Act responsibilities after the initial implementation period in 1975.

The Committee report generally recommended that OMB should pay more attention to its Privacy Act responsibilities.[132] The criticism of OMB in the report drew a reaction from some Committee Members. Representative John Erlenborn, the Republican floor manager for the Privacy Act of 1974, believed that it was the intent of Congress that OMB's role be limited and that OMB should not be condemned for "not having fulfilled a responsibility it was never given."[133] Whether OMB has not engaged in active oversight of the Privacy Act by statutory design or simply by lack of interest, the result is the same. Other Committee Members stated in separate views to the 1983 report that the enactment of the Paperwork Reduction Act increased the expectations of OMB on information management issues, including privacy, but that OMB was entitled to more time to meet the expectations.[134]

There is, however, little evidence in recent years of any significant increase in OMB Privacy Act activity. For example, the 1983 Government Operations Committee report included a discussion of OMB's compliance with the Privacy Act's requirement for an annual report.[135] The report found that OMB had failed to comply with the statutory requirements for a periodic report on the Privacy Act.[136] In recent years, OMB has continued to show little interest in meeting the Privacy Act's reporting requirement. A Privacy Act report was issued in December

131. *Id.* at 8-9.

132. *Id.* at 36-37.

133. *Id.* at 57 (Separate views of Hon. John N. Erlenborn).

134. *Id.* at 58 (Separate views of Hon. Thomas N. Kindness, Hon. Frank Horton, Hon. Lyle Williams, Hon. Dan Burton, Hon. Tom Lewis, Hon. Alfred A. (Al) McCandless, Hon. Larry E. Craig, and Hon. Dan Schaffer).

135. While a comparison of OMB's privacy activities with those of data protection authorities in other countries may be unfair or inappropriate, it is worth observing that the annual reports of those authorities are frequently important, highly visible documents. *See, e.g.*, FLAHERTY, *supra* note 2, at 62 (Germany); 138 (Sweden); 208 (France); 275 (Canada). *See also* 1992 Draft EC Data Protection Directive, *supra* note 6, commentary on Article 30 ("It is very important that the supervisory authority should be able to present a report on its activities at periodic intervals . . . .").

136. *Id.* at 24-27, 36.

1985 covering calendar years 1982 and 1983.[137] By law, that report was supposed to cover a one-year period. Although the Privacy Act was amended in 1988 to change the reporting requirement from annual to biennial,[138] OMB has not promptly or completely met the revised requirement.[139] The next report was dated December 1992, and it formally covered 1988 and 1989. The report also included "for purposes of historic comparison," data concerning access and amendment requests for the four years since the last report.[140]

The history of computer matching offers a later perspective on OMB's response to a complex privacy problem.[141] When computer matching became an issue in the late 1970s, OMB issued additional guidance to agencies under the Privacy Act.[142] In 1982, following the election of President Reagan, pressure from Inspectors General led OMB to revise the matching guidance to make it easier to conduct matching.[143] When the guidance was changed in 1982, OMB did not solicit public comments as it did in 1979. Comments were received only from those who advocated increased use of computer matching.[144] Those concerned about the privacy implications of matching were not given an opportunity to participate in the revision.

As a result of continuing dissatisfaction with computer matching policies, a hearing on legislation to regulate computer matching was

---

137. *The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974 CY 1982 - 1983* (undated, but President Reagan's transmittal letter was dated Dec. 4, 1985).

138. The change was made as part of the Computer Matching and Privacy Protection Amendments of 1988, Pub. L. No. 100-503, § 8, 102 Stat. 2514 (codified at 5 U.S.C. § 552a(s) (1988)).

139. OMB did submit a required annual report on the implementation of the Computer Matching and Privacy Protection Act. The report for calendar year 1990 was transmitted in October, 1992. The report consists primarily of a list of matching programs and the membership of data integrity boards.

140. *The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974 CY 1988 - 1989* (Dec. 4, 1992).

141. A more detailed history of OMB's early computer matching activities can be found in 1983 OVERSIGHT REPORT, *supra* note 119; *see also* COMM. ON GOV'T. OPERATIONS, COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988, H.R. REP. NO. 802, 100th Cong., 2d Sess. (1988).

142. Guidelines for the Conduct of Matching Programs, 44 Fed. Reg. 23,138 (1979). This was part of President Jimmy Carter's privacy initiative. *See infra* notes 161-166 and accompanying text.

143. Revised Supplemental Guidance for Conducting Matching Programs, 47 Fed. Reg. 21,656 (1982). Principal changes to earlier guidance included the elimination of a requirement for a cost-benefit analysis before performing a match, fewer notice and reporting requirements by the matching agency, and elimination of provisions covering intra-agency matching. *See* 1983 OVERSIGHT REPORT, *supra* note 119, at 12-13.

