Congressional Research Service
Informing the legislative debate since 1914

The Privacy Act of 1974: Overview and Issues for Congress

December 7, 2023

Congressional Research Service
https://crsreports.congress.gov
R47863

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47863

December 7, 2023

Meghan M. Stuessy
Analyst in Government Organization and Management

The Privacy Act of 1974: Overview and Issues for Congress

The Privacy Act of 1974 (Privacy Act; 5 U.S.C. §552a) prescribes how federal agency records with individually identifying information are to be stored, who may access such information, and when the government may use or disclose it. The act represents an expansion of the concept of privacy beyond a narrow, property-based concept and the beginnings of understanding privacy based on the content of the information itself rather than its paper or electronic format.

In brief, the Privacy Act governs federal agencies' access, use, and disclosure of information concerning individuals. This information concerning individuals is sometimes referred to as *personally identifiable information*, or PII. With 12 exceptions, information on individuals may not be disclosed without the prior written consent of the individual. The statute also provides 10 exemptions for categories of records that are outside the scope of the Privacy Act's protections.

For purposes of the Privacy Act, an agency may control a group of records where information is retrievable by an individual's name or other unique identifier. This group of records is referred to as a *system of records*. When an agency seeks to establish a new system of records or make significant changes to an existing system of records, the act requires the agency to submit a proposal to the Office of Management and Budget (OMB) and Congress. After review and potential comments from OMB, the agency publishes a system of records notice, or SORN, in the *Federal Register*.

Certain agency officials, including chief information officers (CIOs) and senior agency officials for privacy (SAOPs), are required to oversee the implementation of the Privacy Act's protections into agency information management processes as stipulated through statute and OMB guidance. In addition, the E-Government Act of 2002 (P.L. 107-347) requires CIOs to conduct privacy impact assessments (PIAs) as part of their agencies' privacy programs. A PIA documents what information the agency is collecting and why, with whom the information will be shared, what notice or opportunities for consent would be provided to individuals regarding information collection and sharing, and whether a system of records is being created, among other elements.

Almost 50 years after the statute's initial enactment and as information technology advances, opportunities for use and misuse of individually identifying information may be present in ways not originally considered. When Congress enacted the Privacy Act, it incorporated into statute the Fair Information Practice Principles (FIPPs), a series of tenets intended to guide the oversight, ethical use, and protection of information on individuals. These principles, when combined with the definitions provided in the Privacy Act regarding the types and storage of information subject to its requirements, have ongoing implications for how policymakers may seek to balance individual rights to privacy against public interests in transparency and government efficiency.

While government information can be inherently valuable for researchers, members of the public, and other agencies or governments, uncontrolled access to information may also put individual privacy at risk. OMB has warned of the *mosaic effect*, a problem that could occur when an isolated de-identified information source is combined with other available information, creating re-combined sensitive information on an individual. Developments in computer science and statistics have created new methods of protecting PII while facilitating ethical use of the information. In this light, Congress may wish to examine whether the Privacy Act, in its current form, achieves these principles or whether current agency practices and transparency mechanisms warrant reconsideration.

Contents

Tables

Appendixes

Contacts

Enacted during the 93rd Congress, the Privacy Act of 1974[1] is a product of and response to scandals eroding public trust in the government's handling of personal information, including Watergate and the Federal Bureau of Investigation's Counter Intelligence Program.[2] At the same time, the environment of information management was changing from paper-based recordkeeping to digital formats, allowing for large quantities of information to be exchanged at speeds and distances not previously possible.

Beyond the expanding quantities and speed of information sharing, these new technologies also raised questions about the ability of the government to appropriately store and secure information on individuals. In their corresponding joint report on the Privacy Act's legislative history, the House and Senate Committees on Government Operations found that the "rapid proliferation, at the Federal level, of data banks in the 1960s and 1970s—containing in excess of 1¼ billion separate records on American residents—lent substance to the worries of many that the nation's tradition of limited government was in jeopardy."[3]

Congress had previously passed legislation addressing information access and protection, including the Freedom of Information Act (FOIA),[4] the Fair Credit Reporting Act,[5] and the Family Educational Rights and Privacy Act.[6] With regard to government information, the Privacy Act "represents a landmark achievement in securing for each citizen of the United States the right of privacy with respect to confidential information held by the Federal Government" and is the result of conversations on how to manage and mitigate unintended consequences from computerized recordkeeping.[7]

The Privacy Act prescribes how the government is to store agency records with individually identifying information, who may access information on individuals, and when the government may use or disclose it.[8] Subject to 12 exceptions, the Privacy Act prohibits agency disclosure of records pertaining to an individual without the individual's prior written consent.[9] Under the act,

[1] 5 U.S.C. §552a. The Privacy Act was originally enacted as P.L. 93-579, 88 Stat. 1896.

[2] U.S. Department of Justice (DOJ), *Overview of the Privacy Act of 1974*, 2020, p. 1, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition. DOJ periodically updates this book-length document that it characterizes as a "discussion of various provisions of the Privacy Act, as addressed by court decisions in cases involving the Act's disclosure prohibition, its access and amendment provisions, and its agency recordkeeping requirements." See p. i.

[3] U.S. Congress, Senate Committee on Government Operations and House Committee on Government Operations, *Legislative History of the Privacy Act of 1974, S. 3418 (*P.L. 93-579*): Source Book on Privacy*, committee print, 94th Cong., 2nd sess., September 1976 (Washington: GPO, 1976), p. 1295, https://www.justice.gov/d9/privacy_source_book.pdf.

[4] 5 U.S.C. §552, P.L. 89-487, 80 Stat. 250.

[5] 15 U.S.C. §§1681-1681x, P.L. 91-508, 84 Stat. 1127. For more information about related privacy laws, including the Fair Credit Reporting Act, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[6] P.L. 93-380, §513, 88 Stat. 484, 571-574 (codified at 20 U.S.C. §1232g).

