Order Code RL30671

Personal Privacy Protection: The Legislative Response

Updated May 24, 2001

Harold C. Relyea
Specialist in American National Government
Government and Finance Division

Personal Privacy Protection: The Legislative Response

Summary

An expectation of personal privacy seemingly has long prevailed in American culture and society. The Bill of Rights gave constitutional recognition to privacy expectations in the First Amendment, including the right not to have to speak, privacy of opinion, freedom of association, and the right of anonymous or pseudonymous expression; the Third Amendment, prohibiting the quartering of troops in private homes during peacetime without the owner's consent; the Fourth Amendment, guaranteeing personal security against unwarranted searches and seizures; and the Fifth Amendment, specifying the privilege against self-incrimination. Although there may be some ambiguity about all of the facets of personal privacy, the American people, particularly during the latter half of the 20th century, have increasingly turned to Congress to respond to their concerns regarding perceived threats to, or the loss of, personal privacy. These responses, which have significantly contributed to the policy development of the personal privacy concept, are reviewed here, and current personal privacy issues receiving legislative treatment are identified and discussed. These include developments regarding a comprehensive privacy review, Privacy Act amendments, banking and financial transactions, medical records, online communication, and electronic commerce. This report will be updated as events warrant.

Contents

Personal Privacy Protection: The Legislative Response

An expectation of personal privacy seemingly has long prevailed in American culture and society. Some may regard personal privacy as one of the "Blessings of Liberty" mentioned in the preamble of the Constitution. Others might trace its roots to the "right of the people to be secure in their persons, houses, papers, and effects" given expression in the Fourth Amendment of that document. Although there may be some ambiguity about all of the facets of personal privacy, the American people, particularly during the latter half of the 20th century, have increasingly turned to Congress to respond to their concerns regarding perceived threats to, or the loss of, personal privacy. These responses, which have significantly contributed to the policy development of the personal privacy concept, are reviewed here, and current personal privacy issues receiving legislative treatment are identified and discussed.

An Evolving Value

The concept of privacy has probably long been a value of humankind. As a sentiment—the wish not to be intruded upon—it very likely predates recorded history and was experienced before it was given a name. In the thinking of the influential 17th century British philosopher John Locke, privacy was one of the presocietal or "natural rights" which was preserved when individuals, by social contract, agreed to form a society. Furthermore, when society, by a second social contract, agreed to form a government, privacy was one of the rights the government was expected to preserve and protect. When a Bill of Rights was appended to the American version of Locke's second contract, it gave constitutional recognition to privacy expectations in the First Amendment, including the right not to have to speak, privacy of opinion, freedom of association, and the right of anonymous or pseudonymous expression; the Third Amendment, prohibiting the quartering of troops in private homes during peacetime without the owner's consent; the Fourth Amendment, guaranteeing personal security against unwarranted searches and seizures; and the Fifth Amendment, specifying the privilege against self-incrimination.[1] In a landmark 1965 decision, the Supreme Court viewed these and the Ninth Amendment as being the sources of a penumbral right of privacy.[2]

In his seminal study of privacy, attorney Alan F. Westin has written that American society, prior to the Civil War, "had a thorough and effective set of rules with which to protect individual and group privacy from the means of compulsory

---

[1]Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1970), pp. 330-333.

[2]*Griswold* v. *Connecticut*, 381 U.S. 479 (1965); see R. H. Clark, "Constitutional Sources of the Penumbral Right to Privacy," *Villanova Law Review*, vol. 19, June 1974, pp. 833-884.

disclosure and physical surveillance known in that era."[3] Toward the end of the 19th century, new technology—the telephone, the microphone and dictograph recorder, and improved cameras—presented major new challenges to privacy protection. Consequently, understandings of privacy became a bit desperate. Judge Thomas Cooley, in his influential treatise on torts, described privacy as the inalienable and natural "right to be let alone."[4] This view was given more popular expression by Samuel D. Warren and Louis D. Brandeis in their now famous 1890 *Harvard Law Review* article on the right to privacy.[5] However, as a British study committee observed in 1972, this perspective "turns out on closer examination to go so far beyond any right which the individual living in an organized society could reasonably claim, that it would be useless as a basis for the granting of legal protection. Any law which proclaimed this as a general right," the committee reported, "would have to qualify the right in so many ways that the generality of the concept would be destroyed."[6]

Nonetheless, new technology would continue to threaten and weaken personal privacy. In 1956, sociologist Edward A. Shils described privacy as "the voluntary withholding of information reinforced by a willing indifference."[7] By that time, however, it had become quite apparent to many that it was increasingly difficult and, in some cases, probably impossible to voluntarily withhold personal information any longer because there were elements of society which had obviously forsaken a willing indifference to such desires.

A few years later, Congress began to probe a variety of privacy issues. For example, in 1965, one subcommittee of the Senate Committee on the Judiciary began omnibus hearings on the invasion of privacy by federal agencies,[8] while a companion subcommittee examined psychological testing procedures and the rights of federal employees.[9] The following year, this latter panel explored the privacy rights of federal

---

[3]Westin, *Privacy and Freedom*, pp. 337-338.

[4]Thomas M. Cooley, *A Treatise on the Law of Torts, or the Wrongs Which Arise Independent of Contract* (Chicago: Callaghan and Company, 1888), p. 29.

[5]Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, vol. 4, Dec. 15, 1890, pp. 193-220.

[6]United Kingdom, Committee on Privacy, *Report of the Committee on Privacy* (London: Her Majesty's Stationery Office, 1972), p. 10. The committee was chaired by Kenneth Younger.

[7]Edward A. Shils, *The Torment of Secrecy* (New York: Free Press, 1956), p. 26.

[8]See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Invasions of Privacy*, hearings, 89th Cong., 1st and 2nd sess., 1965-1966 (Washington: GPO, 1965-1967), 6 parts.

[9]See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Psychological Tests and Constitutional Rights*, hearings, 89th Cong., 1st sess., June 7-10, 1965 (Washington: GPO, 1966).

civil servants.[10] Another subcommittee began major hearings in 1967 concerning privacy protection by prohibiting wire interception and eavesdropping.[11] It also scrutinized computer privacy that same year.[12] In 1969, Senate subcommittee attention was given to privacy, the census, and federal questionnaires.[13] In 1971, omnibus hearings were held on federal databanks, computers, and the Bill of Rights.[14]

In the House, the Committee on Government Operations (now Government Reform) chartered a Special Subcommittee on Invasion of Privacy in 1965.[15] It launched a general inquiry that year,[16] then focused upon the computer and invasion of privacy the following year,[17] and was a major critic of a proposed national databank under discussion in the 1960s.[18] In 1968, a subcommittee of the House Committee on Post Office and Civil Service examined privacy and the rights of federal employees.[19] That same year, the special subcommittee explored the practices of commercial credit bureaus and their privacy implications.[20] In 1972, a subcommittee

---

[10]See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Privacy and the Rights of Federal Employees*, hearings, 89th Cong., 2nd sess., Oct. 3-5, 1966 (Washington: GPO, 1966).

[11]See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Right of Privacy Act of 1967*, hearings, 90th Cong., 1st sess., Mar. 20; Apr. 4-6, 19-21; May 17-19, 1967 (Washington: GPO, 1967), 2 parts.

[12]See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Computer Privacy*, hearings, 90th Cong., 1st and 2nd sess., Mar. 14-15, 1967; Feb. 6, 1968 (Washington: GPO, 1967-1968), 2 parts.

[13]See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional *Rights, Privacy, the Census and Federal Questionnaires*, hearings, 91st Cong., 1st sess., Apr. 24-25; May 2; July 1, 1969 (Washington: GPO, 1969).

[14]See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Federal Data Banks, Computers and the Bill of Rights*, hearings, 92nd Cong., 1st sess., Feb. 23-25; Mar. 2-4, 9-11, 15, 17, 1971 (Washington: GPO, 1971), 2 parts.

[15]See Morris S. Ogul, *Congress Oversees the Bureaucracy* (Pittsburgh: University of Pittsburgh Press, 1976), pp. 92-128.

[16]See U.S. Congress, House Committee on Government Operations, *Special Inquiry on Invasion of Privacy*, hearing, 89th Cong., 1st sess., June 2-4, 7, 23; Sept. 23, 1965; May 24, 1966 (Washington: GPO, 1966), 2 parts.

[17]See U.S. Congress, House Committee on Government Operations, *The Computer and Invasion of Privacy*, hearing, 89th Cong., 2nd sess., June 26-28, 1966 (Washington: GPO, 1966).

[18]See U.S. Congress, House Committee on Government Operations, *Privacy and the National Data Bank Concept*, 90th Cong., 2nd sess., H. Rept. 1842 (Washington: GPO, 1968).

[19]See U.S. Congress, House Committee on Post Office and Civil Service, *Privacy and the Rights of Federal Employees*, hearings, 90th Cong., 2nd sess., June 13, 18, 27; July 2, 9-12, 16-17, 1968 (Washington: GPO, 1968).

[20]See U.S. Congress, House Committee on Government Operations, *Commercial Credit Bureaus*, hearings, 90th Cong., 2nd sess., Mar. 12-14, 1968 (Washington: GPO, 1968).

on the House Committee on the Judiciary held hearings on the security and privacy of criminal arrest records.[21]

In 1968, at the urging of Alan F. Westin, the Russell Sage Foundation funded the Project on Computer Databanks of the Computer Science and Engineering Board, National Academy of Sciences. This undertaking, directed by Westin, examined the use of computers by government and private organizations for collecting, processing, and exchanging information about individuals; the effect of such computer use on the way organizations utilize records in order to make judgements about the rights, benefits, and opportunities of individuals; and the impact of computerized records systems on privacy and due process rules. In the final report, published in 1972, the Project found that "computer usage has not created the revolutionary new powers of data surveillance predicted by some commentators"; that some important increases in the efficiency of organizational recordkeeping resulted from computerization; and that, "even where these increases in efficiency are taking place, organizational policies which affect individual rights are still generally following the precomputer patterns in each field of record-keeping."[22]

The report, however, was not satisfied with a pattern of organizations merely adapting their computerized systems of recordkeeping to the existing civil liberties rules in their particular fields. Thus, it recommended that compulsory data collection be limited "so that matters that ought not to be considered in making decisions about individuals do not become part of the formal records at all"; that individuals be given greater rights of access to records maintained about them; and that "new rules for data sharing and confidentiality ... be fashioned."[23]

Early in 1972, Secretary of Health, Education, and Welfare Elliot L. Richardson established the Secretary's Advisory Committee on Automated Personal Data Systems. Headed by Willis H. Ware of the Rand Corporation, the panel was asked to analyze and make recommendations about four areas of interest.

- Harmful consequences that may result from using automated personal data systems;
- Safeguards that might protect against potentially harmful consequences that may result from using automated personal data systems;
- Measures that might afford redress for any such harmful consequences; and

---

[21]See U.S. Congress, House Committee on the Judiciary, *Security and Privacy of Criminal Arrest Records*, hearings, 92nd Cong., 2nd sess., Mar. 16, 22-23; Apr. 13, 26, 1972 (Washington: GPO, 1972).

[22]National Academy of Sciences, Computer Science and Engineering Board, Project on Computer Databanks, *Databanks in a Free Society*, Report of the Project on Computer Databanks (New York: Quadrangle Books, 1972), p. 341.

[23]*Ibid.*, pp. 348-349.

- Policy and practice relating to the issuance and use of individuals' Social Security numbers.[24]

In its final report, issued in July 1973, the advisory committee recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems." Such a code, in the view of the panel, should "define 'fair information practice' as adherence to specified safeguard requirements"; "prohibit violation of any safeguard requirements as an 'unfair information practice'"; "provide that an unfair information practice be subject to both civil and criminal penalties"; "provide for injunctions to prevent violations of any safeguard requirement"; "give individuals the right to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions"; and "also provide for recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful lawsuits."[25]

Legislating Privacy Protection

During the past three decades, Congress has legislated privacy protections in various policy areas and has initiated two broad privacy studies with a view to producing both findings and policy recommendations. Major developments resulting from these initiatives are summarized below.