144. 1983 OVERSIGHT REPORT, *supra* note 119, at 35-36.

held in the Senate in 1986.[145] In the following Congress, the Computer Matching and Privacy Protection Act of 1988 was enacted to regulate computer matching activities.[146] This Act was passed in part because of dissatisfaction with OMB's guidance and oversight.[147]

The matching law required each federal agency involved in matching activities to establish a Data Integrity Board to oversee and coordinate implementation of computer matching.[148] Because of OMB's indifferent record with oversight of the Privacy Act and computer matching, no consideration was given to assigning this more detailed responsibility to OMB. OMB's role was limited by law to developing computer matching guidelines and regulations for agencies.[149] Reporting and appeal responsibilities were also given to OMB.[150] In effect, OMB was asked to undertake only those functions that it had shown some willingness to undertake in the past.[151] The Computer Matching Act and Privacy Protection Act of 1988 did not expand or broaden OMB's privacy responsibilities in any significant way.

Congress did not assign the Data Integrity Boards a broad privacy policy role.[152] The functions of the Data Integrity Boards were narrowly focused on computer matching rather than the Privacy Act as a

---

145. *Computer Matching and Privacy Protection Act of 1986: Hearings Before the Subcomm. on Oversight of Gov't. Management, Senate Comm. on Governmental Affairs*, 97th Cong., 2d Sess. (1986). Earlier hearings had been held in 1982. *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings Before the Subcomm. on Oversight of Government Management of the Senate Committee on Governmental Affairs*, 97th Cong., 2d Sess. (1982); *see also Computer Matching and Privacy Protection Act of 1987: Hearings Before a Subcomm. of the House Comm. on Gov't. Operations*, 100th Cong., 1st Sess. (1987).

146. Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (1988). The 1988 matching law amended the Privacy Act of 1974, 5 U.S.C. § 552a (1988).

147. *See* COMM. ON GOV'T. OPERATIONS, COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988, H.R. REP. 802, 100th Cong., 2d Sess. 11 (1988) (footnotes omitted).

> It is apparent from these studies and reports that, over the course of a few years, computer matching has burgeoned into a major Federal activity. Both the executive and legislative branches have encouraged the growth of matching. However, few administrative controls, procedures, or guidelines are in place. Guidance issued by OMB has been largely ignored by agencies and unenforced by OMB. There is no meaningful oversight of computer matching in the Executive Branch.

Id.

148. 5 U.S.C. § 552a(u) (1988).

149. Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, § 6(b), 102 Stat. 2507 (1988).

150. 5 U.S.C. § 552a(u)(5), (6) (1988).

151. OMB did issue guidance as required by the Computer Matching and Privacy Protection Act of 1988. *See* Final Guidance Interpreting the Provisions of Public Law 100-503, Computer Matching and Privacy Act of 1988, 54 Fed. Reg. 25,818 (1989).

152. COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988, H.R. REP. 802, 100th Cong., 2d Sess. 32 (1988). The Senate had proposed that the Boards have responsi-

whole or other privacy issues. The principal function of the Boards is reviewing and approving matching agreements for compliance with the procedural requirements of the law.[153] Other functions include a variety of different types of reviews of matching activities, but there is no specific mechanism or timetable that will enforce compliance with these requirements.[154] There is no evidence that the Boards have engaged in any non-matching privacy activities, and there has been no comprehensive evaluation of the functioning of the Boards as matching overseers.[155] The evidence that is available suggests that the Boards have not been not effective.[156]

The Committee's 1983 conclusions about OMB's privacy activities remain valid today.[157] OMB has continued to show limited interest in privacy and, at best, reacts only to those Privacy Act issues expressly brought to its attention. Professor Flaherty's evaluation is that "OMB is the closest approximation to a data protection agency, although it is artificial to treat it as such, because OMB's current perception of its duties is so passive."[158]

Whether Congress originally intended a stronger privacy role for OMB may be debated. The Computer Matching and Privacy Protection Act reflects a recent judgment by the Congress that only limited privacy monitoring and oversight can be expected from OMB. Both OMB and the Congress appear to have tacitly agreed that OMB's privacy activities will remain low-key and limited to the Privacy Act of 1974.

---

bility for reviewing and coordinating privacy training programs. This was dropped by the House. *Id.*

There was some concern that the Boards might not be sufficiently independent. Because of fears that agency Inspectors General would not exercise detached judgment about matching, the law expressly prohibits an Inspector General from serving as chairman of a Data Protection Board. 5 U.S.C. § 552a(u)(2) (1988).

153. *Id.* § 552a(u)(3)(A).

154. *Id.* § 552a(u)(3)(B)-(H).

155. As of the date of this report, there has been no independent review of the operations or effectiveness of Data Integrity Boards. A comprehensive review of the Computer Matching and Privacy Protection Act of 1988 is underway at the General Accounting Office.

156. A recent review concluded the Data Integrity Boards were not ensuring agency compliance with the matching requirements. P. Regan, *Data Integrity Boards: Institutional Innovation and Congressional Oversight* (1992) (paper delivered before the American Political Science Association).