[7] U.S. Congress, Senate Committee on Government Operations and House Committee on Government Operations, *Legislative History of the Privacy Act of 1974, S. 3418 (*P.L. 93-579*): Source Book on Privacy*, committee print, 94th Cong., 2nd sess., September 1976 (Washington: GPO, 1976), p. v, https://www.justice.gov/d9/privacy_source_book.pdf.

[8] For an elaboration of Congress's findings and purposes, see the Privacy Act of 1974, §2 (P.L. 93-579, December 31, 1974; 88 Stat. 1896).

[9] DOJ, *Overview of the Privacy Act of 1974*, p. 80. In addition to the 12 *exceptions* from the written consent requirement, the act also stipulates 10 categories of information that are *exempted* from its purview (see DOJ, *Overview of the Privacy Act of 1974*, p. 338). The Privacy Act's 12 exceptions and 10 exemptions are listed in the **Appendix** of this report.

record means "any item, collection, or grouping of information about an individual that is maintained by an agency" that includes the person's name or another identifier.[10]

In addition, the act assigns responsibility to the director of the Office of Management and Budget (OMB) to develop and issue guidelines and regulations for the act's implementation.[11] OMB first issued Privacy Act guidance in 1975 and has subsequently issued related guidance in the form of circulars and memoranda.[12]

The Privacy Act represents the statutory implementation of the Fair Information Practice Principles (FIPPs), a series of tenets intended to guide the oversight, ethical use, and protection of information on individuals.[13] The Department of Justice (DOJ) explains that these principles

> allow individuals to determine what records pertaining to them are collected, maintained, used, or disseminated by an agency; require agencies to procure consent before records pertaining to an individual collected for one purpose could be used for other incompatible purposes; afford individuals a right of access to records pertaining to them and to have them corrected if inaccurate; and require agencies to collect such records only for lawful and authorized purposes and safeguard them appropriately.[14]

These principles, when combined with the definitions provided in the Privacy Act regarding the types and storage of information subject to its requirements, have ongoing implications for how policymakers may seek to balance individual rights to privacy against public interests in transparency and government efficiency. DOJ further cautions, "Just as loss of trust in the governance framework would harm the interests of all, so proper and appropriate use of personal information within a secure governance framework would maintain trust and benefit the interests of all."[15] In this light, Congress may wish to examine whether the Privacy Act, in its current form, achieves these principles or whether current agency practices and transparency mechanisms warrant reconsideration.

This report provides an overview of the Privacy Act and related issues. This includes an examination of the Privacy Act's underlying privacy-related principles and how the act relates to FOIA in both statutory text and practice. With this foundation, the report details the Privacy Act's key terms, exemptions from its coverage, and exceptions allowing disclosure without obtaining written consent from the individual. The report also provides an overview of agency requirements related to the Privacy Act, including systems of records notices (SORNs), privacy impact assessments (PIAs), and the role of senior agency officials for privacy (SAOPs). The report concludes with a discussion of evolving conceptions of privacy and related issues for Congress.

[10] 5 U.S.C. §552a(4). Other statutory definitions of *record* exist outside of the Privacy Act, such as the Federal Records Act definition, located at Title 44, Section 3301, of the *U.S. Code*. For more information on federal records, see CRS In Focus IF11119, *Federal Records: Types and Treatments*, by Meghan M. Stuessy.

[11] 5 U.S.C. §552a(v).

[12] OMB, "Privacy Act Implementation: Guidelines and Responsibilities," 40 *Federal Register* 28948-28978, July 9, 1975 (hereinafter "1975 Privacy Act Guidance"). OMB collects and publishes its privacy act guidance at https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy.

[13] DOJ, *Overview of the Privacy Act of 1974*, pp. 421-422.

[14] DOJ, *Overview of the Privacy Act of 1974*, p. 1. DOJ elaborates: "Judicial redress is afforded to individuals when an agency fails to comply with access and amendment rights, but only after an internal appeals process fails to correct the problem. Otherwise, liability for damages is afforded in the event of a willful or intentional violation of these rights."

[15] DOJ, *Overview of the Privacy Act of 1974*, p. 3.

The Privacy Act: Principles and Framework

In a 1973 report prepared for the Secretary of Health, Education and Welfare (hereinafter, HEW Report), experts alerted federal government officials of the potential harmful consequences "that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens."[16] Congress used the existing information-sharing framework in FOIA and expanded upon principles of information protection through enactment of the Privacy Act.

While Congress was designing the Privacy Act, agencies were grappling with the promise and peril of centralized recordkeeping on individuals. In the HEW Report, then-Secretary of Health, Education and Welfare Caspar Weinberger warned that the management and dissemination of information on individuals could become a double-edged sword: "On the one hand, it can help to assure that decisions about individual citizens are made on the basis of accurate, up-to-date information. On the other, it demands a hard look at the adequacy of our mechanisms for guaranteeing citizens all the protections of due process in relation to the records we maintain about them."[17]

This section discusses the environment in which the Privacy Act was considered, beginning with the development and incorporation of the FIPPs into the Privacy Act, and how the Privacy Act builds upon and integrates with the disclosure and transparency procedures provided in FOIA.

Fair Information Practice Principles (FIPPs)

The Privacy Act represents the implementation of a shared set of values known as the FIPPs.[18] The Federal Privacy Council, an interagency forum to improve agency privacy practices, has circulated these nine principles that DOJ describes as "central to the framework of the Privacy Act" and informing "the basis of almost every other privacy law and treaty in the world today."[19] In this way, the FIPPs tie the Privacy Act together with other privacy and information management statutes, such as the European Union's General Data Protection Regulation and the U.S. Health Insurance Portability and Accountability Act of 1996.[20] However, unlike these other statutes, which typically regulate companies and other third parties, the Privacy Act is concerned specifically with the federal government's collection, use, and access to information on individuals.

---

[16] Department of Health, Education and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, July 1973, p. viii, https://www.justice.gov/opcl/docs/rec-com-rights.pdf (hereinafter, *HEW Report*). DOJ also discusses the relationship between the Privacy Act and the HEW Report: "[i]n drafting the Privacy Act, Congress relied on [the then] recently published and widely read report," which "represented the first comprehensive study of the risks to privacy presented by the increasingly widespread use of electronic information technologies by organizations" (DOJ, *Overview of the Privacy Act of 1974*, p. 1).