Fair Credit Reporting Act. Before the HEW Secretary's Advisory Committee on Automated Personal Data Systems issued its July 1973 final report recommending a Code of Fair Information Practice, Congress experimented with such a set of ground rules when it made an initial effort at legislating a new kind of privacy protection with the Fair Credit Reporting Act of 1970.[26] This statute regulates the collection and dissemination of personal information by consumer reporting agencies and persons, including corporations, who regularly procure or cause to be prepared investigative consumer reports on any individual for use by a third party. Among its provisions, the new law authorized the subject of a consumer report to request of the preparer agency details concerning the nature and scope of all information in its files regarding that individual, the identity of the sources of the information, and the name of any recipient of the information. In addition, the report subject might seek to correct or otherwise amend the preparer agency's information by providing supplemental data.

Crime Control Act. When legislating the Crime Control Act of 1973, Congress prohibited state agencies receiving law enforcement assistance funds pursuant to the statute and federal personnel from making unauthorized disclosures of personally identifiable criminal history research or statistical information. It also permitted "an individual who believes that criminal history information concerning him

---

[24]U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington: July 1973), p. ix.

[25]*Ibid.*, pp. xxiii and 50.

[26]84 Stat. 1128; 15 U.S.C. 1681 *et seq.*

contained in an automated system is inaccurate, incomplete, or maintained in violation of this [law] ... to review such information and to obtain a copy of it for the purpose of challenge or correction."[27]

Privacy Act. With the Privacy Act of 1974, Congress addressed several aspects of privacy protection.[28] First, it sustained some traditional major privacy principles. For example, an agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."[29]

Second, similar to the Fair Credit Reporting Act, the Privacy Act provides an individual who is a citizen of the United States, or an alien lawfully admitted for permanent residence, with access and emendation arrangements for records maintained on him or her by most, but not all, federal agencies. General exemptions in this regard are provided for systems of records maintained by the Central Intelligence Agency and federal criminal law enforcement agencies.

Third, the statute embodies a number of principles of fair information practice recommended by the HEW Secretary's Advisory Committee on Automated Personal Data Systems. For example, it sets certain conditions concerning the disclosure of personally identifiable information; prescribes requirements for the accounting of certain disclosures of such information; requires agencies to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"; requires agencies to specify their authority and purposes for collecting personally identifiable information from an individual; requires agencies to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination"; and provides civil and criminal enforcement arrangements.

Recently, in a survey of online privacy protections at federal Web sites, GAO found that 23 of 70 agencies had disclosed personal information gathered from their Web sites to third parties, mostly other agencies. However, at least four agencies were discovered to be sharing such information with private entities—trade organizations, bilateral development banks, product manufacturers, distributors, and retailers. The offending agencies were not identified by GAO. Responding to these findings, some privacy advocates called for updating the Privacy Act to specify privacy protections for Internet visitors to agency Web sites, while others urged better oversight and enforcement of the statute.[30]

---

[27]87 Stat. 197 at 215-216; 42 U.S.C. 3789g.

[28]88 Stat. 1896; 5 U.S.C. 552a.

[29]5 U.S.C. 552a(e)(7).

[30]Lance Gay, "GAO Finds Agencies Sharing Data of On-line Visitors," *Washington Times*, Sept. 8, 2000, p. A3; U.S. General Accounting Office, *Internet Privacy: Agencies' Efforts* (continued...)

When completing action on the FY2001 appropriations legislation for the Department of Transportation and related agencies, House and Senate conferees included a Web site privacy provision. Section 501 of the conference committee version of the bill (H.R. 4475) prohibits funds appropriated by the Department of the Treasury and related agencies section of the legislation to be used by those entities (1) to collect, review, or create any aggregate list, derived by any means, that includes the collection of any personally identifiable information relating to an individual's access to, or use of, any federal government Internet site of the agency, or (2) to enter into any agreement with a third party, including another government agency, to collect, review, or obtain any aggregate list, derived from any means, that includes the collection of any personally identifiable information relating to an individual's access to or use of any nongovernmental Internet site. These limitations do not apply to any record of aggregate data that does not identify particular persons; any voluntary submission of personally identifiable information; any action taken for law enforcement, regulatory, or supervisory purposes, in accordance with applicable law; and any action that is a system security action taken by the operator of an Internet site and is necessarily incident to the rendition of the Internet site services or to the protection of the rights or property of the provider of the Internet site.[31]

The first limitation may be viewed as a response to a June 2000 press revelation that the National Drug Control Policy Office was secretly tracking visitors to its Web site through the use of "cookies."[32] In response, a June 22, 2000, OMB memorandum to the heads of all executive departments and agencies indicated that "'cookies' should not be used at Federal web sites, or by contractors when operating web sites on behalf of agencies, unless, in addition to clear and conspicuous notice, the following conditions are met: a compelling need to gather the data on the site; appropriate and publicly disclosed privacy safeguards for handling of information derived from 'cookies'; and personal approval by the head of the agency." The second limitation may be regarded as a response to the September GAO report indicating that 23 agencies had disclosed personal information gathered from their Web sites to third parties. President Clinton signed the legislation into law on October 23, 2000.[33]

Two days before the President's action, press disclosures revealed that a GAO followup study contended that 13 federal agencies had ignored the OMB June 22 memorandum prohibiting the tracking of visitors to government Web sites. An appended letter from the OMB deputy director for management defended agency use of so-called "session cookies,"which, the letter said, facilitate transactions at the website and are not banned by OMB. Session cookies last only as long as one is

---

[30](...continued)
to Implement OMB's Privacy Policy, GAO Report GAO/GGD-00-191 (Washington: September 2000).

[31]See *Congressional Record*, daily edition, vol. 146, Oct. 5, 2000, pp. H8935-H8936, H8980.

[32]See John F. Harris and John Schwartz, "Anti-Drug Web Site Tracks Visitors," *Washington Post*, June 22, 2000, p. A23; Lance Gay, "White House Uses Drug-Message Site to Track Inquiries," *Washington Times*, June 21, 2000, p. A3.

[33]P.L. 106-346.

visiting the Web site. Clearly prohibited are "persistent cookies," which may track Web habits for long periods of time, and the dissemination of a person's information to a private company. GAO found seven agencies engaging in one or both of these activities.[34]

In mid-April 2001, Senator Fred Thompson (R-TN), chairman of the Senate Committee on Governmental Affairs, released the preliminary findings of agency Inspectors General who were required by a provision of the Treasury-Postal title of the Consolidated Appropriations Act of 2001 to report on how their agencies collect and review personal information on their Web sites.[35] In the aftermath of these controversies, issues remain concerning the prohibition of agency use of all or certain kinds of "cookies," the conditions to be satisfied in the event certain kinds of "cookies" are used, and if all or certain agencies are to be subject to the prescribed "cookies" use policy.

Privacy Study Commission. The statute also mandated the Privacy Protection Study Commission, a temporary, seven-member panel tasked 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."[36] The commission was 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 [such] organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and 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."[37]

The commission began operations in early June 1975 under the leadership of chairman David F. Linowes, a University of Illinois political economist, educator, and corporate executive, and vice chairman Willis H. Ware, the Rand Corporation research scientist who had headed the HEW Secretary's Advisory Committee on Automated Personal Data Systems.[38] Two years later, in July 1977, the final report of the panel, offering 162 recommendations, was submitted to the President and

---

[34]Associated Press, "U.S. Agencies Ignore Ban, Track Visitors to Web Sites," *Washington Times*, Oct. 22, 2000, p. C3; D. Ian Hopper, "Agencies Track Online Visitors Despite Rules," *Washington Post*, Oct. 22, 2000, p. A13; D. Ian Hopper, "Renewed Ban on U.S. Web 'Cookies'," *Washington Post*, Oct. 24, 2000, p. A25; U.S. General Accounting Office, *Internet Privacy: Federal Agency Use of Cookies*, GAO Letter GAO-01-147R (Washington: Oct. 20, 2000).

[35]P.L. 106-554, sec. 646.

[36]88 Stat. 1906.

[37]*Ibid.*

[38]See David F. Linowes, "The U.S. Privacy Protection Commission," *American Behavioral Scientist*, vol. 26, May-June 1983, pp. 577-590.

Congress.[39] In general, the commission urged the establishment of a permanent, independent entity within the federal government to monitor, investigate, evaluate, advise, and offer policy recommendations concerning personal privacy matters; better regulation of the use of mailing lists for commercial purposes; adherence to principles of fair information practice by employers; limited government access to personal records held by a private sector recordkeeper through adherence to recognized legal processes; and improved privacy protection for educational records. The panel also recommended the adoption of legislation to apply principles of fair information practice, such as those found in the Privacy Act, to personal information collected and managed by the consumer credit, banking, insurance, and medical care sectors of the U.S. economy.

Congressional response to the commission's report was largely positive, some 200 bills incorporating its recommendations being introduced. However, a concerted effort to enact legislation applying principles of fair information practice to personal information collected and managed by the insurance and medical care industries was stalemated into the final days of the 96th Congress. The opposition was sufficient to discourage a return to such legislative efforts for several years.

President Jimmy Carter appointed a cabinet committee to study the commission's recommendations, and received additional evaluations and supplemental recommendations from an interagency task force, resulting in a package of national privacy policy proposals which was sent to Congress on April 2, 1979.[40] While these developments were underway, the Carter Administration worked with Congress to produce the Right to Financial Privacy Act of 1978, discussed below. Congress largely deferred action on the President's 1979 package of privacy proposals until 1981, but this effort became moot with President Carter's 1980 electoral defeat for a second term.

Federal Paperwork Commission. In 1974, Congress also established a temporary, 14-member Commission on Federal Paperwork, giving it a broad mandate to consider a variety of aspects of the collection, processing, dissemination, and management of federal information, including "the ways in which policies and practices relating to the maintenance of confidentiality of information impact upon Federal information activities."[41] The panel was cochaired by Representative Frank Horton (R-NY) and Senator Thomas J. McIntyre (D-NH); conducted its work largely in parallel with the Privacy Protection Study Commission; and produced 36 topical reports, with recommendations, as well as a final summary report of October 3, 1977.[42] One of these reports was devoted to confidentiality and privacy. Issued July

---

[39]U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington: GPO, 1977).

[40]See U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, *Public Papers of the Presidents of the United States: Jimmy Carter, 1979* (Washington: GPO, 1980), pp. 581-587.

[41]88 Stat. 1789.

[42]U.S. Commission on Federal Paperwork, *Final Summary Report: A Report of the* (continued...)

29, 1977, it offered 12 recommendations.[43] Although a House subcommittee devoted a hearing to the report, no immediate action was taken on its recommendations.[44]

Subsequently, however, a recommended new organization to centralize and coordinate existing information management functions within the executive branch, and proposed limits on the use of statistical information or disclosing it in identifiable form without the consent of the data subject, were realized in the Paperwork Reduction Act of 1980.[45] The statute established a new Office of Information and Regulatory Affairs within the Office of Management and Budget (OMB) to assist the OMB director with the governmentwide information coordination and guidance functions assigned to him by the act. Examples of these functions include the OMB director's broad responsibilities for statistical policy and coordination, such as:

> (1) developing long range plans for the improved performance of Federal statistical activities and programs; (2) coordinating, through the review of budget proposals and as otherwise provided in this [statute], the functions of the Federal Government with respect to gathering, interpreting, and disseminating statistics and statistical information; (3) developing and implementing Government-wide policies, principles, standards, and guidelines concerning statistical collection procedures and methods, statistical data classifications, and statistical information presentation and dissemination; and (4) evaluating statistical program performance and agency compliance with Government-wide policies, principles, standards, and guidelines.[46]

Indicating that one of the purposes of the Paperwork Reduction Act was "to ensure that the collection, maintenance, use and dissemination of information by the Federal Government is consistent with applicable laws relating to confidentiality, including ... the Privacy Act,"[47] the statute assigned the OMB director the following privacy functions: "(1) developing and implementing policies, principles, standards, and guidelines on information disclosure and confidentiality, and on safeguarding the security of information collected or maintained by or on behalf of agencies; (2) providing agencies with advice and guidance about information security, restriction, exchange, and disclosure; and (3) monitoring compliance with [the Privacy Act] and related information management laws."[48] These privacy functions would be expanded, and privacy responsibilities would be specified for the federal agencies, in

---

[42](...continued)
Commission on Federal Paperwork (Washington: GPO, 1977).

