Order Code RL30824

The Privacy Act: Emerging Issues and Related Legislation

Updated February 26, 2002

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

The Privacy Act:
Emerging Issues and Related Legislation

Summary

The Privacy Act of 1974 represents an attempt by Congress to legislate several aspects of personal privacy protection as it relates to federal agency operations and practices. First, it sustains some traditional major privacy principles. Second, it 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. Third, the statute embodies a number of principles of fair information practice: 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.

Since its enactment, the Privacy Act has been amended on six occasions; actions in 1988 and 1990 establishing new procedures and data protection boards for computer matching are generally seen as being the most significant. Of late, new issues have arisen concerning these matters and some long-prevailing concerns. This report reviews the background and development of the statute, its current provisions, and emerging issues pertaining to it. As legislative and other relevant developments occur, this report will be updated.

Contents

The Privacy Act: Emerging Issues and Related Legislation

The Privacy Act of 1974 represents an attempt by Congress to legislate several aspects of personal privacy protection as it relates to federal agency operations and practices.[1] Its eclectic provisions can be traced to several contemporaneous events prompting congressional interest in securing personal privacy.

Since the years of the late 19th century, various developments—not the least of which have been new, intrusive technologies—have contributed to more disparate understandings of the concept of privacy and infringements upon it.[2] Congress made an initial effort at legislating a new kind of privacy protection in 1970 when enacting the Fair Credit Reporting Act regulating the collection and dissemination of personal information by consumer reporting entities.[3]

With the Crime Control Act of 1973, Congress prohibited federal personnel and state agencies receiving law enforcement assistance funds pursuant to the statute 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 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."[4]

That same year, the Advisory Committee on Automated Personal Data Systems, established by Secretary of Health, Education, and Welfare Elliot L. Richardson in early 1972, offered an important proposal. The panel's July 1973 final report recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems." Such a code would: punish unfair information practice with civil and criminal penalties; provide injunctive relief to prevent violations of safeguard requirements; empower individuals to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions; and allow the recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits.[5]

---

[1]For the text of the Privacy Act, see 5 U.S.C. 552a.

[2]See CRS Report RL30671, *Personal Privacy Protection: The Legislative Response*, by Harold C. Relyea.

[3] 84 Stat. 1128; 15 U.S.C. 1681 et seq.

[4] 87 Stat. 197, at 215-216; 42 U.S.C. 3789g.

[5]U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*

(continued...)

Congressional efforts to legislate notice, access, and emendation arrangements for individuals concerning personally identifiable records maintained on them by federal departments and agencies began in the House in June 1972, but did not extend beyond the subcommittee hearing stage during the 92nd Congress. However, a few days before these inaugural House hearings on legislation that would evolve into the Privacy Act, a burglary occurred at Democratic National Committee headquarters. It was the beginning of the Watergate incident, which would significantly affect attitudes toward privacy protection legislation and the leadership for such legislation.

Legislation leading to the enactment of the Privacy Act began in the House largely as an effort to create a procedure whereby individuals could learn if federal agencies maintained files on them, could review the contents of the records in those files, could correct inaccuracies they contained, and could know how this information was being used and by whom. In the Senate, a privacy protection bill sponsored by Senator Sam Ervin, Jr., initially sought largely to establish a Federal Privacy Board and to create standards and management systems for handling personally identifiable information in federal agencies, state and local governments, and other organizations. Other aspects of privacy policy were added to these bills as they moved through their respective houses of Congress, and then were reconciled in a somewhat unusual manner to create an amalgamated bill acceptable to the House, the Senate, and the President.

House hearings began in mid-February 1974 under Representative William S. Moorhead, chairman of the Subcommittee on Foreign Operations and Government Information of the Committee on Government Operations (now Government Reform), and a principal manager of the legislation. The subcommittee held markup discussions in May, June, and July. These deliberations resulted in a clean bill (H.R. 16373), which was introduced by Representative Moorhead with 13 bipartisan co-sponsors in mid-August and favorably reported by the Subcommittee without a dissenting vote. The Committee on Government Operations considered the legislation in mid-September, substituted revised text for the original language, and favorably reported it. President Gerald Ford, who had recently succeeded to the Oval Office after President Richard Nixon's early August resignation, endorsed the House bill in an October 9 statement.[6] The measure was considered by the House on November 20 and 21, and approved, with amendments, on a 353-1 yea-and-nay vote.[7]

A somewhat different counterpart privacy proposal emerged in the Senate. Senator Ervin introduced his bill (S. 3418) on May 1, 1974, with bipartisan cosponsorship. Hearings on this and related legislation occurred in June. During June, July, and August, staff of the Senate Committee on Government Operations, its

---

[5](...continued)
(Washington: GPO, 1973), pp. xxiii, 50.