[17] *HEW Report*, p. vi.

[18] *HEW Report*, p. xx.

[19] DOJ, *Overview of the Privacy Act of 1974*, p. 1, and Federal Privacy Council, "Fair Information Practice Principles (FIPPs)," https://www.fpc.gov/resources/fipps/. The text of the nine FIPPs, as detailed by the Federal Privacy Council, is provided in the **Appendix**.

[20] The U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted in P.L. 104-191, 110 Stat. 1936. For more information about associated data protection laws that generally apply to private entities, such as HIPAA and the General Data Protection Regulation, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh. In particular, footnote 65 explains that CRS Report R45631 excludes the Privacy Act because it is a law that is "primarily applicable to government agencies or government employees."

Specifically, the FIPPs provide values to consider when agencies create, collect, use, process, store, maintain, disseminate, or disclose information with an individual's *identifying particular*, such as an individual's name or some identifying number or symbol.[21] Selected principles suggest that agencies, as a best practice:

- provide individuals with appropriate access to view and correct their associated records and seek individuals' consent to use their information;
- minimize the collection and use of individually identifying information and maintain it only for as long as is necessary to accomplish a legally authorized purpose;
- provide notice of the specific purpose and use of individually identifying information; and
- be transparent about its information policies, practices, roles, and responsibilities with respect to individually identifying information.[22]

These principles correspond to provisions of the Privacy Act requiring, for example, that agencies maintain systems of records with only such information about individuals as is relevant and necessary,[23] provide notices in the *Federal Register* about proposed uses of such records,[24] and publish agency procedures for the disclosure to an individual upon request for information pertaining to him or her,[25] among other provisions.

Relationship to the Freedom of Information Act

The Privacy Act builds upon and extends requirements for the federal governance of information from earlier statutes. While FOIA allows any person to request access to government information, DOJ explains that the Privacy Act is designed to maintain trust between individuals and agencies with regard to the use of information on individuals.[26]

FOIA and the Privacy Act are intertwined both in function and statutory placement. Notably, the Privacy Act uses FOIA's definition of *agency*. When agencies process requests for information under the Privacy Act, they must also consider the applicability of FOIA to the request. As DOJ describes, "The Privacy Act and the FOIA are often read in tandem," although the scope of each differs.[27] In practice, agencies generally treat Privacy Act requests in the same manner as FOIA requests when preparing responses. DOJ recommends that agencies process individuals' access

[21] 5 U.S.C. §552a(a)(4). The Privacy Act prohibits agency disclosure of records pertaining to an individual containing the individual's name, number, or *identifying particular*. However, the debate concerning what constitutes an individual's record for the purposes of the Privacy Act has not been definitively resolved. The idea of identifying particulars is further explored in the "Definitions of Key Terms and Scope" section.

[22] The nine FIPPs often overlap with one another. For example, the principle of individual access and amendment dovetails with the principle of individual participation. Similarly, the principle of transparency into agency processes regarding information on individuals can be satisfied with a clear understanding of agency roles and responsibilities, facilitating the principle of accountability. Federal Privacy Council, "Fair Information Practice Principles (FIPPs)."

[23] 5 U.S.C. §552a(e)(1).

[24] These *systems of records notices*, or SORNs, are discussed later in this report in the "Systems of Records Notices (SORNs)" section.

[25] 5 U.S.C. §552a(e)(4).

[26] DOJ, Office of Information Policy, "OIP Guidance: The Interface Between the FOIA and Privacy Act," September 30, 2022, https://www.justice.gov/oip/oip-guidance-interface-between-foia-and-privacy-act.

[27] DOJ, *Overview of the Privacy Act of 1974*, p. 138. For an example of this process, see pp. 141-147.

requests for their own records "under both the Privacy Act and the FOIA, regardless of the statute(s) cited."[28]

Information provided by an agency in response to a records request may be redacted under either FOIA or the Privacy Act and therefore may appear incomplete. While FOIA's main purpose is to inform the public of the federal government's operations, the act excludes certain private and governmental interests from disclosure. FOIA lists nine exemptions from its disclosure requirements that permit (but do not require) agencies to withhold information or records that are otherwise subject to release. These include reasons related to national defense or foreign policy; matters exempted from disclosure under other statutes; and personnel, medical, and similar files.[29]

Definitions of Key Terms and Scope

Moving from the theoretical discussion of what privacy policy could look like, this section examines the statutory framework of the Privacy Act. The Privacy Act governs the access, use, and disclosure of information by agencies and the public. Specifically, the act concerns *agency* use of an *individual's records* that are maintained and retrieved within a *system of records*. Descriptions of these key terms, from both statute and DOJ guidance, are provided below.

- **Agency.** The Privacy Act uses FOIA's definition of *agency*.[30] This definition covers executive branch agencies, their components, and government-controlled entities but excludes Congress, the legislative branch, the White House, federal courts, and state and local governments.[31]
- **Individual.** An *individual* is defined in the act as "a citizen of the United States or an alien lawfully admitted for permanent residence."[32] This definition excludes deceased persons, corporations, or organizations. In certain instances, parents or legal guardians may act on behalf of individuals.[33]
- **Record.** Statute defines *record* as "any item, collection, or grouping of information about an individual that is maintained by an agency" that contains the individual's name, identifying number, or other identifying particular assigned to the individual.[34] Courts have variously interpreted how closely associated the information needs to be with an individual to count as a record for purposes of the Privacy Act.[35] Like FOIA, the Privacy Act pertains only to

[28] DOJ, *Overview of the Privacy Act of 1974*, p. 139.

[29] For more information about the application of FOIA exemptions, see CRS Report R46238, *The Freedom of Information Act (FOIA): A Legal Overview*, by Daniel J. Sheffner.

[30] 5 U.S.C. §552a(a)(1); 5 U.S.C. §552(f)(1).