[43]U.S. Commission on Federal Paperwork, *Confidentiality and Privacy: A Report of the Commission on Federal Paperwork* (Washington: GPO, 1977), pp. 139-175.

[44]U.S. Congress, House Committee on Government Operations, *Privacy and Confidentiality Report and Final Recommendations of the Commission on Federal Paperwork*, hearing, 95th Cong., 1st sess., Oct. 17, 1977 (Washington: GPO, 1978).

[45]94 Stat. 2812; 44 U.S.C. 3501 *et seq.*

[46]94 Stat. 2816.

[47]94 Stat. 2813.

[48]94 Stat. 2816.

a 1995 recodification of the act.[49] In 1988, amendments governing computer matches of personal information by government agencies, discussed below, were enacted.[50]

Family Educational Rights and Privacy Act. Another privacy statute enacted by the 93rd Congress in 1974 was the Family Educational Rights and Privacy Act (FERPA), also known as the Buckley Amendment in reference to its sponsor, Senator James L. Buckley (C/R-NY), who offered the proposal as a floor amendment to the General Education Provisions Act during Senate consideration of the Education Amendments of 1974.[51] As originally approved, the FERPA provided the parents of minor children, and students over 18 years of age, the right to inspect, correct, amend, and control the disclosure of information in the education records of educational agencies or institutions receiving federal funds. It also obliged these institutions to inform parents and students of their rights, and to establish policies and procedures for the exercise of such rights.

In its 1977 final report, the Privacy Protection Study Commission assessed the provisions and implementation of the FERPA, and offered several recommendations for clarifying and strengthening the statute.[52] Prior to 1994, Congress amended the FERPA with technical modifications on a few occasions; substantive amendments were effected, primarily, with the Improving America's Schools Act of 1994[53] and, less so, with the Higher Education Amendments of 1998.[54] These included provisions explicitly prohibiting the allocation of federal funds to any state educational agency or institution "that has a policy of denying, or effectively prevents, the parents of students the right to inspect and review the education records maintained by the State ... on their children"; permitting access to student records by "State and local officials or authorities to whom such information is specifically allowed to be reported or disclosed pursuant to State statute ... if the allowed reporting or disclosure concerns the juvenile justice system"; permitting the disclosure of student records to "the entity or person designated in a Federal grand jury subpoena" or in other subpoenas issued "for a law enforcement purpose"; prohibiting an educational agency or institution from releasing students records, "for a period of not less than five years," to a third party that violated the FERPA requirements governing access to such records; and clarifying that nothing in the FERPA prohibits an educational agency or institution from placing relevant disciplinary information in a student's records or revealing that information to teachers or other school officials "who have legitimate educational interests in the behavior of the student." According to one estimate, "these amendments [were] apparently intended to expand the coverage of FERPA, strengthen incentives to comply with the Act, eliminate schools' and institutions' dilemmas about restricting access to records that are subpoenaed, and prevent the Act

---

[49]109 Stat. 163; 44 U.S.C. 3501 *et seq*.

[50]102 Stat. 2507.

[51]88 Stat. 571; 20 U.S.C. 1232g.

[52]U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society*, pp. 393-444.

[53]108 Stat. 3924.

[54]112 Stat. 1835.

from interfering with educational professionals' need to know about students' behavior."[55]

Financial Privacy Act. As noted above, the Right to Financial Privacy Act of 1978 (RFPA) grew out of the concerns of the Privacy Protection Study Commission for limiting government access to personal records held by a private sector recordkeeper through adherence to recognized legal processes. It was a product of the joint efforts of the Carter Administration and the 95th Congress. The commission's concerns and the cooperative legislative efforts of the two branches to enact the RFPA, as the following contemporaneous comments reflect, were fueled by several recent developments.

> Prior to 1970, there was little need for concern about the privacy of financial records. Bank records were considered confidential by bank officials and records were kept only for internal bank use. This practice was challenged upon the passage of the Bank Secrecy Act of 1970 [84 Stat. 1114]. This legislation was designed to aid government agencies in their investigations of criminal, tax, and regulatory matters. The Bank Secrecy Act requires, *inter alia*, depository institutions to maintain duplicate records of almost all customer transactions. In particular, it requires that checks and other charges in excess of $100 be microfilmed and retained for five years. Banks have found, however, that sorting checks over $99 is so expensive that it is easier and cheaper to microfilm all checks. Concomitant with this development has been an increase in personal checking accounts and an expansion of commercial banking into the open-end credit market. Commercial banks, by complying with the recordkeeping requirements of the Bank Secrecy Act, now possess information about the activities and relationships of millions of people. As a result, the amount of financial and personal information available to the government has been commensurately expanded.
>
> Improved technology has exacerbated this threat to financial privacy. For example, the use of Electronic Funds Transfer services (EFT) promises to increase the amount of personal information available to financial institutions. These services involve the processing and documentation of deposits, withdrawals, and transfers of money with the help of computers and telecommunications. One type of EFT services, point-of-sale services, allows an individual to use funds on deposit without having to visit the financial institution and without having to write a check. The development of point-of-sale services will have several ramifications. First, the expansion of this service will result in an increase in the amount and detail of personal information recorded by financial institutions as it is likely that accounting and administrative information will accompany periodic payment. Second, financial records will become more centralized and accessible. Third, financial records will contain information not usually considered payment data, such as information concerning the purpose of the transaction.
>
> These developments served to increase public concern over privacy during the 1970s. In addition, the Watergate investigations focused attention on privacy

---

[55] U.S. Library of Congress, Congressional Research Service, *Family Educational Rights and Privacy Act: P.L. 103-382 Amendments*, by Richard N. Apling, CRS Report 94-980 EPW (Washington: Dec. 7, 1994), p. 2.

> interests by disclosing that government officials used information from private financial records to conduct illegitimate investigations of certain individuals.[56]

Then, amidst this atmosphere and the deliberations of the Privacy Protection Study Commission, the Supreme Court's April 21, 1976, decision in *United States* v. *Miller* burst.[57] The respondent, Mitchell Miller, had been convicted of possessing an unregistered still, engaging in the business of a distiller without giving bond and with the intent to defraud the government of whiskey tax, possessing 175 gallons of whiskey for which no taxes had been paid, and conspiring to defraud the United States of tax revenues. Prior to his trial, Miller had moved to suppress copies of checks and other bank records obtained by means of allegedly defective subpoenas *duces tecum* issued by the United States Attorney, not a court, and served on two banks where he had accounts. The banks had maintained the records in compliance with the requirements of the Bank Secrecy Act. The trial court overruled the motion to suppress, and the evidence was admitted. The United States Court of Appeals for the Fifth Circuit reversed the decision on the ground that a depositor's Fourth Amendment rights are violated when bank records, maintained pursuant to the Bank Secrecy Act, are obtained by means of a defective subpoena, and held that any evidence so obtained must be suppressed. However, the court rejected Miller's contention that the provisions of the Bank Secrecy Act requiring banks to microfilm all checks violated a depositor's Fourth Amendment right to be free from unreasonable searches and seizures.[58]

Affirmance of the appellate court's ruling seemingly would have established a constitutional right to financial privacy under the Fourth Amendment. However, the Supreme Court, in its 7-2 decision, held:

- The subpoenaed materials were business records of the banks, not respondent's private papers.

- There is no legitimate "expectation of privacy" in the contents of the original checks and deposit slips, since the checks are not confidential communications but negotiable instruments to be used in commercial transactions, and all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities. The [Bank Secrecy] Act recordkeeping requirements do not alter these considerations so as to create a protectable Fourth Amendment interest of a bank depositor in the bank's records of his account.

- Issuance of a subpoena to a third party does not violate a defendant's rights, even if a criminal prosecution is contemplated at the time the subpoena is issued.

---

[56]Lorena Kern Davitt, "The Right to Financial Privacy Act: New Protection for Financial Records," *Fordham Urban Law Journal*, vol. 8, 1979-1980, pp. 597-599.

[57]*United States* v. *Miller*, 425 U.S. 435 (1976).

[58]500 F.2d 751 (5th Cir. 1974).

- Access to bank records under the [Bank Secrecy] Act is to be controlled by "existing legal process." That does not mean that greater judicial scrutiny, equivalent to that required for a search warrant, is necessary when a subpoena is used to obtain a depositor's bank records.[59]

In brief, the *Miller* decision effectively gave the federal government unrestricted access to a bank customer's or depositor's financial records through administrative subpoena. The Privacy Protection Study Commission disagreed with the breadth of the *Miller* decision and proffered corrective recommendations.[60] From these origins came the Right to Financial Privacy Act (RFPA). Enacted as Title XI of the far-ranging Financial Institutions Regulatory and Interest Rate Control Act of 1978, the RFPA prohibits any federal agency from obtaining access to financial records of the customers of a financial institution, except when access is required in connection with a legitimate law enforcement inquiry, unless one of five specified procedures is followed: (1) customer authorization; (2) administrative summons or subpoena, which is authorized by law, judicially enforceable, used in connection with a legitimate law enforcement inquiry, and with advance notice to the customer; (3) search warrant, which meets the existing "probable cause" standard for the issuance of such instruments and with advance notice to the customer; (4) judicial subpoena; or (5) formal written request, which is designed for federal agencies which do not have administrative summons or subpoena authority.[61]

The concept of "financial institutions" is broadly defined to include all banking-type and consumer finance businesses, as well as credit unions and companies issuing credit cards, located within the United States or its territories. The term "customer" is narrowly defined to include only natural persons or partnerships of five or fewer individuals who utilize a financial institution in connection with an account maintained under the individual's or partnership's name. "Financial records" is broadly defined to mean "an original copy of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution."

The RFPA provides procedures which a customer may follow to challenge an attempt by a government agency to obtain access to his or her financial records under the terms of the statute. A civil penalties provision prescribes damage awards to customers when federal agencies or financial institutions are found to be obtaining or disclosing financial records or information in violation of the RFPA.

Privacy Protection Act. Congress enacted the Privacy Protection Act of 1980 to protect a First Amendment right of privacy threatened by police searches. The statute was prompted by a Supreme Court ruling involving a Stanford University newspaper complaint. On April 12, 1971, four local police officers, armed with a search warrant, conducted a no-notice, surprise search of the offices of the *Stanford Daily*, a student newspaper published at Stanford University. They were seeking

---

[59]425 U.S. 435-436.

[60]See U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society*, pp. 362-373.