157. *See also* GENERAL ACCOUNTING OFFICE, PRIVACY ACT: FEDERAL AGENCIES' IMPLEMENTATION CAN BE IMPROVED (1986) (GGD-86-107).

158. FLAHERTY, *supra* note 2, at 316.

B. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (DEPARTMENT OF COMMERCE, 1978-PRESENT)

The privacy responsibilities of the National Telecommunications and Information Administration of the Department of Commerce (NTIA) originated with the establishment of a privacy coordinating committee by President Carter in 1977 as part of a presidential privacy initiative. This committee — which was co-chaired by the Secretary of Commerce and the President's Domestic Policy Advisor — developed privacy proposals following the release of the recommendations of the Privacy Protection Study Commission in 1977.[159] The staff that carried out the work was transferred to the National Telecommunications and Information Administration (Department of Commerce) at the time of its establishment in 1978.[160]

On April 2, 1979, President Carter announced "sweeping proposals to protect the privacy of individuals."[161] President Carter's privacy policies were based on two principles:

> • *Fair Information Practices.* Standards must be provided for handling sensitive, personal records. Individuals should be told what kind of information is being collected about them, how it will be used, and to whom it will be disclosed. They should be able to see and obtain a copy of the records and correct any errors. They should be told the basis for an adverse decision that may be based on personal data. And they should be able to prevent improper access to the records.
>
> • *Limits on the Government.* Government access to and use of personal information must be limited and supervised so that power over information cannot be used to threaten our liberties.[162]

The Carter initiative included proposed legislation to protect the privacy of medical records, to extend fair information protections to consumer credit, banking, and insurance records, to protect the privacy of records used for research purposes, and to revise the Privacy Act of 1974.[163] Four of the five bills proposed as part of the Carter initiative

---

159. President's Message to Congress on Proposals To Protect the Privacy of Individuals, I PUB. PAPERS 582 (1979) [hereinafter Carter Privacy Message].

160. *See* GENERAL ACCOUNTING OFFICE, PRIVACY POLICY ACTIVITIES OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (Aug. 31, 1984) (GGD-84-93) [hereinafter GAO NTIA REPORT]; *see also Right to Privacy Proposals of the Privacy Protection Study Commission: Hearings Before a Subcomm. of the House Comm. on Gov't. Operations*, 95th Cong., 2d Sess. 164-65 (1978) (testimony of C.L. Haslam, General Counsel, Department of Commerce).

161. Carter Privacy Message, *supra* note 159, at 581.

162. *Id.*

163. *Id.* at 583-86. Other proposals addressed use of lie detectors, government access to news media files, and wiretapping. *Id.*

failed to pass.[164]

In his message, President Carter also addressed international privacy issues.[165] He said that the United States was working with other governments in several international organizations to develop principles to protect personal data crossing international borders and to harmonize privacy rules. The President stated that enactment of his proposals should help this process by assuring other countries that the United States is committed to the protection of personal data.[166]

President Carter did not address the recommendation of the Privacy Protection Study Commission for a permanent privacy agency. He did, however, indicate that the Office of Management and Budget would take some actions to implement administrative components of the privacy initiative.[167] Also, NTIA was designated as the lead agency on other privacy matters and on the continuing development of privacy policy.[168]

NTIA's mission was much broader than privacy.[169] Its principal mission was to develop telecommunications and information policy, allocate and manage federal use of radio frequencies, and provide grants for public telecommunications facilities. NTIA was specifically authorized to consider privacy in the coordination of telecommunications activities of the executive branch.[170] NTIA's more general privacy work was part of its general responsibility to study and make recommendations on the impact of the convergence of computer and communica-

164. GAO NTIA REPORT, *supra* note 160. The one bill that did pass was the Privacy Protection Act of 1980, a bill to regulate searches of newsrooms. This legislation was a response to a Supreme Court decision rather than to the report of the Privacy Protection Study Commission. *See* 42 U.S.C. § 2000aa. (1988). Limiting newsroom searches is not a traditional data protection issue. The Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (1988), was enacted following recommendations of the Privacy Protection Study Commission, but its enactment predated the Carter Privacy Initiative.

165. This represented one of the first official recognitions in the United States of the international importance of privacy protection. Earlier privacy efforts focused exclusively on domestic issues. Interest in transborder data flows and the international consequences of privacy protection became much stronger in the late 1970s and early 1980s. *See generally* FLAHERTY, *supra* note 2.

166. Carter Privacy Message, *supra* note 159, at 587.

167. One of the actions taken by OMB following the President's directive was the issuance of computer matching guidelines in 1979. The guidelines were substantially weakened three years later. *See* 1983 OVERSIGHT REPORT,*supra* note 119, at 9-13.

168. Carter Privacy Message, *supra* note 159, at 586.

169. Exec. Order No. 12,046, 15 C.F.R. 2301 (1989), *reprinted in* CODIFICATION OF PRESIDENTIAL PROCLAMATIONS AND EXECUTIVE ORDERS 937 (April 13, 1945 - January 20, 1989). The reorganization combined the functions and resources of the Office of Telecommunications Policy in the Executive Office of the President and the Office of Telecommunications within the Department of Commerce.