[31] The definitions of the Privacy Act have been discussed and decided in various court cases. DOJ summarizes relevant caselaw in its *Overview of the Privacy Act*. For a discussion of the definition of *agency*, see DOJ, *Overview of the Privacy Act of 1974*, pp. 15-17. Please note that determining when information becomes an *agency* record may have implications regarding the government's use and purchase of information created by contractors or collected by third parties, such as data brokers. For more information on the federal procurement process and contracting, see CRS Report RS22536, *Overview of the Federal Procurement Process and Resources*, by Dominick A. Fiorentino. For more information on how consumer data may be collected by data brokers, see CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Kristen E. Busch.

[32] 5 U.S.C. §552a(a)(2).

[33] DOJ, *Overview of the Privacy Act of 1974*, pp. 23-26.

[34] 5 U.S.C. §552a(a)(4).

[35] DOJ, *Overview of the Privacy Act of 1974*, pp. 28-36.

federal information, and most courts have held that it does not require agencies to create records.[36]

- **System of Records.** A *system of records* is a "group of any records under the control of any agency" from which the information is retrieved by the name of the individual or other identifying particular.[37]

Identifying Particulars and Personally Identifiable Information (PII)

The Privacy Act prohibits agency disclosure of records pertaining to an individual containing an individual's name, number, or *identifying particular*. However, the debate concerning what constitutes an individual's record for the purposes of the Privacy Act has not been definitively resolved.[38]

As outlined by DOJ, while some courts have broadly interpreted the statute as governing any record linked to an individual's identifying information, others have claimed more narrowly that the record must reflect "some quality or characteristic of the individual involved."[39] Still other courts have held a middle ground approach: Records "must both be 'about' an individual and include his name or other identifying particular."[40] DOJ concludes that additional courts "have adopted different, narrow, and, at times, conflicting interpretations of the term 'record.'"[41] Relatedly, the Privacy Act's protections related to transparency and ethical use of such information hinges on whether or not a series of records is considered a system of records, where the information is queried and retrieved by an identifying particular.[42] These divergent and conflicting interpretations affect the ability of individuals and policymakers to ensure appropriate application of the Privacy Act to such types of records.

In its initial 1975 Privacy Act guidance, OMB provided examples of what would constitute a unique identifying particular. OMB explained that information that "suggests any element of data (name, number) or other descriptor (finger print, voice print, photographs)" could be used to identify individuals. However, OMB also notes that identifying particulars "are not always unique (i.e., many individuals share the same name) but when they are not unique (e.g., name) they are individually assigned—as distinguished from generic characteristics."[43]

More recently, in 2006, OMB began publicly referring to information with identifying particulars as *personally identifiable information* or PII.[44] In 2007, OMB defined PII as "information which

[36] DOJ, *Overview of the Privacy Act of 1974*, p. 37.

[37] 5 U.S.C. §552a(a)(5) and DOJ, *Overview of the Privacy Act of 1974*, p. 37. According to DOJ, in exploring the idea of retrieval, "The statutory definition of a 'system of records' requires that: (1) 'there is an indexing or retrieval capability using identifying particulars built into the system'; and (2) the agency 'does, in fact, retrieve records about individuals by reference to some personal identifier.'" See also OMB, "1975 Privacy Act Guidance," pp. 28948 and 28952.

[38] 5 U.S.C. §552a(a)(4).

[39] DOJ, *Overview of the Privacy Act of 1974*, pp. 28-29.

[40] DOJ, *Overview of the Privacy Act of 1974*, p. 30.

[41] DOJ, *Overview of the Privacy Act of 1974*, p. 33.

[42] DOJ elaborates that "Searching through a box or collection of unidentified photos with the hope of recognizing an inmate does not fit the definition because the photos are not 'retrieved' by any 'assigned' personal identifier." DOJ, *Overview of the Privacy Act of 1974*, p. 38.

[43] OMB, *1975 Privacy Act Guidance*, p. 28952.

[44] OMB, "Safeguarding Personally Identifiable Information," M-06-15, May 22, 2006, p. 1, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2006/m-06-15.pdf.

can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[45] OMB has incorporated this term in related information management documents, such as OMB Circular No. A-130,[46] as well as in guidance concerning the Federal Information Security Management Act (FISMA),[47] the Confidential Information Protection and Statistical Efficiency Act (CIPSEA),[48] and others.

10 Exemptions for Certain Records and Systems of Records[49]

The Privacy Act exempts certain records and systems of records from its coverage in 10 circumstances. These exemptions permit federal government use of individually identifying information in instances where notifying the individual may hinder the purpose of the information sharing, such as in cases of national security or investigations or where the information cannot reasonably be associated with an individual, such as for statistical research.

Of the 10 exemptions, 3 are self-executing, meaning the agency holding the information does not have to take action in order to assert an exemption. Seven exemptions permit agencies to publish rules exempting certain systems of records from specific Privacy Act provisions.[50] A full list of the Privacy Act's 10 exemptions is located in the **Appendix** of this report. Two of these exemptions may warrant particular congressional interest: investigatory material compiled for law enforcement purposes and statistical records.[51]

Investigatory Material[52]

The Privacy Act excludes from its scope investigatory material compiled for law enforcement purposes that did not result in an individual's loss of a right, benefit, or privilege.[53] According to DOJ, this exemption covers:

1. material compiled for other investigative law enforcement purposes by any agency, and
2. material compiled for criminal investigative law enforcement purposes by nonprincipal function criminal law enforcement entities.[54]

---

[45] OMB, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," M-07-16, May 22, 2007, p. 1, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2007/m07-16.pdf. On June 15, 2007, OMB incorporated this definition of *personally identifiable information* in its guidance on implementation of Title V of the E-Government Act of 2002 and the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA); see 72 *Federal Register* 33362-33377. S. 116, introduced in 2005 during the 109th Congress, appears to be the first legislative instance of the term *personally identifiable information*. However, the bill was not enacted. In the years since CIPSEA's implementation, Congress may consider whether OMB's response is still sufficient.

[46] OMB, "Circular No. A-130, Managing Information as a Strategic Resource," July 28, 2016, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.