[61]92 Stat. 3697; 12 U.S.C. 3401 *et seq*.

unpublished photographs which they believed would assist them in identifying the assailants of fellow officers injured at a recent demonstration before the Stanford University Hospital. The officers, after thoroughly exploring the newspaper offices, failed to find the photographs. Subsequently, both they and the local district attorney were sued, pursuant to 42 U.S.C. 1983, by staff members of the student newspaper alleging violations of their civil rights and contending that a subpoena, rather than a search warrant, should have been used. Both the federal trial and appellate courts agreed with the plaintiffs that the Fourth and Fourteenth Amendments barred issuing warrants to search for materials held by nonsuspect third parties when no probable cause was shown that a subpoena, which can be challenged in court before being enforced, would be impractical. On May 31, 1978, the Supreme Court, in a 5-3 decision, ruled that the Constitution did not bar police officers from obtaining warrants and then making unannounced searches of newspaper offices for evidence, even though neither the newspaper nor its reporters were suspected of criminal activity.[62]

Sorting out the ramifications of the court's decision, Congress responded with the Privacy Protection Act of 1980, which prohibits federal, state, and local law enforcement officers from using warrants to search and seize "work products" of news and other organizations engaged in First Amendment activities, except in specified circumstances; defines "work products" as materials prepared for communicating information to the public, including mental impressions, conclusions, opinions, or theories of the person who prepared the material; prohibits federal, state, and local law enforcement officers from seizing "documentary materials" from persons engaged in First Amendment activities, except in specified circumstances; defines "documentary materials" as materials upon which information is recorded, including written or printed materials, photographs, films, negatives, and video and audio tapes; provides a civil cause of action for damages for any person aggrieved by a search for, or seizure of, materials in violation of the statute; requires the Attorney General to issue guidelines for the procedures to be employed by federal officers in searching for evidence held by a person not suspected of a crime; and allows administrative sanctions against any Department of Justice officer or employee who violates such guidelines, but prohibits a private individual from filing a lawsuit regarding such a violation.[63]

Cable Communications Policy Act. The day before its final adjournment, the 98th Congress approved the Cable Communications Policy Act of 1984, culminating a four-year effort to balance the rights of the industry against those of the cities that granted franchises.[64] Section 631 of the statute requires cable services to provide subscribers an initial and, thereafter, an annual, written statement concerning the services' collection, use, and management of personally identifiable information with respect to subscribers. Information required to be included in this statement is specified in the section. A cable subscriber has a right of access to all personally identifiable information regarding himself or herself which is collected and maintained

---

[62] *Zurcher* v. *Stanford Daily*, 436 U.S. 547 (1978).

[63] 94 Stat. 1879; 42 U.S.C. 2000aa *et seq*.

[64] 98 Stat. 2779.

by a cable service, and may correct any error in such information. A cable service may use the cable system to collect personally identifiable information in order to obtain information necessary to render a cable or other service provided by the cable operator to the subscriber or to detect unauthorized reception of cable communications. With very limited exceptions, a cable service is prohibited from disclosing personally identifiable information concerning any subscriber without his or her prior consent. Any person aggrieved by any act of a cable service in violation of section 631 may bring a civil action and the court may award actual damages, punitive damages, and litigation costs and attorney fees reasonably incurred.

Electronic Communications Privacy Act. In October 1986,Congress cleared legislation providing privacy protection to communications transmitted with new forms of technology. The Electronic Communications Privacy Act of 1986 (ECPA) extends existing privacy guarantees for conventional telephones to cellular telephones operated by high-frequency radio waves, transmissions by private satellite, paging devices, and electronic mail messages transmitted by, and stored in, computers.[65]

Title I of the statute amends the federal criminal code to extend the prohibition against the unauthorized interception of wire and oral communications to include, with some exceptions, specific types of electronic communications and the communications of any provider of wire or electronic communication services. Providers of an electronic communication service, with specified exceptions, are prohibited from knowingly divulging the contents of any communication carried on that service. Any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of chapter 119 of the federal criminal code may bring a civil action to recover damages, but must do so not later than two years after the date upon which the alleged violation was discovered. The title also specifies additional crimes for which the interception of wire, oral, or electronic communication can be authorized in order to facilitate the investigation of such crimes. It provides additional requirements for applications, court orders, and the implementation of court orders for the interception of such communications. Certain intelligence activities approved by the Attorney General are not to be affected by the communications interception provisions of chapters 119 and 121 of the federal criminal code, and allowance is made for a court-authorized mobile tracking device to be used outside the jurisdiction of the authorizing court. The warning of a person that he or she is the subject of electronic surveillance is made a criminal offense, and a final provision allows the Attorney General to initiate a civil action to obtain an injunction to prevent felony level violations of the ECPA.

Title II, concerning stored wire and electronic communications and transactional records access, makes it a criminal offense to access, without authorization, a facility through which an electronic communication service is provided, or to exceed an authorized access to such a facility. It also prohibits the provider of an electronic communication service or remote computing service, except under certain circumstances, from divulging the contents of any communication stored, carried, or maintained by such service. The title specifies procedural requirements for a

---

[65]100 Stat. 1848.

government entity to obtain access to electronic communications in electronic storage, including court-ordered creation of back-up copies of the contents of such communications. Provision is made for any subscriber or customer of a communication service who is aggrieved by a willful or intentional violation of the title, which is chapter 121 of the federal criminal code, to initiate a civil action to recover appropriate relief. Lastly, the director of the Federal Bureau of Investigation (FBI) is granted access to telephone or communication service information and records relevant to any authorized foreign counterintelligence investigation. No officer, employee, or agent of a wire or electronic communication service provider may disclose to any person that the FBI has sought or obtained such access to telephone or communication service information.

Title III of the statute addresses the use of pen registers and trap and trace devices. A pen register is a device that records or decodes numbers dialed or otherwise transmitted by telephone; a trap and trace device captures an incoming electronic or other impulse and can identify the number from which the call was made. The title prohibits the installation or use of a pen register or a trap and trace device without a court order pursuant to the ECPA or the Foreign Intelligence Surveillance Act of 1978, and imposes criminal penalties for violations of this prohibition.[66] Government attorneys and state law enforcement officers are authorized to apply for a court order allowing the installation and use of a pen register or a trap and trace device, a certification by the applicant that information likely to be obtained by such an installation is relevant to an ongoing criminal investigation being required for the issuance of such an order. Furthermore, providers of a wire or electronic communication service, landlords, custodians, and other persons are required to furnish all information, facilities, and technical assistance necessary to accomplish the installation of a pen register or a trap and trace device if such assistance is ordered by the court. Anyone so providing such assistance shall be compensated for any reasonable expenses incurred, and no cause of action shall lie in any court against anyone so providing such assistance. The Attorney General must report annually to Congress on the number of applications made by law enforcement agencies of the Department of Justice for pen register and trap and trace device orders.

Computer Security Act. Recognizing the increasing use of computers by federal agencies and the vulnerability of computer-stored information, including personal information, to unauthorized access, Congress enacted the Computer Security Act of 1987.[67] The statute requires each federal agency to develop security plans for its computer systems containing sensitive information. Such plans are subject to review by the National Institute of Standards and Technology (NIST) of the Department of Commerce and a summary, together with overall budget plans for information technology, is filed with OMB. NIST is authorized to set security standards for all federal computer systems except those containing intelligence, cryptologic, or certain military information, or information specifically authorized under criteria established by an executive order or statute to be kept secret in the interest of national defense or foreign policy. The statute also mandates a Computer Systems Security and Privacy Advisory Board within the Department of Commerce,

---

[66]The latter statute may be found at 50 U.S.C. 1801 *et seq.*

[67]101 Stat. 1724.

which, among other duties, is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy and advise NIST and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems. Each federal agency is directed to provide all employees involved with the management, use, or operation of its computer systems with mandatory periodic training in computer security awareness and accepted computer security practice.

Computer Matching and Privacy Protection Act. Congress amended the Privacy Act in 1988 to regulate the use of computer matching conducted by federal agencies or making use of federal records subject to the statute. The amendments were denominated the Computer Matching and Privacy Protection Act of 1988.[68] A controversial matter for more than 10 years, computer matching—the computerized comparison of records for the purpose of establishing or verifying eligibility for a federal benefit program or for recouping payments or delinquent debts under such programs—had begun in 1977 at the Department of Health and Human Services. The effort, dubbed Project Match, compared welfare rolls in selected jurisdictions with federal payroll records in the same areas. The controversy surrounding this and similar computerized matches pitted privacy protection advocates, who alleged that personally identifiable data were being used for purposes other than those prompting their collection, against those using the technique to ferret out fraud, abuse, and the overpayment of federal benefits. As the practice subsequently became more widespread, controversy over its use grew.

The amendments regulate the use of computer matching by federal agencies involving personally identifiable records maintained in a system of records subject to the Privacy Act. Matches performed for statistical, research, law enforcement, tax, and certain other purposes are not subject to such regulation. In order for matches to occur, a written matching agreement, effectively creating a matching program, must be prepared specifying such details, as explicitly required by the amendments, as the purpose and legal authority for the program; the justification for the program and the anticipated results, including a specific estimate of any savings; a description of the records being matched; procedures for providing individualized notice, at the time of application, to applicants for and recipients of financial assistance or payments under federal benefits programs and to applicants for and holders of positions as federal personnel that any information they provide may be subject to verification through the matching program; procedures for verifying information produced in the matching program; and procedures for the retention, security, and timely destruction of the records matched and for the security of the results of the matching program. Copies of such matching agreements are transmitted to congressional oversight committees and are available to the public upon request. Executive oversight of, and guidance for, matching programs is vested in the director of OMB. Notice of the establishment or revision of a matching program must be published in the *Federal Register* 30 days in advance of implementation.

The amendments also require every agency conducting or participating in a matching program to establish a "Data Integrity Board," composed of senior agency

---

[68] 102 Stat. 2507.

officials, to oversee and coordinate program operations, including the execution of certain specified review, approval, and reporting responsibilities.

Agencies are prohibited from reducing, suspending, or terminating financial assistance to an individual without first verifying the accuracy of computerized data used in the matching program and without first giving the individual 30 days to contest the action.

Video Privacy Protection Act. Another 1988 privacy statute was enacted in response to an incident that occurred during the 1987 fight over the unsuccessful nomination of Robert H. Bork to the Supreme Court. During the Bork confirmation hearings, a reporter obtained and published a list of the videotapes the Bork family had rented, prompting an outcry from members of Congress in both political parties who felt Bork's privacy had been invaded. A legislative response was enacted the following year. The Video Privacy Protection Act of 1988 prohibits videotape service providers from disclosing their customers' names, addresses, and specific videotapes rented or purchased, except in specifically defined circumstances.[69] Such exceptions include disclosure to the customer; to any person with the informed, written consent of the customer given at the time the disclosure was sought; to a law enforcement agency pursuant to a warrant, grand jury subpoena, or court order; or, name and address only, to a direct marketing business, as long as the customer has an opportunity to reject such a disclosure. Any person aggrieved by any action of a person in violation of the statute may bring a civil action, the court being authorized to award actual damages, punitive damages, and litigation costs and attorneys fees reasonably incurred. Such a lawsuit must be initiated within two years of the discovery of the alleged violation.

Driver's Privacy Protection Act. Enacted as Title XXX of the omnibus Violent Crime Control and Law Enforcement Act of 1994, the Driver's Privacy Protection Act (DPPA) prohibits a state department of motor vehicles, and any officer, employee, or contractor of such an entity, from knowingly disclosing or otherwise making available to any person "personal information about any individual obtained by the department in connection with a motor vehicle record" without the driver's consent.[70] Explicit exceptions to this rule include "matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes" of certain enumerated statutes. A criminal fine may be levied against any person who knowingly violates the statute, and a civil penalty of not more than $5,000 may be imposed by the Attorney General against a state department of motor vehicles for each day of substantial noncompliance. A civil action may be brought against a person who knowingly violates the DPPA by the driver whose privacy was compromised by the violation.

---

[69]102 Stat. 3195; 18 U.S.C. 2710 note.

[70]108 Stat. 2099; 18 U.S.C. 2721 note.

On January 12, 2000, the Supreme Court unanimously ruled that the DPPA is a valid exercise of the constitutional authority of Congress to regulate commerce, and does not violate the 10th Amendment.[71] The drivers' information that the statute governs was seen as being used by insurers, marketers, and others engaged in interstate commerce to contact drivers with customized solicitations, making this information "an article of commerce" subject to congressional regulation. Relying on a 1988 ruling, the court found the DPPA does not "commandeer" states into enforcing federal law applicable to private entities.[72] The statute regulates state activities directly rather than seeking to control the manner in which states regulate private parties. Also, the DPPA was seen as generally applicable, regulating both the states as initial suppliers and private parties that resell drivers' information—"the universe of entities that participate as suppliers to the market for motor vehicles."

Telecommunications Act. Enacted in response to significant structure and marketing changes occurring within the telecommunications industry, the Telecommunications Act of 1996 is a major rewrite of national telecommunications policy, establishing a single, comprehensive regulatory framework that will capture the benefits of competition while ensuring that the users and suppliers of a developing and diversified information industry will be protected from exploitative practices and abuse.[73] Among the provisions of the statute, section 702 specifies that, except as required by law or with the approval of the customer, a telecommunications carrier receiving or obtaining customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in providing the telecommunications service from which such information derives or services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories. Upon affirmative written request of the customer, a telecommunications carrier shall disclose that customer's proprietary network information to any person designated by the customer, including the customer himself or herself. Customer proprietary network information, according to the statute, is information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, and includes, as well, information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier, but does not include subscriber list information.