[6]U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, *Public Papers of the Presidents of the United States: Gerald R. Ford, 1974* (Washington: GPO, 1976), pp. 243-244.

[7]*Congressional Record*, vol. 120, Nov. 20, 1974, pp. 36643-36660; Ibid., Nov. 21, 1974, pp. 36955-36977.

Ad Hoc Subcommittee on Privacy and Information Systems, and the Subcommittee on Constitutional Rights of the Committee on the Judiciary—all panels chaired by Senator Ervin—further refined the language of the bill. In a mid-August committee mark-up, a staff-developed version of the measure was amended and favorably reported to the Senate.

The new text of the bill would have established the Privacy Protection Commission, composed of five members appointed by the President from private life and subject to Senate approval. It would have been responsible for compiling and publishing an annual directory of information systems subject to the provisions of the bill, enforcing the legislation, and developing model guidelines for its implementation, including the conduct of research in this regard. The bill also would have established federal agency standards and management systems for handling information relating to individuals. These included fair information practice principles, disclosure standards, mailing list restrictions, and civil and criminal penalties.

On November 21, 1974, the Senate considered the Ervin legislation; amendments developed by committee staff and the Office of Management and Budget (OMB) were adopted, and the resulting version of the legislation was approved.[8] The following day, the Senate took up the House counterpart bill, struck its language and substituted in lieu there of the language of the Ervin bill, and approved the amended version of the House bill.[9]

With only a few weeks remaining before the 93rd Congress would adjourn *sine die*, House and Senate managers found they had very little time to reconcile the two differing bills. There was, however, strong desire for the passage of such legislation, not only as a so-called Watergate reform, but also as a tribute and memorial to Senator Ervin, who was retiring from congressional service. Consequently, Representative Moorhead and Senator Ervin, with the concurrence of their respective committees, agreed to the rare arrangement of having their committee staffs negotiate a mutually agreeable legislative measure. After this effort reduced 108 substantive differences to eight, the leaders of the respective House and Senate committees brought those to resolution.[10] In lieu of a conference committee report, a staff analysis of the compromise legislation was produced.[11] The major concession was the relegation of the enforcement commission to the status of a temporary national study commission. Its oversight responsibilities were vested in OMB, but without enforcement authority.

On December 11, the House adopted the Senate bill as amended with the language of its own bill.[12] The Senate concurred with the House amendment by passing its own amendment on a 77-8 vote on December 17, clearing the measure for

---

[8]*Congressional Record*, vol. 120, Nov. 21, 1974, pp. 36882-36921.

[9]Ibid., Nov. 22, 1974, pp. 37064-37069.

[10]Ibid., Dec. 17, 1974, p. 40400.

[11]See ibid., pp. 40405-40408.

[12]Ibid., Dec. 11, 1974, pp. 39200-39204.

further House action.[13] The following day, the House agreed to the Senate amendments with an amendment of its own,[14] and the Senate concurred with the House amendments the same day, clearing the measure for the President's signature.[15] The Privacy Act was signed into law by President Ford on December 31, 1974.[16] In his signing statement, the President said the new law "signified an historic beginning by codifying fundamental principles to safeguard personal privacy in the collection and handling of recorded personal information by federal agencies."[17]

Major Provisions

The Privacy Act provides privacy protection in several ways. First, it sustains 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."[18]

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. 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.

---

[13]Ibid., Dec. 17, 1974, pp. 40397-40413.

[14]Ibid., Dec. 18, 1974, pp. 40879-40886.

[15]Ibid., pp. 40730-40731.

[16]88 Stat. 1896; 5 U.S.C. 552a.

[17]U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, *Public Papers of the Presidents of the United States: Gerald R. Ford, 1975* (Washington: GPO, 1977), pp. 1-2.

[18] 5 U.S.C. 552(e)(7).