[47] 44 U.S.C. §§3551-3559, P.L. 107-347, 116 Stat. 2946.

[48] 44 U.S.C. §§3561-3583, P.L. 107-347, 116 Stat. 2962; and P.L. 115-435, 132 Stat. 5544.

[49] Benjamin M. Barczewski, Legislative Attorney, contributed to this section of the report.

[50] 5 U.S.C. §552a(k).

[51] 5 U.S.C. §552a(k)(2) and 5 U.S.C. §552a(k)(4).

[52] Benjamin M. Barczewski, Legislative Attorney, contributed to this section of the report.

[53] 5 U.S.C. §552a(k)(2).

[54] DOJ, *Overview of the Privacy Act of 1974*, p. 357.

The first prong is known as a "general exemption."[55] It permits heads of agencies that perform law enforcement as a principal function (e.g., the Federal Bureau of Investigation or the Drug Enforcement Agency)[56] to promulgate rules to exempt a system of records from Privacy Act coverage when the record falls into one of three categories: (1) "information compiled for the purpose of identifying individual criminal offenders and alleged offenders," (2) "information compiled for the purpose of a criminal investigation," and (3) "reports identifiable to an individual compiled at any stage of the process of enforcement."

The second prong applies to agencies whose principal function is not law enforcement but nonetheless conduct some law enforcement activities. This specific exemption permits agency heads to promulgate rules that exempt any system of records if the records are "investigatory material compiled for law enforcement purposes."[57]

The Privacy Act limits the scope of the special exemption for investigatory material by requiring that individuals have access to investigative records that were used as a basis for denying their rights, privileges, or benefits.[58] Examples of the types of investigations covered by this exemption include investigations of deportability under the Immigration and Nationality Act, taxpayer audits, and attorney misconduct investigations.[59] Information gathered for a routine background check as a condition of federal employment is not usually a law enforcement purpose unless the background check involves specific allegations of illegal activity.[60]

Statistical Records

The Privacy Act also permits agency heads to exempt a system of records when that system of records is "required by statute to be maintained and used solely as statistical records."[61] The Privacy Act defines *statistical record* as "a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual."[62] Relatedly, other statutory provisions that involve the use of information by statistical agencies or units define *statistical purpose* as involving the description,

[55] 5 U.S.C. §552a(j)(2). The sweep of the Privacy Act's general exemption is broad and includes records compiled at any stage of a criminal investigation through incarceration and release of a criminal defendant. Courts have held that records including psychological reports compiled while an individual was incarcerated and investigation reports that did not lead to prosecution are exempt from the Privacy Act. See, for example, Taccetta v. FBI, No. 10-6194, 2012 WL 2523075, at *5 (D.N.J. Jun. 29, 2012) (holding that all records created by FBI in investigating violations of criminal law are exempt); Kates v. King, 487 F. App'x 704, 706 (3d Cir. 2012) (per curiam) (finding that the Bureau of Prisons has exempted its central record system). See, for example, Jordan v. Dep't of Justice, 668 F.3d 1188, 1201-02 (10th Cir. 2011) (psychological records of inmate); Smith v. Treasury Inspector Gen. for Tax Admin., No. JKB-11-2033, 2011 WL 6026040, at *3 (D. Md. Dec. 1, 2011), *aff'd per curiam*, 474 F. App'x 929 (4th Cir. 2012) (investigation report not leading to prosecution).

[56] Courts have held that the following agencies are also principal law enforcement agencies: the Federal Bureau of Prisons, U.S. Attorney's offices, the Naval Criminal Investigative Service, the Criminal Investigation Division of the Internal Revenue Service, the U.S. Secret Service, the Postal Inspection Service, and offices of inspector general, among others. See DOJ, *Overview of the Privacy Act of 1974*, pp. 342-344.

[57] 5 U.S.C. §552a(k)(2).

[58] 5 U.S.C. §552a(k)(2).

[59] DOJ, *Overview of the Privacy Act of 1974*, pp. 357-358.

[60] Vymetalik v. FBI, 785 F.2d 1090, 1093-98 (D.C. Cir. 1986) (routine background checks generally exempt); Strang v. U.S. Arms Control & Disarmament Agency, 864 F.2d 859, 862-63 n.2 (D.C. Cir. 1989) (investigation of existing employee for alleged violations of national security violations).

[61] 5 U.S.C. §552a(k)(4).

[62] 5 U.S.C. §552a(a)(6). The definition of *statistical record* does not include records covered by Title 13, Section 8, of the *U.S. Code*, which governs the use of certain records created during the decennial census.

estimation, or analysis of the characteristics of groups without identifying the individuals or organizations that comprise such groups.[63]

OMB's 1975 Privacy Act guidelines state that the purpose of this exemption is to permit use of records for statistical research or program evaluation that, by law, cannot be used to make a determination about an individual.[64] Records that are subject to this exemption, accordingly, cannot be used to make decisions about the rights, benefits, or entitlements of any individual.[65] Due to the fact that these records are used entirely for statistical purposes, Congress did not believe that disclosure would provide any benefit to an individual because they have no direct effect on any individual in particular.[66]

As a matter of policy and practice, however, the delineation between statistical records and other types of records may be artificially clear. While statistical records can be construed to be information where the identity of the subject is separated from other data in the record, experts at the time of the Privacy Act's initial consideration did note that data from administrative records containing individually identifiable information could sometimes be used for statistical purposes.[67] Use of statistical records is further explored in the "Statistical Information and Census" portion of this report.

Conditions of Disclosure

The Privacy Act allows individuals to request and view their information from agencies and generally prohibits disclosure of individually identifiable information to third parties without written consent. Specifically, an agency may not disclose a record to a third party without the individual's prior written consent unless such a disclosure falls under an exception in Title 5, Section 552a(b), of the *U.S. Code*.[68] This section examines the Privacy Act's individual right of amendment, how disclosure to third parties operates under the act, and recent developments related to the act's written consent requirement in a digital age.