Health Insurance Portability and Accountability Act. Compared with the Clinton Administration's famous, but failed, 1994 plan to overhaul the entire health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was miniature in scope.[74] The statute sought to guarantee the portability of health insurance coverage for individuals who had health insurance benefits. It also

---

[71] *Reno* v. *Condon*, 120 S. Ct. 666; 68 USLW 4037 (Jan. 12, 2000).

[72] See *South Carolina* v. *Baker*, 485 U.S. 505 (1988).

[73] 110 Stat. 56.

[74] 110 Stat. 1936.

created a pilot program for medical savings accounts, increased the deductibility of health insurance for the self-employed, and provided tax breaks to increase the use of long-term care insurance.

Of particular interest for privacy protection are provisions of the statute's administrative simplification subtitle instructing the Secretary of Health and Human Services (HHS) to develop standards to support electronic data interchange for a variety of administrative and financial health care transactions. Specifically, HIPAA requires the Secretary to issue regulations to establish standard electronic formats for billing and other common transactions, including the use of uniform data codes for reporting diagnoses, referrals, authorizations, and medical procedures; mandates the development of unique identifiers (*i.e.*, identification numbers) for patients, employers, health plans, and health care providers; and requires the Secretary to issue security standards, including an electronic signature standard, to safeguard confidential health information against unauthorized access, disclosure, and misuse.

Beyond these obligations, the subtitle prescribes a timetable for Congress and the Secretary to develop comprehensive medical records privacy standards which would define the circumstances under which the uses and disclosures of such information required a patient's authorization, and gave patients the right to access and amend their personally identifiable health information. The Secretary was required to report to Congress by August 1997 on ways to protect the privacy of personally identifiable health information; Congress was given two years after receiving that report to enact health records privacy legislation, and, if it failed to do so, the Secretary was instructed to issue health privacy regulations by February 21, 2000.[75] As discussed below, the Secretary presented her recommendations to Congress on September 11, 1997, and, because Congress did not enact legislation guided by those recommendations, she issued proposed health records privacy regulations on November 3, 1999. The newly installed Bush Administration initially delayed final issuance of the regulations, but then decided to proceed with implementation.[76]

Children's Online Privacy Protection Act. Although the Clinton Administration and many members of Congress preferred to rely upon industry self regulation for realizing Internet privacy protection, frustration with the industry's slow response regarding minors led to the enactment of the Children's Online Privacy Protection Act of 1998 (COPPA) as part of the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999.[77] The statute requires the operator of a commercial Web site or online service targeted at children under the age of 13 to provide clear notice of information collection and use practices; to obtain verifiable parental consent prior to collecting, using, and disseminating personal

---

[75]110 Stat. 2021; 42 U.S.C. 1320d.

[76]See Robert O'Harrow, Jr., "Protecting Patient Data," *Washington Post*, Mar. 23, 2001, pp. E1, E4; Kristina Stefanova, Privacy Rules Revisited," *Washington Times*, Mar. 29, 2001, pp. B8, B9; Associated Press, "Bush Moves to Protect Patient Privacy," *Washington Times*, Apr. 13, 2001, B9, B10; Amy Goldstein and Robert O'Harrow, "Bush Will Proceed on Patient Privacy," *Washington Post*, Ar. 13, 2001, pp. A1, A10.

[77]112 Stat. 2681-728; 15 U.S.C. 6501-6506.

information about children under 13; and to provide parents access to their children's personal information and the option to prevent its further use. On October 20, 1999, the Federal Trade Commission issued a final rule to implement the COPPA.[78] The statute authorizes the commission to bring enforcement actions and impose civil penalties for violations of the rule in the same manner as for its other rules. At the end of the first year of COPPA implementation, most Web sites geared for children reportedly failed to follow the statute's requirements,[79] but also prompted a reduction of Web site services available to children under the age of 13.[80] The FTC announced that three online companies had agreed to pay $100,000 in fines to settle charges that they had collected personal information from children without their parent's permission.[81]

Gramm-Leach-Bliley Act. Enacted in November 1999, the Financial Services Modernization Act, popularly known as the Gramm-Leach-Bliley Act, constitutes a historic overhaul of federal laws governing the financial services industry.[82] Repealing laws restricting cross-ownership among banks, brokerages, and insurers, the statute establishes a new regulatory framework for maintaining the safety and stability of the financial services industry and requires a number of regulatory agencies to develop new regulations for its implementation. Named for its principal congressional champions—Senator Phil Gramm (R-TX), Representative James A. Leach (R-IA), and Representative Tom Bliley (R-VA)—the statute requires relevant federal regulatory agencies to issue rules obligating financial institutions to establish standards to insure the security and confidentiality of customer records; prohibits financial institutions from disclosing nonpublic personal information to unaffiliated third parties without providing customers the opportunity to decline such disclosures; prohibits financial institutions from disclosing customer account numbers to unaffiliated third parties for use in telemarketing, direct mail marketing, and e-mail marketing; requires financial institutions to disclose, when a customer relationship is initially established and annually thereafter, their privacy policies, including their polices regarding the sharing of information with affiliates and unaffiliated third parties; and mandates a study of the information sharing practices among financial institutions and their affiliates to be conducted by the Secretary of the Treasury, relevant regulatory agencies, and the Federal Trade Commission. Regulatory agency rules implementing these privacy protections became effective on November 12, 2000. Although a May 2001 GAO report indicated that assessment of the statute's privacy

---

[78]*Federal Register*, vol. 64, Nov. 3, 1999, pp. 59888-59915.

[79]Associated Press, "Children's Web Sites Ignore Privacy Rules," *Washington Times*, Mar. 29, 2001, p. B9.

[80]Associated Press, "Law to Protect Children from Internet Intrusion Curtailing their Usage," *Washington Times*, April 14, 2001, p. C12.

[81]William Glanz, "Web Sites Fined Over Privacy of Children," *Washington Times*, Apr. 20, 2001, p. B8; Robert O'Harrow, Jr., "3 Web Firms to Pay Finmes for Collecting Data on Children," *Washington Post*, Apr. 20, 2001, p. E3.

[82]113 Stat. 1338.

provisions was premature,[83] the FTC conducted a sting operation in April that resulted in violations of the act's identity theft protections,[84] and criticism of financial institution's required privacy policy notices to consumers as being too confusing and obscure were beginning to appear in the press.[85]

Safe Harbor Privacy Principles. On July 21, 2000, the Department of Commerce issued a set of Safe Harbor Privacy Principles to enable U.S. companies receiving personal data transfers from European Union (EU) countries to meet the "adequacy" requirements of the EU's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data*.[86] This directive requires all 15 EU member states to make their national privacy laws consistent with the directive, and permits the EU to limit the flow of data among countries not having comparable protections for personally identifiable data. The U.S. approach to privacy, which differs from that of the European Community, relies upon a sectoral approach, based upon a combination of legislation, regulation, and self-regulation. Because of these differences in approach, U.S. companies feared that the EU directive might impede the flow of information from EU states if the United States were deemed to have inadequate privacy protection in critical areas such as medical information.

To address this concern, the Commerce Department, through negotiations with the European Commission, and in consultation with U.S. industry and the general public, developed the Safe Harbor Privacy Principles to ensure that data flows between the EU and the United States are not interrupted. Organizations receiving personal data transfers from the EU and complying with the principles should be considered to meet the "adequacy" requirements of the directive. The European Commission is expected to issue an "adequacy determination" for the safe harbor arrangement soon.[87]

Children's Internet Protection Act. Included as Title XVII of the Consolidated Appropriations Act, 2001, the Children's Internet Protection Act began as separate legislation sponsored by several Members in both houses of Congress.[88] As enacted, the statute requires schools and libraries that receive "E-rate" discounts, or reduced charges, for Internet access to certify to the Federal Communications

---

[83]U.S. General Accounting Office, *Financial Privacy: Too Soon to Assess the Privacy Provisions in the Gramm-Leach-Bliley Act of 1999*, GAO Report GAO-01-617 (Washington: May 2001).

[84]Robert O'Harrow, Jr., "Three Charged with Selling Confidential Data in FTC Sting," *Washington Post*, Apr. 19, 2001, p. E3.

[85]Eileen Alt Powell, "Banks' Privacy Policies Hidden Among Mail Inserts," *Washington Post*, Apr. 26, 2001, pp. B9, B10; John Schwartz, "Privacy Policy Notices are Called Too Common and Too Confusing," *New York Times*, May 7, 2001, pp. A1, A12.

[86]See *Federal Register*, vol. 65, July 24, 2000, pp. 45665-45686.

[87]For information concerning further developments regarding the Safe Harbor Principles, see the Department of Commerce Web site at [http://www.ita.doc.gov/td/ecom/menu.html].

[88]P.L. 106-554.

Commission that they are using filters to block child pornography and obscene, hard-core pornography sites. Other material, "inappropriate for minors," such as soft-core pornography, may be blocked as well. Opponents of the proposal have contended that it is an unfunded mandate, a federal intrusion into family and local community matters, and a violation of First Amendment guarantees.[89] Anticipated court challenge of the new law by civil liberties and library organizations occurred in March 2001when a lawsuit was filed in federal district court in Philadelphia.[90]

Privacy Issues Before Congress

Comprehensive Review. During the 20th century, comprehensive reviews of personal privacy issues were undertaken by the Privacy Protection Study Commission and, to a lesser extent, the Commission on Federal Paperwork, both panels reporting in 1977. These commissions recommended the creation of a permanent federal agency to address, exclusively or in balanced measure, personal privacy matters. Some realization of this proposal occurred with the establishment of the Office of Information and Regulatory Affairs within OMB, which, critics allege, has shown only limited interest in privacy since its creation in 1980.[91]

In a climate of opinion supportive of government downsizing, the creation of a new federal privacy review agency is considered not likely to occur. Indeed, the chartering of such an entity has not been legislatively proposed in Congress for almost a decade.[92]

Alternatively, an existing agency might be tasked with performing studies and evaluations that would collectively result in a comprehensive review of personal privacy issues. This approach, however, presents problems of finding a host agency having a sufficiently broad and compatible mandate to support the desired studies and evaluations; assuring that the host agency has adequate resources to perform the desired studies and evaluations; and assuring that the host agency would not relegate its new privacy responsibilities to a low level of priority.

Another, perhaps less encumbered, alternative would be a temporary privacy study body. Producing a comprehensive review of personal privacy issues would be the only mission of the entity, and all of its resources would be devoted to that

---

[89]Cheryl Wetzstein, "New Measure Takes Aim at Obscene Sites on Web," *Washington Times*, Dec. 24, 2000, p. C2.

[90]Associated Press, "Libraries Lodge Legal Challenge to Internet Filters," *Washington Times*, Mar. 20, 2001, pp. B6, B10; Robert O'Harrow, Jr., "Curbs on Web Access Face Attack," *Washington Post*, Mar. 20, 2001, p. A4; Cheryl Wetzstein, "ACLU, Library Group Sue to Stop Child Internet Protection Act," *Washington Times*, Mar. 21, 2001, p. A3.

[91]See Robert M. Gellman, "Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions," *Software Law Journal*, vol. 6, April 1993, pp. 199-238.

[92]See, however, Robert Gellman, "Taming the Privacy Monster: A Proposal for a Non-Regulatory Privacy Agency," *Government Information Quarterly*, vol. 17, no. 3, 2000, pp. 235-241.

mission. The operating arrangements and products of the Privacy Protection Study Commission provide precedential models for a new entity, and the resulting final report might offer findings and recommendations that could have currency for a few years, allowing the development of implementing proposals and related legislative strategies conducive with the agendas of relevant congressional committees of jurisdiction.