170. *Id.* 2-405.

tions technology.[171] This responsibility had its origins in President Carter's response to the report of the Privacy Protection Study Commission.[172]

President Carter designated NTIA as the lead agency for (a) coordinating the legislative work of the privacy initiative; (b) developing international privacy initiatives, subject to the State Department's authority for conducting foreign policy;[173] and (c) studying the consequences of the growth of information technology on privacy, and monitoring nonfederal information practices.[174]

NTIA's privacy activities diminished rapidly after 1980. According to GAO, in 1979 and 1980, there were fifteen staff positions associated with privacy activities. In 1981, the number of positions were reduced to six. In 1982, there were only four privacy staff positions, and this number was reduced to one in 1983, 1984, and 1985.[175] By 1989, it appeared that privacy had entirely disappeared as an activity at NTIA. At a hearing on legislation reauthorizing the agency, the head of NTIA testified broadly about the agency's responsibilities, activities, and interests. Her prepared testimony did not directly or indirectly mention any privacy activities.[176]

At a hearing in 1984, a former NTIA privacy staffer confirmed the agency's loss of interest in privacy. Jane Yurow, Director of the OECD Privacy Guidelines Project, testified that the NTIA privacy initiative disappeared with the Reagan Administration:

> Shortly after Mr. Reagan took office, the privacy staff at NTIA was dismantled. No one associated with that effort is currently working on privacy-related issues, and most of the staff has left the Government.[177]

---

171. GAO NTIA REPORT, *supra* note 160.

172. *See supra* notes 101-116 and accompanying text.

173. *See infra* notes 195-204 and accompanying text.

174. GAO NTIA REPORT, *supra* note 160.

175. *Id.*

176. *NTIA Authorization: Hearings before the Subcomm. on Communications of the Senate Comm. on Commerce, Science, and Transportation*, 101st Cong., 1st Sess. (1989) (testimony of Janice Obuchowski, Assistant Secretary for Communications and Information, Department of Commerce) (S. Hrg. 101-428).

177. *Privacy and 1984: Public Opinions on Privacy Issues: Hearings Before a Subcomm. of the Comm. on Gov't. Operations*, 98th Cong., 1st Sess. 115 (1984) [hereinafter *1984 Privacy Hearings*].

See also id. at 271 (testimony of John Shattuck, National Legislative Director, American Civil Liberties Union) ("[The Reagan Administration] emasculated the one federal agency charged with developing privacy protections inside the federal government, the National Telecommunications and Information Administration.").

But see Letter from David J. Markey, Assistant Secretary for Communications and Information, Department of Commerce, to Chairman Glenn English, Subcommittee on Government Information, Justice, and Agriculture (April 13, 1984), *reprinted in 1984 Pri-*

The principal international privacy activities of NTIA related to privacy guidelines adopted in 1980 by the Organization for Economic Cooperation and Development (OECD).[178] The OECD is an international organization that promotes economic and social welfare and stimulates and harmonizes efforts on behalf of developing nations. The United States is a member along with nearly all industrialized free market countries. The OECD privacy guidelines were adopted in part because of concerns about the potential loss of privacy protections as a result of the flow of personal data from countries with strong privacy laws to countries with weaker laws.[179]

NTIA took the position that voluntary adoption of the guidelines by American companies — as opposed to formal legislative or administrative action — would demonstrate a serious commitment to privacy protection.[180] In 1981 and 1982, NTIA requested private sector endorsement of the OECD guidelines.[181] By 1983, 182 major U.S. multinational corporations and trade associations had endorsed the guidelines.[182]

Evaluating NTIA's privacy activities is not a simple task. The agency was engaged in domestic and legislative privacy efforts, but there is little to show for them. The period of activity was brief, and

---

vacy Hearings, *supra*, at 165. Mr. Markey took issue with Ms. Yurow's testimony and claimed that NTIA continued to be concerned with privacy protection and has adequate personnel to address the issues. *See also* GAO NTIA REPORT, *supra* note 160 ("At the present time [1984], NTIA maintains a minor residual capability to respond to or refer request for information on privacy matters.").

178. *See supra* note 5.

179. *See, e.g., supra* note 5, at Explanatory Memorandum, paragraph 7.

> For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favor of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.

Id.

180. GAO NTIA REPORT, *supra* note 160. In support of this position, NTIA produced a paper on U.S. privacy law. *See* DEPARTMENT OF COMMERCE, PRIVACY PROTECTION LAW IN THE UNITED STATES (1982) (NTIA Report 82-98), *reprinted in Oversight of the Privacy Act of 1974: Hearings before a Subcomm. of the House Comm. on Gov't. Operations*, 98th Cong., 1st Sess. 491-584 (1983).