Disclosure to the Individual

U.S. citizens and lawful permanent residents may request access to their information from agencies under the same guidelines as requests under FOIA.[69] An individual may request an agency to perform a search for information in a system of records based on his or her identifiers, such as a name or Social Security number. An individual might do this, for example, to ensure that his or her records are accurate and in order to request corrections.

[63] The definition continues to include "the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described" as relating to description, estimation, or analysis of groups. Inversely, the statute defines *nonstatistical purpose* in part as "the use of data in identifiable form for any purpose that is not a statistical purpose, including any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular identifiable respondent." See 44 U.S.C. §3561(8) and §3561(10).

[64] OMB, *1975 Privacy Act Guidance*, p. 28973.

[65] OMB, *1975 Privacy Act Guidance*, p. 28973.

[66] U.S. Congress, House Committee on Government Operations, *Privacy Act of 1974*, report to accompany H.R. 16373, 93rd Cong., H.Rept. 93-1416, p. 19.

[67] *HEW Report*, p. 6.

[68] For discussion of these exceptions, see DOJ, *Overview of the Privacy Act: 2020 Edition*, "Conditions of Disclosure to Third Parties," https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties.

[69] 5 U.S.C. §552a(d).

Consistent with the FIPPs principle of access and amendment, the Privacy Act permits individuals to gain access to their records or any information pertaining to them for purposes of review. An individual may also be accompanied by another person to review the records.[70]

Individuals are also statutorily able to request amendment of their records should they believe the records are not "accurate, relevant, timely, or complete," and agencies are to acknowledge such a request in writing within 10 business days.[71] The agency must then inform the individual of whether it has decided to make the correction or, in the event the agency refuses, provide and explain to the individual the reason for the refusal, agency procedures to request a review of the refusal by the agency head or an officer designated by the agency head, and the name and business address of that officer.

Disclosure to Third Parties

Commonly, the need for an individual's written consent to disclose his or her documents to third parties arises in conducting congressional casework and during agency processing of benefits (for example, the administration of military and veterans' benefits). In these instances, the third party is often coordinating among federal agencies or governments on behalf of the individual for benefits administration, information correction, or research purposes.

Congressional Casework[72]

In conducting casework, Members of Congress routinely solicit and respond to requests from constituents for assistance with federal agencies. In general, an agency cannot reply to a congressional inquiry without a Privacy Act release form signed by the constituent requesting assistance. The form authorizes the Member to access a constituent's individually identifiable information to assist in the resolution of a case and prevents the unauthorized disclosure of individually identifying information.[73]

Manually obtaining a signed privacy release form and transmitting the form to an agency has been a time-consuming process for both constituents and caseworkers, which sometimes delays consideration of the case by an agency. In addition, agencies across the federal government have required different versions of privacy release forms specific to their agencies. Some agencies have accepted electronic versions of privacy release forms from congressional offices in a variety of formats despite lacking clear authorization to do so. This has raised casework management concerns in some congressional offices. A discussion on efforts to modernize this process, including the creation of privacy release form templates, follows in the "Written Consent" section below.

Veterans' Benefits and Next of Kin

Military servicemembers, veterans, and next of kin frequently seek access to military service records to receive related benefits, correct their service information, or conduct family research.[74]

[70] 5 U.S.C. §552a(d).

[71] 5 U.S.C. §552a(d)(2). However, the act also specifies at Section 552a(d)(5) that this right of access does not allow an individual access to information compiled in "reasonable anticipation of a civil action or proceeding."

[72] R. Eric Petersen, Specialist in American National Government, contributed to this section of the report.

[73] For more information on casework, see CRS Report RL33209, *Casework in a Congressional Office*, by R. Eric Petersen and Sarah J. Eckman.

[74] For more information about requesting military service records and associated challenges, see CRS Report R47212, *Modernizing Access to Military Service Records: Frequently Asked Questions*, by Meghan M. Stuessy.

Disclosure of military service records, like other individually identifiable information the federal government maintains, is restricted by the Privacy Act. The Privacy Act pertains to living U.S. citizens and lawful permanent residents, and the courts and DOJ have interpreted the Privacy Act's definition of *individual* to exclude deceased individuals.[75]

To comply with the Privacy Act, the agency solicits written consent of the servicemember via completion of form SF-180.[76] The form notes that FOIA provisions may restrict the release of complete information. However, the servicemember or his or her authorized legal recipient has "access to almost any information" contained in the servicemember's own record.[77]

Requests for a living servicemember's records by someone other than the servicemember must be accompanied by the signature of the servicemember, court appointment documentation, authorization letter, or proof of power of attorney in order for documents to be released to the servicemember, next of kin, or authorized representative. Next of kin can receive greater access to a deceased veteran's records than a member of the general public by submitting proof of the servicemember's death with the form SF-180.[78]

Written Consent[79]

While the Privacy Act explicitly requires an individual's written consent, continued movement toward electronic recordkeeping has renewed conversations about how agencies can best solicit individuals' written consent while also streamlining the agencies' processes and user experience with government. The statute, however, does not further define the components of written consent.[80]

Agencies have generally interpreted this requirement as requiring a paper document with a "wet" signature, which may be either notarized or submitted to the agency under penalty of perjury.[81] Certain agencies may also require additional information from the individual to verify his or her identity, including such information as current address and date and place of birth.[82] Individuals may opt to include their Social Security numbers in the request but are not mandated to disclose their Social Security numbers unless required by statute.[83] Further, the Privacy Act does provide

[75] DOJ, *Overview of the Privacy Act of 1974*, p. 24.

[76] Form SF-180 provides an instruction and information sheet that explains the procedures required to request and release military service records in detail. See also National Archives and Records Administration (NARA), "Standard Form 180—Requests Pertaining to Military Records," https://www.archives.gov/files/research/order/standard-form-180.pdf.

[77] NARA, "Standard Form 180."

[78] The form specifies that such proof can include a DD Form 1300, Casualty Report, copy of a death certificate, newspaper article (obituary), or death notice, among other documents.

[79] R. Eric Petersen, Specialist in American National Government, contributed to this section of the report.