In the 106th Congress, three bills were introduced to establish a temporary study commission to examine personal privacy issues. One of these, offered in the House on March 21, 2000, by Representative Asa Hutchinson (R-AR) as the Privacy Commission Act (H.R. 4049), would have created a 17-member Commission for the Comprehensive Study of Privacy Protection to "conduct a study of issues relating to protection of individual privacy and the appropriate balance to be achieved between protecting individual privacy and allowing appropriate uses of information." The final report of the panel would have been submitted to the President and Congress not later than 18 months after the appointment of all of the members of the commission. Referred to the Committee on Government Reform, the bill was considered at May 15-16, 2000, hearings before the Subcommittee on Government Management, Information, and Technology.[93] At these hearings, OIRA Administrator John T. Spotila expressed the concern of the Clinton Administration "that some might use the commission as a reason to delay much-needed privacy legislation." Another witness, Minnesota Attorney General Mike Hatch, offered similar views, saying "further study is not the proper course, given the volume of ink already spilled on the privacy subject as well as the volume of consumer outcry and violations." He contended that the commission could delay enforcement and legislative action at the federal and state levels; that it would discover "what everyone already knows: that companies collect a lot of information and disclose it without our knowledge"; and that constituents want, not a privacy study, but real privacy protection now."

Supporting the legislation, Robert R. Belair, former deputy counsel of the presidential Committee on the Right of Privacy during the Ford Administration and Office of Telecommunication Policy attorney responsible for Carter Administration follow-up projects based the Privacy Protection Study Commission recommendations, thought "the work of the privacy commission will lead to better decisions about privacy." Joining him in supporting the bill, Georgetown University professor of electronic commerce Mary J. Culnan cautioned that the commission's "usefulness will be short-lived if it only focuses on today's technologies and privacy issues and fails to address ... emerging issues."[94]

Amidst such divided opinion, the Subcommittee on Government Management amended the bill on June 14, increasing the panel's funding authorization from $2.5

---

[93]U.S. Congress, House Committee on Government Reform, *H.R. 4049, to Establish the Commission for the Comprehensive Study of Privacy Protection*, hearings,106th Cong., 2nd sess., May 15-16, 2000 (Washington: GPO, 2001); also see U.S. Congress, House Committee on Government Reform, *The Privacy Commission: A Complete Examination of Privacy Protection*, hearing, 106th Cong., 2nd sess., Apr. 12, 2000 (Washington: GPO, 2001).

[94]Shruti Date, "Privacy Commission Proposal Gets an Unenthusiastic Reception," *Government Computer News*, vol. 19, June 12, 2000, pp. 12, 14.

million to $5 million; authorizing it to issue subpoenas to obtain needed information, but prohibiting the panel from acquiring any classified information relating to national security; and reducing the number of required field hearings from 20 to 10. Forwarded to the full Committee on Government Reform, the bill was further amended on June 29 before being ordered to be reported, as modified, to the House. One amendment indicated that prompt passage of privacy protections could occur before the commission competed its work; another tasked the panel with studying financial fraud against elderly people victimized by schemers who gain access to their banking and investment records; a third required banks and other financial institutions to seek objective, third-party audits of their computer safeguards to assure depositors and investors that their records are secure; and a final amendment added civil liberties experts to the diverse membership of the panel. Brought up on the floor on October 2, 2000, for approval under a suspension of the House rules, the bill failed to pass on a vote of 250 yeas to 146 nays (two thirds approval required).[95]

Representative Hutchinson reintroduced his privacy study commission bill in the 107th Congress on February 13, 2001, with bipartisan support (H.R. 583). Again referred to the Committee on Government Reform, the measure cleared the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations on a voice vote on May 8. It was opposed by Representative Janice Schakowsky (D-IL) who contended that commission operations would delay or obstruct active legislative efforts to protect consumers' privacy. Compared with the earlier Hutchinson proposal, the new bill would reduce the number of commission members appointed by the President from four to two, and increases the appointees of the House and Senate Minority Leaders from two to three each.

A companion bill, of sorts, was introduced in the Senate on May 9, 2001, with bipartisan support (S. 851), by Senator Fred Thompson (R-TN), the chairman of the Committee on Governmental Affairs, to which the bill was referred.[96] Unlike the Hutchinson bill, the Thompson measure would focus commission attention on public sector privacy issues, including the extent to which federal, state, and local governments collect, use, and distribute personal information; their compliance with the Privacy Act, and the extent to which individuals can obtain redress for privacy violations by these governments. The proposed legislation would not limit the commission to examining privacy policies and practices of only executive entities. Another difference: the Hutchinson bill would create a 17-member commission, the Thompson legislation would establish an 11-member panel, giving the President, the Speaker of the House, the House minority leader, and the Senate majority and minority leaders each authority to appoint two members, with the chair jointly selected by all five leaders. Both bills would give the commission 18 months to complete its work.

Privacy Act Amendment. Several issues are before the 107th Congress regarding the Privacy Act. As noted earlier, a September 2000 GAO found that 23

---

[95]*Congressional Record*, daily edition, vol. 146, Oct. 2, 2000, pp. H8561-H8570, H8588-H8589.

[96]See *Congressional Record*, daily edition, vol. 147, May 9, 2001, pp. S4604-S4607.

of 70 agencies had disclosed personal information gathered from their Web sites to third parties, mostly other agencies, but at least four were discovered to be sharing such information with private entities. Responding to these findings, some privacy advocates called for updating the Privacy Act to specify privacy protections for Internet visitors to executive agency Web sites, while others urged better oversight and enforcement of the statute.[97]

Another issue concerns continued vestment of Privacy Act oversight and enforcement in the director of OMB or, alternatively, in another entity. Options for consideration in this regard include a small privacy agency having no regulatory authority over the private sector[98] or a Chief Information Officer of the United States (CIOUS). A Progressive Policy Institute report recommended such a position in March 2000,[99] and legislation in support of the concept was offered in the House during the 106th Congress.[100] Texas Governor George W. Bush, the anticipated Republican presidential nominee, endorsed the CIOUS idea in a June 9, 2000, government reform speech in Philadelphia. During a September 2000 House subcommittee hearing on the proffered CIOUS bills[101] and in related published views, proponents of the new position contended that many aspects of information technology (IT) management would benefit from having a IT expert in charge of this area, that such an official would better facilitate OMB oversight of IT applications and use, and that efficiencies and economies could well result if this official could prevent federal agencies from purchasing computer systems that did not work or otherwise performed poorly in, or failed, security tests. Critics maintained that the CIOUS would unnecessarily perform a subset of duties currently vested in the OMB deputy director for management, would seemingly have little immediate enforcement powers, and, in some versions, might be controlling funds outside the traditional appropriations process. Members of the CIO Council reportedly are at odds over the need for the CIOUS.[102]

---

[97]Lance Gay, "GAO Finds Agencies Sharing Data of On-line Visitors," *Washington Times*, Sept. 8, 2000, p. A3; U.S. General Accounting Office, *Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy*, GAO Report GAO/GGD-00-191 (Washington: September 2000).

[98]See Robert Gellman, "Taming the Privacy Monster: A Proposal for a Non-Regulatory Privacy Agency," *Government Information Quarterly*, vol. 17, no. 3, 2000, pp. 235-241.

[99]See Robert D. Atkinson and Jacob Ulevich, *Digital Government: The Next Step to Reengineering the Federal Government* (Washington: Progressive Policy Institute, March 2000), p. 13.

[100]H.R. 4670 was introduced on June 15 by Rep. Jim Turner (D-TX), and H.R. 5024 was introduced on July 27 by Rep. Tom Davis (R-VA); both bills were referred to the Committee on Government Reform.

[101]U.S. Congress, House Committee on Government Reform, Subcommittee on Government Management, Information, and Technology, *Establishing a Federal CIO: Information Technology Management and Assurance Within the Federal Government*, hearing, 106th Cong., 2nd sess., Sept. 12, 2000 (Washington: transcript awaiting publication).

[102]See Christopher J. Dorobek, "Experts Debate Need for Federal IT Czar," *Government Computer News*, vol. 19, Mar. 6, 2000, p. 58; Christopher J. Dorobek, "CIO Council on (continued...)

A third issue concerns inclusion of the White House Office and the Office of the Vice President within the scope of the Privacy Act, and to what extent, if any, the legislative branch should be subject to the statute or parallel requirements set by rule or standing order. Disclosures of personally identifiable information by the White House during the Clinton Administration has fueled this issue. Similarly, although Congress and the legislative support agencies are not subject to the Privacy Act, the issue of legislatively requiring such is fueled by considerations of executive and legislative branch parity in this regard, as well as by the deemed need for more explicit privacy protections within the legislative branch.[103]

A fourth issue arises from a September 2000 federal district court ruling that the *Feres* doctrine, which prohibits military personnel from suing the government for injuries, applies equally to lawsuits brought under the Privacy Act, resulting in a prohibition on suing not only for damages, but also even for the correction of records.[104]

Still another issue concerns the possible modification of the "routine use" clause of the Privacy Act to improve citizen awareness of the routine uses that agencies have indicated they will make of personally identifiable information and to limit the discretion of agency officials to share personally identifiable information with other agencies. The Privacy Act requires each agency in possession of systems of records to publish for each system the routine uses to which the information might be put. Such notices are published in the *Federal Register*. Most citizens are unaware of these notices and their implications, with the result that they have little understanding of how information supplied by or about them to government agencies might be used. Furthermore, in the view of one policy analyst examining the situation, "agency officials have interpreted the routine use clause broadly and have created almost unlimited ability to move data among Federal agencies."[105]

Finally, an issues has arisen regarding the circumstances, if any, when computer matching of personally identifiable information in systems of records across government programs and agencies should be permitted. Agency officials responsible for combating waste, fraud, and abuse in federal benefits programs urge a

---

[102](...continued)
Track, Members Say," *Government Computer News*, vol. 19, May 8, 2000, p. 65; Christopher J. Dorobek, "What Would Governmentwide CIO Do?," *Government Computer News*, vol. 19, July 10, 2000, p. 74; Joseph J. Petrillo, "David Bill Would Give IT Czar Carrots, but No Stick," *Government Computer News*, vol. 19, Sept. 11, 2000, p. 24.

[103]See U.S. Congress, House Committee on Government Reform, Subcommittee on Criminal Justice, Drug Policy, and Human Resources, *The Privacy Act and the Presidency*, hearing, 106th Cong., 2nd sess., Sept. 8, 2000 (Washington: transcript awaiting publication).

[104]*Mary Louise Cummings* v. *Department of the Navy*, Civil Action No. 98-1183 (D.C. D.C., Sept. 6, 2000).

[105]Gloria Cox, "Implementation of the Routine Use Clause of the Privacy Act," *Policy Studies Review*, vol. 10, Winter 1991-1992, p. 43.

reconsideration of the Privacy Act's strict matching requirements, while privacy advocates would retain the status quo.[106]

Banking and Financial Transactions. As noted above in the discussion of the recently enacted Gramm-Leach-Bliley Act, this statute requires various regulatory agencies to develop new regulations to implement its provisions, including those pertaining to privacy protection. Before the legislation was signed into law, bills had been introduced to modify its privacy provisions, and industry experience with new regulatory rules may prompt other attempts at fine-tuning the statute.[107] So, too, may the findings, conclusions, and recommendations resulting from studies of the information sharing practices among financial institutions and their affiliates conducted by the Secretary of the Treasury, relevant regulatory agencies, and the Federal Trade Commission.

Other recent developments coming to congressional attention include the "know your customer" rules proposed by banking regulators which would have required banks to report suspicious transactions to federal officials in an effort to detect money laundering and other crimes.[108] These elicited considerable public opposition as an invasion of personal privacy. Shortly after the comment period ended on March 8, 1999, the regulators withdrew their rulemaking proposals. The Federal Deposit Insurance Corporation reported receiving 254,394 comments, for example, and the Board of Governors of the Federal Reserve indicated receipt of "over 17,000 comments." Of these, both entities noted, the "overwhelming majority ... were strongly opposed to the adoption of the proposed regulation."[109] By this time, several bills had been introduced to block the proposed rules,[110] and a House subcommittee held a hearing to explore the invasion of privacy implications of the regulations.[111] Whether these regulations will be proposed again in some modified form is uncertain.