181. *See* Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce, to Interagency Committee on International Communications and Information Policy, *Report on OECD Guidelines Program* (Oct. 30, 1981), *reprinted in International Telecommunications and Information Policy: Hearings before a Subcomm. of the House Comm. on Gov't. Operations*, 97th Cong., 1st & 2d Sess. 27-58 (1981-82) [hereinafter *International Policy Hearings*].

182. GAO NTIA REPORT, *supra* note 160.

the agency cannot exclusively be blamed for the failure of the Carter privacy legislation agenda.

On the international front, a variety of alternate conclusions can be drawn depending on what is being evaluated. United States efforts in the early 1980s to avoid the imposition of international controls over the transfer of personal information across national borders were successful.[183] This was a goal of NTIA, and it is fair to assume that NTIA's work contributed to the success.[184] In addition, at least one observer found that NTIA's foreign visibility as a privacy office was valuable.[185]

However, the sincerity and substantive effect of NTIA's efforts to secure domestic corporate compliance with international privacy standards have been questioned. The Director of NTIA's OECD Privacy Guidelines Project testified that the focus of NTIA's interest was on avoiding embarrassment. As soon as the international pressure was off, NTIA's staff was no longer allowed to discuss the guidelines project with the press or to make speeches urging corporations to comply with the guidelines.[186] The activities involving advising multinational corporations on data privacy policies were disbanded by the fall of 1982.[187] By 1983, the privacy protection aspects of the transborder data flow issue warranted only a brief mention in an NTIA report on long-range international telecommunications and information goals.[188]

Further, it is not clear if the endorsement of the OECD guidelines

---

183. The transborder data flow issue faded in importance as the 1980s progressed. But at the end of the decade, strong European data protection efforts produced a renewal of concern and activity, capped by the 1990 proposed European Community directive on data protection. *See supra* note 6 and accompanying text.

184. *See, e.g, International Policy Hearings*, *supra* note 180, at 83-84 (testimony of Joseph R. Wright, Jr., Deputy Secretary of Commerce, Department of Commerce); *see also* HOUSE COMM. ON GOV'T. OPERATIONS, INTERNATIONAL INFORMATION FLOW: FORGING A NEW FRAMEWORK, 96th Cong., 2d Sess. 41 (1980) [hereinafter 1980 HOUSE INTERNATIONAL INFORMATION REPORT].

185. *See* FLAHERTY, *supra* note 2, at 319. ("[F]or a government the size of the United States, the minimal investment in NTIA was surely productive, especially in terms of giving foreign data protectors a contact point for issues of transborder data flow.").

186. *1984 Privacy Hearings*, *supra* note 176, at 115 (testimony of Jane Yurow, former Director of the Department of Commerce Project on International Privacy Guidelines). Ms. Yurow also testified that "the administration's policy was that once the Commerce Department had made corporations aware of the problem, it has done its job. From then on, corporations were expected to fend for themselves. This, despite the fact that it was the U.S. Government and not U.S. industry, that had committed to implementing the guidelines." *Id.*

187. *Id.*

188. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, LONG-RANGE GOALS IN INTERNATIONAL TELECOMMUNICATIONS AND INFORMATION: AN OUTLINE FOR UNITED STATES POLICY (1983), (printed as Senate Print 98-22, 98th Cong., 1st Sess. (printed for use of the Senate Committee on Commerce, Science, and Transportation)).

by American companies had any actual effect on privacy practices.[189] Because there are no independent audits of corporate privacy practices, direct evidence on this point is not readily available. Nevertheless, there are indications that the NTIA efforts produced little change in practice. Some such evidence is provided by a study conducted by Business International in 1983 on transborder data flows. The study reported that European data protection authorities were skeptical of the OECD guideline endorsements. These authorities noted that the guidelines are voluntary and that the endorsements of most firms amount to little more than lip service. A survey conducted by Business International in connection with the report offered some confirmation. It found that interviewees in ten out of thirty-four U.S. companies that had endorsed the guidelines did not even know that their firms had done so.[190] Only seven executives interviewed even knew that their firms had endorsed the guidelines, and three strongly denied that their firms had done so.[191]

A more recent survey of private protections in big business was conducted in 1989 by David Linowes, Professor of Political Economy and Public Policy, University of Illinois.[192] Professor Linowes is the former chairman of the Privacy Protection Study Commission. The survey is based on a sample of companies selected from among the Fortune 500 corporations.

In testimony summarizing the results, Professor Linowes said that too many of the nation's largest industrial corporations do not have adequate private policies:

> It has been fourteen years since the U.S. Privacy Protection Study Commission submitted its recommendations to President Carter and the Congress urging business to adopt privacy safeguards for its employment-related records. Yet today, too many of the nation's largest industrial corporations still do not have adequate policies to protect sensitive, confidential employee data from possible abuse. This was revealed by a recent survey of the Fortune 500 Companies I had conducted by the Survey Research Laboratory at the University of

189. One knowledgeable privacy observer concluded that "[e]arlier regional and international action on privacy and data protection, specifically the OECD Guidelines and the Council of Europe's Convention, had little or no effect on the development of privacy law in the United States." P. Regan, The Globilization of Privacy: Implications of Recent Changes in Europe, Paper Delivered Before the American Sociological Association (1992).