[80] DOJ, *Overview of the Privacy Act of 1974*, p. 77.

[81] OMB, "Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act," M-21-04, November 12, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-04.pdf; and NARA, "Guide to Making a Privacy Act Request: What Is a Privacy Act Certification of Identity?," https://www.archives.gov/privacy/guide.html.

[82] See, for example, DOJ's requirements at Title 28, Section 16.41(d), of the *Code of Federal Regulations*.

[83] The Privacy Act makes it unlawful for any local or state government or the federal government to deny a right, privilege, or benefit because a person refuses to provide his or her Social Security number. The Social Security number disclosure limitation applies only where a person has been denied a right, benefit, or privilege as a result of not providing a Social Security number. If no right, benefit, or privilege was denied, simply requesting that a person disclose his or her Social Security number does not violate the Privacy Act (5 U.S.C. §552a note). The limitation on (continued...)

that "Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000."[84]

Intending to modernize and simplify the written consent process, Congress enacted the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act).[85] The CASES Act required OMB to issue guidance requiring agencies to (1) accept electronic identity proofing and authentication processes, (2) create templates for electronic consent and access forms and require posting of the templates on agency websites, and (3) accept electronic consent and access forms. Agencies were required to comply with implementation guidance in OMB Memorandum M-21-04 by November 21, 2021.[86]

However, implementation of electronic identity proofing may continue to be of interest to Congress. OMB Memorandum M-21-04 requires agency implementation to conform to OMB privacy guidance and related National Institute of Standards and Technology (NIST) standards.[87] Challenges related to electronic identity proofing remain, as recently demonstrated by a March 2023 General Services Administration (GSA) inspector general report finding that Login.gov, "a single-sign on solution for government websites," was not meeting NIST electronic identity proofing criteria.[88] As of April 14, 2023, NIST has concluded its call for comments on its initial public draft revision to its digital identity guidelines.[89] This revision may impact both implementation of the CASES Act and administration of Login.gov.[90]

12 Exceptions to Written Consent[91]

Information on an individual may be shared with other persons, such as congressional caseworkers or government agencies, subject to the Privacy Act's written consent requirement. However, the Privacy Act also provides 12 exceptions to the written consent requirement from

disclosing Social Security numbers appears in a "Historical and Statutory" note following Section 552a. That it is included in a statutory note rather than codified as part of Section 552a does not diminish its legal import. See Stephan v. United States, 319 U.S. 423, 426 (1943) (holding "the Code cannot prevail over the Statutes at Large when the two are inconsistent"). See, for example, El-Bey v. N.C. Bd. of Nursing, No. 1:09CV753, 2009 WL 5220166, at *2 (M.D.N.C. Dec. 31, 2009).

[84] 5 U.S.C. §552a(i)(3).

[85] P.L. 116-50. The act further explains that it is the sense of Congress that agency interactions with constituents "should be simplified through the creation of electronic forms that may be submitted" under the Privacy Act. For more information about the CASES Act, see CRS In Focus IF12159, *The CASES Act: Implementation and Issues for Congress*, by Meghan M. Stuessy and R. Eric Petersen; and CRS In Focus IF12382, *The CASES Act: Implementation Challenges*, by R. Eric Petersen.

[86] OMB, M-21-04.

[87] See OMB, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," M-19-17, May 21, 2019, https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf. See also David Temoshok et al., *Digital Identity Guidelines*, NIST SP 800-63-4 (Initial Public Draft), NIST, December 16, 2022, https://csrc.nist.gov/pubs/sp/800/63/4/ipd.

[88] See also CRS In Focus IF12395, *Login.gov: Administration and Identity Authentication*, by Dominick A. Fiorentino, Natalie R. Ortiz, and Meghan M. Stuessy; and General Services Administration, Office of Inspector General, *GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards*, March 7, 2023, https://www.gsaig.gov/content/gsa-misled-customers-logingovs-compliance-digital-identity-standards.

[89] For a timeline of NIST's efforts to update NIST SP 800-63-4, see NIST, "Roadmap: NIST Special Publication 800-63-4 Digital Identity Guidelines," https://www.nist.gov/identity-access-management/roadmap-nist-special-publication-800-63-4-digital-identity-guidelines.

[90] The public comment period for the revision to NIST SP 800-63-4 was extended to April 14, 2023, from March 24, 2023. Temoshok et al., *Digital Identity Guidelines*.

[91] Benjamin M. Barczewski, Legislative Attorney, contributed to this section of the report.

individuals, which may raise questions about the interpretation and intended use of these exceptions by government agencies. A full list of these exceptions is located in the **Appendix** of this report.

Three of the exceptions have at times raised particular congressional concern. First, the Privacy Act permits an agency to disclose covered information with other employees of the same agency who have a *need to know* the information. Second, an agency can disclose information to the public if FOIA requires its disclosure. Third, an agency may disclose information if the purpose of the disclosure is a *routine use* of the information. A routine use, under the Privacy Act, is "use of such record for a purpose which is compatible with the purpose for which it was collected" and may include the sharing of information across agencies.[92]

Need to Know[93]

The Privacy Act permits an agency to disclose records covered by the Privacy Act "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties."[94] This exception is known as the *need to know* exception, and it permits intra-agency disclosures for necessary, official purposes.

The need to know exception applies when the employee receiving the information—rather than the employee disclosing it—has a need for access to the information. In some circumstances, the need to know exception covers contractors who serve the function of agency employees.[95]

The need for access to information includes a broad range of agency activities. Whether a need for the information truly exists, however, is determined on a case-by-case basis. In general, courts have held that intra-agency disclosure of records related to personnel or employment matters, medical treatment or expenses, administrative duties, and national security risks can all fall into the need to know exception so long as the information is needed to perform the receiving employee's duties.[96] The need for access is not unlimited, however. Courts have generally found that a need for access to information does not exist in instances where disclosing information serves to embarrass, discredit, or reveal personal information unrelated to the work of the agency.[97]

Disclosure Under FOIA[98]

The Privacy Act does not prohibit disclosure in cases where FOIA requires disclosure.[99] FOIA creates a presumption that all agency records are open to the public.[100] However, that broad presumption in FOIA is tempered by FOIA's nine statutory exemptions, which serve as reasons that an agency can invoke to withhold information.[101] FOIA's exemptions allow an agency to

---

[92] 5 U.S.C. §552a(a)(7).