Since its enactment, the Privacy Act has been amended on six occasions. In 1982, the Debt Collection Act added a new exception to the disclosure prohibition for disclosures made to consumer credit reporting agencies.[19] That same year, the Congressional Reports Elimination Act changed the annual report requirement of the Privacy Act and modified the provision for publication of agency systems of records.[20] In 1984, the Central Intelligence Agency Information Act resolved a long-standing controversy by specifying that the Privacy Act is not authority "to withhold from an individual any record which is otherwise accessible to the individual under the provisions of" the Freedom of Information Act.[21] Amendments in 1988[22] and 1990[23] established new procedures and data protection boards to ensure privacy, integrity, and verification of data disclosed for computer matching. Recently, the Federal Reports Elimination and Sunset Act of 1995, as amended by the Miscellaneous Appropriations Act for FY 2000, repealed the requirement for a biennial Privacy Act report to Congress.[24]

Emerging Issues

Better Enforcement or Overhaul. Several issues are before the 107th Congress regarding the Privacy Act. A September 2000 General Accounting Office (GAO) report on a survey of online privacy protections at federal Web sites 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.[25]

Managing "Cookies". Federal agencies obtained personal information about visitors to their Web sites through the use of computer software known as "cookies." In June 2000, press disclosures revealed that the National Drug Control Policy Office, an agency within the Executive Office of the President, was secretly tracking visitors

---

[19]96 Stat. 1749, adding 5 U.S.C. 552a(b)(12).

[20]96 Stat. 1819, at 1821-1822, modifying 5 U.S.C. 552a(e)(4) and (p).

[21]96 Stat. 2209, at 2211-2212, adding 5 U.S.C. 552a(q)(2).

[22]102 Stat. 2507, adding 5 U.S.C. 552a(o),(p),(q), and (u), and amending 5 U.S.C. 552a(a), (e), and (v).

[23]104 Stat. 1388-334, modifying 5 U.S.C. 552a(p).

[24]109 Stat. 707, as amended by section 236 of H.R. 3425, as incorporated, at 113 Stat. 1537-296, repealing 5 U.S.C. 552a(s).

[25]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, Sept. 2000.

to its Web site through the use of "cookies."[26] In response, OMB issued a June 22, 2000, memorandum to the heads of all executive departments and agencies indicating 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, [certain specified] ... conditions are met."[27]

In October 2000, 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, facilitated transactions at the website and were not banned by OMB. Session cookies last only as long as one is visiting the website. 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.[28]

In mid-April 2001, Senator Fred Thompson, 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.[29] Reports on 16 agencies found 64 Web sites making use of "persistent cookies."[30] Shortly thereafter, a GAO senior attorney criticized OMB's contradictory guidelines about federal agency use of "cookies." OMB, it was observed, had encouraged agencies to comply with the fair information practice principles of the Federal Trade Commission, which are not statutorily mandated, and also adhere to the requirements of the Privacy Act.[31] The Privacy Act might be amended to eliminate any such contradiction, to prescribe conditions when "sessions cookies" may be used, and to outlaw the use of "persistent cookies."

---

[26]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.

[27]The memorandum is available from the OMB Web site at: [http://www.whitehouse.gov/omb/memoranda/m00-13.html].

[28]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, Oct. 20, 2000.

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

[30]Associated Press, "Federal Web Sites Can Track Visitors," Washington Times, Apr. 17, 2001, p. A8; Senator Thompson's release of the preliminary findings may be found at [http:www.senate.gov/~gov_affairs/041601a_press.htm].

[31] Drew Clark, "Conflicting Guidelines on Web 'Cookies' Spur Confusion," *GovExec.com Daily Briefing*, Apr. 24, 2001, available at [http://www.govexec.com/].

Oversight and Enforcement Responsibility. 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[32] or a Chief Information Officer of the United States (CIOUS). Such an official had been proposed in 1995 Senate legislation underlying the Clinger-Cohen Act governing information technology acquisition and management. A Progressive Policy Institute report recommended such a position in March 2000,[33] and legislation in support of the concept was offered in the House during the 106th Congress.[34] 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[35] 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 few 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.[36] In the early weeks of the new administration, President Bush vacated his earlier endorsement of a CIOUS.

Broader Application. 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

---

[32]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.

[33]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.

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

[35]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).