190. Business International, *Transborder Data Flow: Issues, Barriers and Corporate Responses* 16 (1983) (Executive Summary).

191. Jake Kirchner, *Despite Data Flow Restriction Woes, U.S. Firms Seen Lax in Data Privacy*, COMPUTERWORLD, May 9, 1983, at 13.

192. UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, RESEARCH SURVEY OF INDIVIDUAL PRIVACY PROTECTION IN BIG BUSINESS (1989) *in* LINOWES, PRIVACY IN AMERICA: IS YOUR PRIVATE LIFE IN THE PUBLIC EYE? 40-61 (1989).

Illinois.[193]

While the Linowes survey does not address the OECD guidelines directly, many of the questions pertained to privacy practices that are within the scope of the guidelines. For example, the openness principle in the OECD guidelines calls for a general policy of openness about developments, practices, and policies for personal data. This means that there should be a readily available way to establish the existence and nature of personal data systems and the main purposes of their use.[194]

The Linowes survey found that most employees are not told much about their own records. Over half of responding companies do not inform their personnel of the types of records maintained on them (57%), how the records are used (59%), and what the company's routine disclosure practices are (58% for government, 57% for nongovernment). Almost two in five (38%) do not tell their personnel that records are accessible to them.[195]

While these survey results must be interpreted with caution, there is both internal and external evidence to support the view that NTIA's efforts on international data protection produced few actual or long-lasting changes in American business record keeping practices. It is clearer that NTIA's commitment to improving privacy protection was neither broad nor deep nor long-lasting. At no time did NTIA serve as a general resource or overseer of either governmental or private sector privacy practices.

C. Bureau of International Communications and Information Policy (Department of State, 1983-Present)

In 1983, legislation was passed codifying the existing State Department Office of the Coordinator for International Communications and Information Policy.[196] In 1985, the Office was combined with the Office of International Communications Policy as the Bureau of International Communications and Information Policy.[197] This Bureau plays a role in

193. *Domestic and International Data Protection Issues: Hearings Before the Gov't. Information, Justice, and Agriculture Subcomm. of the House Comm. on Gov't. Operations*, 102d Cong., 1st Sess. 93 (1991) (statement of David F. Linowes) [hereinafter *1991 Privacy Hearings*].

194. *OECD Guidelines, supra* note 5, at 12.

195. *1991 Privacy Hearings, supra* note 193. Linowes compared the results of the 1989 survey with a similar survey conducted shortly after the Privacy Protection Study Commission was dissolved in 1977. He concluded that there was "some progress, but extremely little progress." *Id.*

196. 22 U.S.C. § 2707 (1988). For a discussion of the origins of the office, see *International Policy Hearings, supra* note 180, at 119 (testimony of James Buckley, Under Secretary of State for Security Assistance, Science and Technology, Department of State).

197. A 1980 report of the House Committee on Government Operations included a recommendation for a Bureau of International Communications and Information. 1980

coordinating and negotiating international privacy matters. The legislation does not refer expressly to privacy or data protection. Instead, the tasks are defined in terms of "international communications and information policy."[198] The legislative history also contains no direct reference to privacy or data protection.[199] Most of the Bureau's activities have centered on its telecommunications responsibilities.

Along with NTIA, the Bureau played a role in the negotiations that led to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[200] While the bulk of the work on the OECD Guidelines was done by NTIA, it appears that the State Department was more actively involved with negotiations on international data protection in the late 1970s and early 1980s than in later years.[201]

It is difficult to find much documentation of international privacy activities of the Bureau during the last decade. For example, there is only a brief mention of privacy in the prepared testimony of the Director of the Bureau for a 1986 oversight hearing.[202] The Bureau has also operated an advisory committee on international communications and

---

HOUSE INTERNATIONAL INFORMATION REPORT, *supra* note 183, at 11. This was one of several structural recommendations in response to the developing issue of transborder data flow. Data protection is one aspect.

The report reviewed the response of the United States to the entire range of international information flow issues and found that "The United States Government has no coordinated policy regarding barriers to international data flow. Neither does it have any coherent policy regarding particular barriers and the problems they create for the United States and its political, social and economic interests." *Id.* at 10.

198. *Id.*

199. *See* HOUSE COMM. ON FOREIGN AFFAIRS, AUTHORIZING APPROPRIATIONS FOR FISCAL YEARS 1985 AND 1985 FOR THE DEPARTMENT OF STATE, THE UNITED STATES INFORMATION AGENCY, THE BOARD FOR INTERNATIONAL BROADCASTING, THE INTER-AMERICAN FOUNDATION, AND THE ASIA FOUNDATION, TO ESTABLISH THE NATIONAL ENDOWMENT FOR DEMOCRACY, AND FOR OTHER PURPOSES, H.R. Rep. No. 130, 98th Cong., 1st Sess. 50-56 (1983) (report to accompany H.R. 2915).