Medical Records. Current efforts to legislate privacy protection for medical records are, in many regards, a renewal of the failed 1980 attempt to act upon the recommendations of the Privacy Protection Study Commission. A laboriously crafted compromise on medical records legislation collapsed in the final days of the 98th Congress because sponsors could not reconcile the conflicting demands of civil libertarians, psychiatrists, and the intelligence and law enforcement communities. The proposal basically would have applied the principles of the Code of Fair Information Practice, developed by the HEW Secretary's Advisory Committee on Automated

---

[106]See U.S. General Accounting Office, *The Challenge of Data Sharing: Results of a GAO-Sponsored Symposium on Benefit and Loan Programs*, GAO Report GAO-01-67 (Washington: October 2000).

[107]These bills included H.R. 3320 and S. 1903, and, subsequently, S. 1924.

[108]*Federal Register*, vol. 63, Dec. 7, 1998, pp. 67516-67542.

[109]*Ibid.*, vol. 64, Mar. 29, 1999, p. 14845, and Mar. 31, 1999, p. 15210.

[110]See, for example, H.R. 516, H.R. 530, H.R. 575, H.R. 621, S. 403, S. 466, and S. 508.

[111]U.S. Congress, House Committee on the Judiciary, Subcommittee on Commercial and Administrative Law, *"Know Your Customer" Rules: Privacy in the Hands of Federal Regulators*, hearing, 106th Cong., 1st sess., Mar. 4, 1999 (Washington: GPO, 2000).

Personal Data Systems in 1973, to the patient records of medical and health institutions, not to those kept by private physicians.

Several developments have prompted the recent return to legislating medical records privacy. Growth in the application of information technologies to all aspects of health care and structural changes in health care delivery and payment systems have not only offered significant opportunities for providing improved health care at contained costs, but also increased the threats to patient privacy and medical records confidentiality. Examples include the use of electronic medical records for maintaining clinical information and the use of telemedicine to provide remote access to physicians, medical equipment, and diagnostic facilities by underserved communities. A 1997 study by the National Research Council reported that "the health care industry spent an estimated $10 billion to $15 billion on information technology in 1996."[112]

Major organizational changes in the health care industry also have provided an impetus for expanding the use of information technology. There is a greater need to integrate information provided by participating institutions that are part of managed care systems, as compared to fee-for-service providers. Managed care organizations collect vast amounts of data on the costs, processes, and outcomes associated with various diseases, conditions, and treatments. In this new environment, data must be coordinated from patient services delivered in different settings, such as hospitals, clinics, pharmacies, and physicians' offices, so that care and payment can be provided efficiently. The result has been a growing number of secondary and tertiary users of personal health information.

Rapidly increasing requirements for the collection, integration, analysis, and storage of health information has resulted in the creation of large scale databases, the capability to link data from distributed databases, and the ability for more people in dispersed locations to access data. A variety of mechanisms, both technological and organizational, may be employed to ensure that unauthorized access does not occur and that sufficient audit trails are maintained for proper accountability. Technical measures can be employed to limit access to authorized users for specifically designated purposes. Encryption, the use of smart cards or other unique identifiers for authenticating users, access control software, firewalls to prevent external attacks, and physical security and disaster recovery procedures have all become important elements in creating a technologically secure environment. Computerization has also made it possible to develop approaches for making data anonymous so that individuals cannot be identified. Management practices, including the establishment of strong privacy policies, education and training, and implementing effective sanctions for abuses can contribute substantially to maintaining confidentiality of medical records.

The implementation of the European Union (EU) Data Privacy Directive in October 1998 provided further impetus for congressional action in the 106th Congress.

---

[112]National Research Council, Computer Science and Telecommunications Board, *For the Record: Protecting Electronic Health Information* (Washington: National Academy Press, 1997), p. 2.

Article 25 of the directive requires EU member states to enact laws that prohibit the transfer of personal data to non-EU countries that lack an "adequate level of protection." Determinations of adequacy are to be made by the European Commission. If a finding of inadequacy is made, EU member states must block transfers of personal data to that third country. The United States views, with concern, the prohibition on the transfer of data from EU member countries to third countries that do not provide adequate privacy protection. Following two years of discussions with the Europeans, the Department of Commerce recently issued a set of Safe Harbor principles to enable U.S. companies to meet the "adequacy" requirements of the EU directive.

However, if these developments added impetus for current efforts at legislating medical records privacy, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided both impetus and opportunity. The administrative simplification subtitle of the HIPAA instructed the Secretary of Health and Human Services (HHS) to develop standards to support electronic data interchange for a variety of administrative and financial health care transactions. It required the Secretary to issue regulations to establish standard electronic formats for billing and other common transactions, including the use of uniform data codes for reporting diagnoses, referrals, authorizations, and medical procedures. The development of unique identifiers (*i.e.*, identification numbers) for patients, employers, health plans, and health care providers was also mandated. In addition, the subtitle required the Secretary to issue security standards, including an electronic signature standard, to safeguard confidential health information against unauthorized access, disclosure, and misuse.

Finally, the legislation included a timetable for Congress and the Secretary to develop comprehensive medical records privacy standards, which would define the circumstances under which the uses and disclosures of such information require a patient's authorization, and give patients the right to access and amend their personally identifiable health information. The Secretary was required to report to Congress by August 1997 on ways to protect the privacy of personally identifiable health information. It then gave Congress until August 21, 1999, to enact health records privacy legislation. If Congress failed to act, then the Secretary was instructed to issue health records privacy regulations by February 21, 2000.[113]

The Secretary presented her recommendations on health privacy legislation to Congress on September 11, 1997, at a hearing before the Senate Committee on Labor and Human Resources. The recommendations were intended to serve as guidance to Congress in developing comprehensive privacy legislation. The Secretary outlined the following five key principles as being fundamental to the protection of personally identifiable health information.

- Limit, with few exceptions, the use of an individual's health care information to health purposes only.

---

[113]110 Stat. 2021; 42 U.S.C. 1320d.

- Require organizations that are entrusted with health information, including providers and payers, service organizations, organizations receiving information for specified purposes without patient authorization, organizations receiving information pursuant to a patient's authorization, and employers, to provide adequate security measures to protect that information from misuse or disclosure.

- Provide patients with new rights, such as the ability to get copies of records and propose corrections, to control how their health information is used.

- Hold those who misuse personal health information accountable, and provide redress for persons harmed by its misuse through criminal and civil penalties.

- Balance privacy protections with public responsibility to support national priorities, including public health, research, quality care, and fraud and abuse reduction, which includes allowance of law enforcement access to personal health information in accordance with existing law.[114]

Several health records privacy bills were introduced during 1999, but lawmakers were unable to meet the HIPAA-imposed deadline for enacting comprehensive health privacy legislation. In June 1999, the Senate Committee on Health, Education, Labor, and Pensions (formerly Labor and Human Resources) delayed indefinitely an attempt to mark up a health privacy bill after lawmakers failed to agree on whether to give patients the right to sue over breaches of medical record confidentiality, and whether to allow preemption of all state health privacy laws. With the failure of Congress to meet its self-imposed deadline, the Secretary, on November 3, 1999, issued proposed health records privacy regulations based on the five principles outlined in her report to Congress. The Secretary was unable to propose comprehensive health privacy protections because the HIPAA limits the application of the proposed rule to health plans, health care clearinghouses, and health care providers that maintain and transmit health information electronically.

The proposed health privacy rule gives patients the right to inspect and amend their medical records and requires health plans and providers to obtain a patient's voluntary consent to disclose information, unless the disclosure is related to treating an individual or paying for his or her care. Key provisions of the rule are summarized below.

Applicability. The rule covers health plans, health care providers, and health care clearinghouses, but does not directly apply to other entities that collect and maintain health information. It also covers only information that is electronically transmitted or maintained.

---

[114]See U.S. Congress, Senate Committee on Labor and Human Resources, *Protecting Our Personal Heath Information: Privacy in the Electronic Age*, hearings, 105th Cong., 1st sess., Sept. 11 and Oct. 8, 1997 (Washington: GPO, 1998), pp. 21-24.

Individual Rights. Under the proposal, individuals may inspect, copy, and amend their medical records and request restrictions on the use and disclosure of their personally identifiable information in some instances.

Permitted Uses and Disclosures Without Individual Authorization. Personally identifiable information may be used and disclosed for treatment, payment, and health care operations. It may also be used and disclosed for various specified public policy purposes, including research, health care oversight, and law enforcement. All other uses and disclosures require individual authorization. Health plans and health care providers must sign contracts with their business partners that limit how the partners use personally identifiable information.

Information Practices. Covered entities must disclose the minimum amount of personally identifiable information necessary to fulfill the purpose of the disclosure, and may not condition treatment or payment on obtaining an authorization if one is required. Covered entities must provide up-to-date notice to patients describing their rights and how the entity intends to use personally identifiable information.

Preemption. The proposed rule preempts state laws that are contrary to, or less protective of, privacy, with some exceptions (*e.g.*, state public health surveillance laws, parental notification laws).

Enforcement. The proposed rule provides civil and criminal penalties for non-compliance, but does not give patients the legal right to sue for violations of their health information privacy.[115]

A number of comprehensive health privacy bills were introduced during the 106th Congress. Also, patients' rights legislation, offered in both the House and the Senate, included provisions relating to the confidentiality of health information and the right of individuals to have access to their personal health information. There continues to be general consensus that a federal statute that provides baseline medical records privacy protection would improve safeguards over the existing patchwork of state and federal laws. There also is strong support for a legislative solution to this issue, rather than reliance on federal regulations to protect health privacy rights. The bills introduced during the 106th Congress sought to place restrictions on the use and disclosure of personally identifiable health information, establish security and auditing capabilities for records systems, ensure patients' access to their records, provide the right to seek corrections, require entities to provide notices of their privacy practices, and establish penalties for abuse of privacy rights. The bills varied on the methods for assuring protection, the relationship between federal law and state law, the mechanisms for acquiring informed consent or the use of federal statutes as the basis for allowable disclosures, the rules governing the use of protected health information in conducting research, and procedures for law enforcement access to confidential health information. Finally, the bills also differed in terms of the scope of protected

---

[115]For information on the development of the Secretary's HIPPA health records privacy regulations, including the text of the *Federal Register* notice and all related public comments, see the HHS Administrative Simplification homepage at [http://aspe.os.dhhs.gov/admnsimp/index.htm].

health information covered and the definitions used for such concepts as "non-identifiable health information."

As the 106th Congress moved toward final adjournment, the White House announced in early October that President Clinton was preparing to realize his patients' bill of rights proposal through Department of Labor regulations mandating such guarantees to the 130 million Americans enrolled in private, employer-provided health plans.[116] The regulations were subsequently issued on December 21, 2000, pursuant to the department's authority over employee health benefit and pension benefit programs. In addition to determining medical records disclosure and protection policy, the regulations extend to paper records and oral communications, as well as electronic forms and formats; require patients' written consent for even routine disclosure of information; and establish new criminal and civil penalties for health care providers and insurers that improperly use or disclose medical information. The regulations become fully effective in two years.[117]

Online Communication. During the past decade, as greater numbers of Americans have explored the Internet, privacy concerns have grown regarding the collection, use, and storage of personal information by website operators. The Clinton Administration and many members of Congress have preferred to rely upon industry self-regulation for realizing privacy protection, but frustration with industry's slow response regarding minors led to the enactment of the Children's Online Privacy Protection Act of 1998, which is profiled above.[118] During the 106th Congress, legislation was offered to address several issues regarding Internet privacy. These included, among others, the responsibilities of Web site operators who collect, use, and store personal information; the extent to which the activities and operations of "individual reference services" or "look-up services" result in personal privacy invasion; online profiling to determine what Web sites are visited by a particular user and the development of a profile of the user's preferences and interests; and the extent to which the personal information storage and transmittal practices of Web site operators contribute to identity theft, in which one individual assumes the identity of another using personal information.[119]

When press disclosures in July 2000 revealed the existence of Carnivore, a new FBI e-mail surveillance system, Congress took immediate interest. The Subcommittee on the Constitution of the House Committee on the Judiciary held a July 24 oversight hearing on Fourth Amendment issues raised by the Carnivore program, receiving testimony from FBI and Department of Justice officials, as well as concerned legal

---

[116]Reuters News Agency, "Clinton Moves to Grant Patients Rights," *Washington Times*, Oct. 10, 2000, p. A8.