[36]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 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.

information by the White House during the Clinton Administration has fueled this issue. Similarly, although Congress and the legislative support agencies are not currently subject to the Privacy Act, the issue of legislatively requiring their inclusion is fueled by considerations of executive and legislative branch parity in this regard, as well as by the perceived need for more explicit privacy protections within the legislative branch.[37]

Military Exclusion. 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,[38] 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.[39] In this case, a U.S. Navy fighter pilot sought damages for the leaking of her confidential flight evaluation to Robert L. Gandt, an author researching a book on navy fighter pilots. The evaluation's recommendation that Cummings be stripped of her flight status was rejected by the commander of the Naval Air Force for the Atlantic Fleet. Gandt's 1997 book, *Bogey's and Bandits: The Making of a Fighter Pilot*, quoted from the evaluation, but assigned Cummings a pseudonym. A 1988 graduate of the U.S. Naval Academy, Cummings left the navy in 1999 and is currently an assistant professor of engineering at Virginia Polytechnic Institute and Statute University.[40]

On August 2, 2001, Representative Rick Boucher, with bipartisan cosponsorship, introduced H.R. 2738 to amend Title 5, United States Code, to clarify that all of the protections of the Freedom of Information Act and the Privacy Act apply to members of the armed forces to the same extent and in the same manner as to any other individual. The bill was referred to the Committee on Government Reform.

On February 15, 2002, the U.S. Court of Appeals for the District of Columbia reversed the trial court in the navy fighter pilot case seeking Privacy Act relief. The 2-1 ruling said that members of the military can sue the government for invading their privacy, indicating that the *Feres* doctrine does not take precedence over the Privacy

---

[37]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).

[38]*Feres* v. *U.S.*, 340 U.S. 135 (1950). The *Feres* case involved a liability claim under the Federal Tort Claims Act by the executor of a soldier who had died in a barracks fire. The Supreme Court, while continuing to uphold the doctrine, has stressed that it "cannot be reduced to a few bright-line rules," but rather "each case must be examined in light of the [Tort Claims Act] as it has been construed in *Feres* and subsequent cases." *U.S.* v. *Shearer*, 473 U.S. 52, 105 (1985). The Privacy Act affords liability damages apart from the Tort Claims Act.

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

[40]Steve Vogel, "Navy Pilot Fights Privacy Ruling," *Washington Post*, Oct 3, 2000, pp. B1, B7.

Act.[41] Because the decision is binding only on the courts of the circuit, a legislative clarification may still be sought.

Routine Use Reconsidered. 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."[42]

However, from another perspective, the routine use clause may not be quite as broadly interpreted as has been asserted. A May 1998 report, prepared by a benefit eligibility verification study committee of the President's Council on Integrity and Efficiency, for example, considered it doubtful that, given prevailing judicial interpretation, "disclosure of information collected by one agency for a specific program, to another agency for eligibility verification in an unrelated program, would be considered a routine use."[43]

Matching and Sharing. Finally, an issue 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 reconsideration of the Privacy Act's strict matching requirements, while privacy advocates would retain the status quo.[44] The case for reconsideration began to emerge a few years ago, the May 1998 benefit eligibility verification study report of the President's Council on Integrity and Efficiency being exemplary. Describing the demanding and cumbersome requirements for producing and executing a computer matching agreement, the report reiterated earlier OMB findings "that the procedures for renegotiating agreements for recurring matches, such as would be required for program eligibility verification, require the expenditure of enormous personnel resources with little substantive benefit, and that "verifying eligibility before

---

[41]*Mary Louise Cummings* v. *Department of the Navy*, 2002 WL 226134 (D.C. Cir. No. 00-5348).

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

[43]President's Council on Integrity and Efficiency, Ad Hoc Committee on Benefit Eligibility Verification, *Eligibility Verification Needed to Deter and Detect Fraud in Federal Government Benefit and Credit Programs*, May 1998, p. 3.

[44]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, Oct. 2000.

payments are initiated ... would avoid overpayments and allow agencies to ' ... move from a pay and chase mode to one that is far more proactive and efficient'."[45]

[45]President's Council on Integrity and Efficiency, Ad Hoc Committee on Benefit Eligibility Verification, *Eligibility Verification Needed to Deter and Detect Fraud in Federal Government Benefit and Credit Programs*, p. 4.

Influenced by Californiaâ€™s Consumer Privacy Act and Europe Unionâ€™s General Data Protection Regulation, a wave of new data privacy legislation has been introduced across the United States. Visit this page for the latest developments during this critical juncture in US privacy regulation. Californiaâ€™s Consumer Privacy Act (CCPA). The far-reaching Consumer Privacy Act of 2018 (CCPA) requires many companies doing business in California to implement new policies and procedures no later than July 1, 2020. The CCPA can be enforced by the California Attorney General or by private plaintiffs with the p