200. *See International Policy Hearings*, *supra* note 180, at 120-21 (testimony of James Buckley, Under Secretary of State for Security Assistance, Science and Technology, Department of State); *See also supra* notes 177-194 and accompanying text.

201. *Id.*

202. *Oversight of the Bureau of International Communications and Information Policy: Hearings before the Subcomm. on International Operations of the House Comm. on Foreign Affairs*, 99th Cong., 2d Sess. (1986) (testimony of Diana Lady Dougan, U.S. Coordinator and Director, Bureau of International Communications and Information Policy, Department of State).

In 1990, the State Department Inspector General conducted a study of the strengths and weaknesses of the Bureau. While a number of Bureau policy initiatives were mentioned in the report, there was no specific mention of any work on data protection. The report cited internal problems such as inefficiency, stress, dissension. The Bureau was described as "a troubled bureau, with generally poor morale." *See generally* DEPARTMENT OF STATE OFFICE OF INSPECTOR GENERAL, REPORT OF INSPECTION — THE BUREAU OF INTERNATIONAL COMMUNICATIONS AND INFORMATION POLICY (Nov. 1990) (ISP/I-91-1).

information policy that from time to time has considered data protection issues when events abroad have warranted.

From the completion of the work on the OECD Guidelines until the issuance of the 1990 proposed European Community directive on data protection, it appears that the Bureau paid little attention to privacy matters. During this period, the data protection movement in Europe developed deeper roots while the attention of the Bureau was focused elsewhere. There is no evidence of continuing effort within the State Department to encourage American compliance with the Guidelines or to address routine international data protection issues.

One observer described the effect of the absence of an American presence at international data protection events during the last decade:

> There is nobody in the United States for the French data protection agency or the Canadian data protection agency or the German data protection agency to talk to. It is a considerable embarrassment to me as a student of American affairs to sit at these international meetings of data protection officials, which happen once a year, and there is an empty chair where the United States should be. If you had a data protection board, there would be somebody who could represent the interests of American companies and the American government in terms of these transfers of personal information that are taking place abroad. It is really an embarrassment. Often the American private sector is in the audience at these international meetings, but they can't speak; they are not officially represented; there is simply nobody carrying the can for the United States, and it is regrettable.[203]

At best, the Bureau of International Communications and Information Policy can be expected to react to major new international data protection initiatives and to represent U.S. interests in ongoing discussions about specific international agreements. For example, the Bureau has recently been engaged in discussions about the proposed EC data protection directive.[204] Otherwise, there is no evidence that the Bureau

---

203. *Data Protection, Computers, and Changing Information Practices: Hearings Before the Gov't. Information, Justice, and Agrigulture Subcomm. of the House Comm. on Gov't. Operations*, 101st Cong., 2d Sess. 11 (1990) (testimony of David Flaherty, Professor of History and Law, University of Western Ontario) [hereinafter *1990 House Data Protection Hearings*].

In 1991, the United States was formally represented — apparently for the first time — at the 13th annual International Data Protection & Privacy Commissioners Conference in Strasbourg, France. The activities of the U.S. delegation at this conference were controversial. *See* PRIVACY TIMES, at 1-6 (Oct. 17, 1991).

204. *See, e.g., US Criticizes EC Data Directive's Potential Burdens and Barriers*, 14 TRANSNAT'L DATA AND COMM. REP. 8 (Nov./Dec. 1991) (describing presentation of Ambassador Bradley P. Holmes, Coordinator, Bureau for International Communications and Information Policy, at the TELECOM 91 Economic Symposium). International meetings have been attended by representatives from a variety of U.S. agencies, including the Departments of State; Justice; Health and Human Services; Commerce; U.S. Trade Repre-

has the interest or ability to serve as a resource on data protection outside of any international negotiations. In the absence of pressure from specific international data protection negotiations that bear on U.S. interests, the Bureau does not appear to have any continuing concern or expertise about privacy matters.

V. CONCLUSION

Although the United States has never established a permanent data protection authority, the notion of such an authority remains a matter of discussion. Of the four major privacy studies identified in the last twenty years, three recommended the establishment of a permanent new federal agency with responsibilities including privacy policy. The fourth study, the earliest of the four, rejected the notion of a privacy regulatory agency, although it did recommend institutional change within one cabinet department to implement and oversee recommended new privacy policies. In addition, legislative proposals to establish a data protection authority continue to be introduced and discussed in Congress.

The failure of any of these proposals to move beyond the hearing stage is due to several factors. First, public concerns about privacy do not translate directly into support for an institutional remedy.[205] Specific privacy problems that have been identified in the popular press ("horror stories") tend to result in proposals for sectorial legislation rather than more generic solutions.[206] There is support for a data protection authority from consumer and professional organizations,[207] but it has been insufficient to sustain a serious legislative effort.

---

sentative; and the Office of Consumer Affairs. The role and continuing responsibilities of each of these agencies for general data protection matters is unclear.