[117]Associated Press, "Clinton Ensures Privacy for Patients," *Washington Times*, Dec. 20, 2000, p. A4; Associated Press, "New Medical-Privacy RulesCap Almost 10 Years of Debate," *Washington Times*, Dec. 21, 2000, p. A6; Juliet Eilperin, "U.S. Moves to Cloak Medical Records," *Washington Post*, Dec. 20, 2000, pp. A1, A4-A5.

[118]112 Stat. 2681-728; 15 U.S.C. 6501-6506.

[119]Identity theft is punishable under the Identity Theft and Assumption Deterrence Act of 1998, 112 Stat. 3007.

experts and representatives of civil liberties organizations. In early August, the Attorney General announced that an independent review of the Carnivore program and its implications for personal privacy would be conducted, but declined, contrary to the request of 28 Members of Congress, to suspend the program during the interim period before study results were reported.[120] The Senate Committee on the Judiciary reviewed the Carnivore program at a September 6 hearing. In late November, a preliminary draft of the Carnivore study, conducted by the Illinois Institute of Technology Research Institute, found the Internet wiretap program to be a sound law enforcement tool, but recommended some modifications to protect people's routine e-mail and other communications from unlawful interception.[121] Some critics contended that those conducting the study were biased in favor of the new technology, while others argued that biased resulted not only from the selection of the reviewers, but also the ground rules for the study.[122]

At an October 3 Senate Committee on Commerce hearing on proposed legislation to protect the privacy of Internet users (S. 809, S. 2606, and S. 2928), representatives from America Online, Inc., and Hewlett-Packard Company voiced support for a bipartisan proposal introduced by Senator John McCain (R-AZ), the committee chair, and Senator John F. Kerry (D-MA), among others. The measure (S. 2928) would have required Web sites to give online visitors conspicuous notice of their privacy policies, as well as the choice to opt out of efforts to collect data about visitors. Enforcement authority was vested in the Federal Trade Commission. Consumer advocates, however, regarded the bill as too weak. Nonetheless, a consensus prevailed that some legislation was needed, and Senator McCain announced at the end of the proceeding that he would hold more hearings on the online privacy issue early in 2001.[123]

Electronic Commerce. The convergence of computer and telecommunications technologies has not only revolutionized the storage, retrieval, and sharing of information, but also, in the considered view of many, produced an information economy resulting from commercial transactions on the Internet, both retail business-to-customer and business-to-business in character, which are commonly referred to as electronic commerce or e-commerce. During the past few years, Congress has taken an active interest in e-commerce issues, including some having a bearing upon, or implications for, personal privacy. The utilization of electronic signatures, a means of verifying the identity of a user of a computer system to control access to, or to authorize, a transaction, is one such issue. Legislation supporting electronic signatures could give them legal status equal to that of written

---

[120]Elisabeth Frater, "Law Enforcement: The Carnivore Question," *National Journal*, vol. 32, Sept. 2, 2000, pp. 2722-2723.

[121]The final version of the evaluation, "Independent Technical Review of the Carnivore System: Final Report," issued December 8, 2000, may be found at the Department of Justice Web site[www.usdoj.gov/jmd/publications/carniv_final.pdf].

[122]David A. Vise and Dan Eggen, "Study: FBI Tool Needs Honing," *Washington Post*, Nov. 22, 2000, p. A2.

[123]Ariana Eunjung Cha, "Key Firms Back Bill on Web Privacy," *Washington Post*, Oct. 4, 2000, pp. E1, E10.

signatures, override the inconsistencies of state law and policies that might hamper or retard the growth of e-commerce, and establish requirements for their use in transactions with the federal government. Just before final adjournment, the 105th Congress enacted the Government Paperwork Elimination Act (GPEA) as part of the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999.[124] The statute directed OMB to establish procedures for executive branch agencies to accept electronic submissions using electronic signatures, and required them to accept those submissions except where they were found to be impractical or inappropriate. OMB published procedures and guidance for implementing the GPEA on May 2.[125] A July 25, 2000, memorandum from the OMB director to agency chief information officers provides instruction for the preparation and submission of GPEA implementation plans to OIRA.[126]

The 106th Congress enacted the Electronic Signatures in Global and National Commerce Act in June 2000.[127] The statute, dubbed E-SIGN, promotes the use of electronic signatures, contract formation, and recordkeeping in private commerce by establishing legal equivalence between contracts in paper or electronic form, pen-and-ink and electronic signatures, and other legally-required written documents and the same information in electronic form. It applies broadly to commercial, consumer, and business transactions in or affecting interstate or foreign commerce, and to transactions regulated by both federal and state government. OMB draft procedures and guidance for implementing the E-SIGN were circulated within the executive branch for comment on August 3 with a closure date of August 11. The E-SIGN became effective on October 1, 2000.

These initiatives promoting the use of electronic signatures in e-commerce have raised some personal privacy issues. For example, the initial procedures and guidance OMB proposed for implementing the GPEA prompted concerns for some privacy advocacy groups that a reliance on using personal information to establish one's identity was being created, with the result that, as a consequence of its collection by the federal government and federal contractors, larger holdings of such information would be realized. Also, some urge that more attention be given to the danger of identity theft resulting from electronic signatures being stolen or sold by unauthorized persons, a privacy invasion portending a variety of legal and financial problems for the victims.

Encryption, the encoding and decoding of electronic messages through the use of "keys" to communicate sensitive information and data, is another important aspect of e-commerce development. At the core of the congressional debate on this subject is the issue of who holds the keys. The 105th Congress considered several bills addressing national encryption policy, but none was enacted, and the controversy continued into the 106th Congress. Initially, the Clinton Administration favored a

---

[124]112 Stat. 2681-749.

[125]*Federal Register*, vol. 65, May 2, 2000, pp. 25508-25521.

[126]This memorandum is available in the "Information Policy and Technology" section of the OMB Web site at [http://www.whitehouse.gov/OMB/inforeg/index.html].

[127]114 Stat. 464.

policy of the federal government holding the encryption keys for major commercial transactions. When industry and congressional critics contended that this arrangement could easily result in violations of citizen's privacy rights, the administration shifted to a policy of having a "spare key" held by a third party "key recovery agent," and not directly held by the federal government. Critics remained uncomfortable with the prospect of the federal government ultimately having access to the "spare key" for law enforcement and national security purposes. Other factors under consideration are liability protection for proper release of keys and penalties for improper use or release of keys. Congressional discussion and exploration of national encryption policy continues.

Another e-commerce issue under congressional consideration is the regulation of unsolicited commercial e-mail (UCE), sometimes referred to as "spam" or "junk e-mail." There are several dimensions to the issue, including the question of UCE qualifying as a form of commercial speech that is protected by the First Amendment, the perpetration of fraud, and the matter of UCE cost being passed on to consumers through higher charges from Internet service providers who must upgrade their systems to handle the increased traffic. Also, for some, the intrusiveness of UCE constitutes an invasion of privacy. Congress enacted a statute in 1991, the Telephone Consumer Protection Act, that required the Federal Communications Commission to prohibit unsolicited calls from automatic dialing devices that played a recorded message to all private residences and police, fire, and other emergency lines, and also banned the automatic calls from facsimile machines that transmitted unsolicited marketing materials via the telephone lines.[128] Whether there should be an analogous law for regulating UCE, or a requirement that would allow a consumer, before opening an e-mail message, to determine whether or not it is unsolicited advertising and to direct the sender to cease transmissions of such messages, remains under congressional consideration.

Finally, an attempt to protect personal privacy by prohibiting the public display of an individual's Social Security number for commercial purposes without consent became embroiled in controversy in the closing days of the 106th Congress. Legislation on this matter was introduced by Senator Judd Gregg (R-NH) on May 15, 2000 (S. 2554). It was denominated Amy Boyer's Law in memory of a New Hampshire woman who was slain by a man who tracked her down after buying her Social Security number on the Internet. A modified version of the proposal was subsequently attached in the Senate to legislation appropriating funds for the Departments of Commerce, Justice, and State and related agencies for FY2001 (H.R. 4690). Critics of the modified version reportedly contended it was a Trojan Horse because exceptions to the proposal's regulatory arrangements allowed giant data brokers, banks, marketers, and private detectives to exchange or sell Social Security numbers among themselves.[129] In an October 26 letter to the House and Senate leadership, President Clinton expressed "serious concerns" about several provisions of the Commerce, Justice, State appropriations bill, saying, at one point:

---

[128]105 Stat. 2394; 47 U.S.C. 227.

[129]Robert O'Harrow, Jr., "New Privacy Bill Called 'Trojan Horse'," Washington Post, Oct. 25, 2000, pp. E1, E6.

> The bill fails to address in any meaningful way the real privacy concerns about Social Security numbers raised by the Administration. Regrettably, it does not include needed protections against the inappropriate sale and display of individual citizen's Social Security numbers. Moreover, the bill creates loopholes that seriously undermine the goal of the legislation to protect privacy.[130]

The bill was not immediately presented to the President and conferees subsequently agreed to remove the section.[131]

For additional information concerning personal privacy issues receiving congressional consideration, consult the relevant CRS products identified in the reading list at the end of this report.

---

[130]The White House, Office of the Press Secretary, *Text of a Letter from the President to the Speaker of the House of Representatives, the Majority Leader of the Senate, and the Democratic Leaders of the House and Senate* (Washington: Oct. 26, 2000), available from the Virtual Library at [http://www.whitehouse.gov].

[131]See the supplemental explanatory statement in *Congressional Record*, daily edition, vol. 146, Dec. 15, 2000, p. H12481 (indicating no conference agreement on section 635 of H.R. 5548 as appended to H.R. 4942 in conference; see *Congressional Record*, daily edition, Oct. 25, 2000, p. H11143).

For Further Reading

CRS Report RS20026, *Banking's Proposed "Know Your Customer" Rules*, by M. Maureen Murphy

CRS Report RL30323, *Confidentiality of the Taxpayer Identification Number Under the Internal Revenue Code*, by Marie B. Morris.

CRS Report RS20426, *Electronic Commerce: An Introduction*, by Glenn J. McLoughlin.

CRS Report RL30745, *Electronic Government: A Conceptual Overview*, by Harold C. Relyea.

CRS Report RS20344, *Electronic Signatures: Technology Developments and Legislative Issues*, by Richard M. Nunno.

CRS Report RL30914, *Federal Chief Information Officer (CIO): Opportunities and Challenges*, by Jeffrey W. Seifert.

CRS Report RS30620, *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations*, by C. Stephen Redhead.

CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia S. Smith.

CRS Report RS20035, *Internet Privacy—Protecting Personal Information: Overview and Pending Legislation*, by Marcia S. Smith.

CRS Report RS20500, *Medical Records Privacy: Questions and Answers on the Proposed Federal Regulations*, by C. Stephen Redhead.

CRS Report RL30322, *Online Privacy Protection: Issues and Developments*, by Gina Marie Stevens.

CRS Report RS20919, *Privacy Protection: Creating a Commission to Assess Current Privacy Policy and Practice*, by Harold C. Relyea.

CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

CRS Report RS20066, *Religious Objections to Use of Social Security Numbers on Tax Returns*, by Marie B. Morris.

CRS Report RL30477, *Summary of the Proposed Rule for the Privacy of Individually Identifiable Health Information*, by Gina Marie Stevens and Melinda DeAtley

CRS Report RL30824, *The Privacy Act: Emerging Issues and Related Legislation*, by Harold C. Relyea.

CRS Report 30318, *The Social Security Number: Chronology of Federal Developments Affecting Its Use*, by Kathleen S. Swendiman.