205. A recent public opinion poll asked people to choose between three alternative models for protecting privacy. Thirty-one percent favored staying with the present system of specific laws, congressional oversight, and individual lawsuits; twenty-four percent favored the creation of a nonregulatory privacy protection board to research and publicize new controversies over privacy for public policy consideration; and forty-one percent favored the creation of a regulatory privacy protection commission with powers to issue enforceable rules for businesses handling consumer information. Thus, sixty-five percent favored the creation of some type of privacy entity. *See* LOUIS HARRIS & ASSOCIATES, EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE 106 (1990), *reprinted in 1991 House Data Protection Hearings*, *supra* note 50, at 290, 427.

206. *See, e.g.*, The Telephone Privacy Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991) (to protect residential telephone subscribers' privacy rights to avoid receiving telephone solicitations to which they object); Consumer Reporting Reform Act of 1992, H.R. 3596, 102d Cong., 2d Sess. (1992) (proposing amendments to the Fair Credit Reporting Act).

207. *See, e.g.*, *1990 House Data Protection Hearings*, *supra* note 205, at 105 (testimony of Marc Rotenberg, Director, Washington Office, Computer Professionals for Social Responsibility).

Second, it is difficult to create a new administrative agency in the face of opposition from the business community. This has been especially true during the strong anti-regulatory period in the 1980s. Those industries that maintain large quantities of personal information as part of their operations have not expressed support for a data protection board. While there is some recognition that a board could serve a useful role,[208] there is a greater fear that a board would investigate or regulate industry.[209] Opposition from the business community is typically couched in anti-regulatory terms, even though the legislation proposed in recent years would create a board without any regulatory authority over the private sector.

Third, the restrictions on the transborder flow of personal information that are being considered in Europe[210] have not yet impinged seriously on American businesses. Thus, neither the American business community nor the American government has felt the need for a definitive response. Also, the pressures that exist in other countries to prevent data on their citizens from being transferred to other locations, where the data will be unprotected, are absent in the United States. No one has expressed concern that information on American citizens will be sent abroad and misused.

Of the three existing agencies that have had general domestic or international privacy policy responsibilities, only the Office of Management and Budget appears to have ongoing interest in privacy, albeit at the lowest possible level of activity. The other two agencies maintain no significant privacy expertise and, at best, address privacy matters only when there are significant international treaties or agreements

---

208. *See 1991 House Data Protection Hearings, supra* note 50, at 6, 23 (testimony of John Baker, Senior Vice President, Equifax Inc.) ("[T]he board's focus on the interpretation and harmonization of foreign privacy laws and the laws of the United States is extremely positive.").

209. *Id.* at 22-3.

> [Data protection board legislation] runs the risk that the proposed board will be nothing more than a worrisome venture. By vesting the proposed board with the authority to investigate complaints about alleged violations of data protection rights — as well as the power to compel the testimony of witnesses and the production of books and records — the board could easily be used to sensationalize or simply harass.

Id.

In addition, Richard Barton, Senior Vice President of Government Affairs, Direct Marketing Association has expressed concern:

> [W]e have been very skeptical about the creation of a permanent bureaucracy, so to speak, in this area, largely because of the experience of some of our members in Great Britain. The regulations have gotten so onerous that they are threatening what some people would call the legitimate exercise of business.

1990 House Data Protection Hearings, supra note 205, at 78.

210. *See supra* note 6.

pending. None of these agencies appear to offer routine assistance to individuals, businesses, or foreign countries facing privacy problems.

Each of these agencies is large and has many other functions assigned to it. Since the end of the Carter privacy initiative and the termination of the OECD Guideline compliance effort in the early 1980s,[211] privacy has become or remained as a very low priority issue. There are no bureaucratic rewards for attempting to give privacy a higher visibility. This is due to a lack of presidential leadership and to the factors listed above that have prevented data protection legislation from progressing.

In addition, the agencies have no effective tools that would permit them easily to respond to the domestic and international pressures that do exist. The limitations of the existing American privacy policy structure become clearer when current international data protection trends are considered. An important feature of "second generation"[212] data protection laws is the emphasis on industry codes of conduct. The codes may be developed by industry with the assistance of the data protection authority. The codes become part of the formal regulatory scheme when formally approved by the data protection authority.[213] Professor Spiros Simitis describes codes of conduct as "a welcome complement of a sectorial regulation whenever an additional specification appears necessary, but the limits of legislative intervention have been reached."[214]

Whether industrial privacy codes are appropriate for the United States is an open question. The point is that use of industry codes with formal government approval is not an option that is available at this time in the United States. None of the agencies with privacy responsibilities has the authority to assist in the development, approval, and enforcement of industry codes.

The response of the United States to privacy issues remains just as fragmented, incomplete, and discontinuous as it has been in the past. There is no U.S. data protection authority in law or in practice.

---

211. *See supra* notes 159-190 and accompanying text.

212. *See supra* note 122.

213. *See* SIMITIS, *supra* note 7, at 23-24.

214. *Id.* at 24.