[93] Benjamin M. Barczewski, Legislative Attorney, contributed to this section of the report.

[94] 5 U.S.C. §552a(b)(1).

[95] See Mount v. U.S. Postal Serv., 79 F.3d 531, 532-34 (6th Cir. 1996).

[96] See DOJ, *Overview of the Privacy Act of 1974*, pp. 83-88.

[97] See DOJ, *Overview of the Privacy Act of 1974*, p. 88.

[98] Benjamin M. Barczewski, Legislative Attorney, contributed to this section of the report.

[99] 5 U.S.C. §552a(b)(2).

[100] 5 U.S.C. §552(a).

[101] See CRS Report R46238, *The Freedom of Information Act (FOIA): A Legal Overview*, by Daniel J. Sheffner; and CRS Report R41933, *The Freedom of Information Act (FOIA): Background, Legislation, and Policy Issues*, by Meghan (continued...)

withhold an agency record, but an agency is not required to invoke an exemption even if one would be applicable. Under FOIA alone, agencies generally have discretion to invoke one or more of the exemptions to withhold information.[102]

The Privacy Act's FOIA exception is limited, however. The FOIA exception permits disclosure only where FOIA requires disclosure—that is, in situations in which no FOIA exemption applies. Where a FOIA exemption is applicable (i.e., when an agency can choose to withhold the record), the Privacy Act requires the agency to withhold the record from disclosure.

Among the nine classes of records FOIA exempts from disclosure, two are most likely to arise in the Privacy Act context.[103] FOIA permits agencies to withhold personnel files, medical files, or similar files "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[104] FOIA also permits agencies to withhold "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information … could reasonably be expected to constitute an unwarranted invasion of personal privacy."[105]

Routine Use

One of the most discussed and debated exceptions is the *routine use* exception, which was included to allow individually identifiable information disclosures "for a purpose which is compatible with the purpose for which it was collected."[106]

As described by DOJ:

> Courts have generally held that routine use disclosures to process an individual's application for a benefit, program participation, or a position are "compatible" disclosures under the routine use disclosure exception.[107]

Determining a qualifying routine use is often left to the discretion of agencies and OMB, although routine uses must be noted and defined in publicly available SORNs.[108] As a result, agency and court interpretations of the routine use exception may both help and hinder the sharing of information for a variety of purposes, including congressional casework, benefits and program administration, and law enforcement.

The application and interpretation of routine use may therefore warrant congressional interest. In addition to legislative options, Congress, in its oversight efforts, may consider directing agencies to proactively review their interpretation of compatible routine uses to make agencies more responsive and to improve constituent interactions with the federal government.

M. Stuessy. 5 U.S.C. § 552(b); see also Trea Senior Citizens League v. U.S. Dep't of State, 923 F. Supp. 2d 55, 62 (D.D.C. 2013) (describing exemption as permitting an agency to withhold information that is otherwise responsive to FOIA).

[102] 5 U.S.C. §552(b); Davis v. DOJ, 968 F.2d 1276, 1279 (D.C. Cir. 1992).

[103] 5 U.S.C. §§552(b)(6), (7).

[104] 5 U.S.C. §552(b)(6).

[105] 5 U.S.C. §552(b)(7).

[106] 5 U.S.C. §552a(a)(7).

[107] DOJ, *Overview of the Privacy Act of 1974*, p. 108.

[108] 5 U.S.C. §552a(r). See also OMB, "Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," December 23, 2016, p. 11, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdfp.

Statistical Information and Census[109]

An agency may also disclose information for use in statistical research. The Privacy Act states that the recipient of this information must provide the agency with "advance adequate written assurance that the record will be used solely as a statistical research or reporting record" and that the information is to be "transferred in a form that is not individually identifiable."[110] Concerning this exception, OMB commented in its 1975 Privacy Act guidelines that:

> One may infer from the legislative history and other portions of the Act that an objective of this provision is to reduce the possibility of matching and analysis of statistical records with other records to reconstruct individually identifiable records. An accounting of disclosures is not required when agencies publish aggregate data so long as no individual member of the population can be identified.[111]

To further facilitate statistical activities, OMB has issued a series of directives to provide standards and guidelines for statistical surveys; maintaining, collecting, and presenting federal data on race and ethnicity; and responsibilities of federal statistical agencies (FSAs) and statistical units.[112] With respect to FSA roles and responsibilities, OMB Statistical Policy Directive No. 1 is incorporated in part into the CIPSEA protections and requires FSAs to provide a uniform approach "any time an agency pledges to keep confidential the information it collects exclusively for statistical purposes."[113] Additionally, OMB requires FSAs to use sound scientific and statistical limitation techniques to minimize risking re-identification of respondents' data.[114]

The Privacy Act also acknowledges Census Bureau–specific protections for statistical information. Under Title 13 of the *U.S. Code*, the Census Bureau is prohibited from using any data collected from its surveys "for any purpose other than the statistical purposes for which it is supplied," and any data collected during a Census Bureau survey may be accessed only by Department of Commerce and Census Bureau officers or employees.[115] Additionally, published data must be de-identified.[116]

Agency Requirements and Roles

The Privacy Act prescribes certain agency requirements regarding accountability for and transparency into disclosures of individually identifying information. In addition to being required to keep an accurate accounting of disclosures, including to whom they are made and their purpose, agencies are obligated to issue and maintain SORNs and conduct PIAs for individually identifiable information that the agency maintains.[117]

---

[109] Taylor R. Knoedl, Analyst in American National Government, contributed to this section of the report.

[110] 5 U.S.C. §552a(b)(5).

[111] OMB, *1975 Privacy Act Guidance*, p. 28954.

[112] See also CRS Insight IN12197, *The Federal Statistical System: A Primer*, by Taylor R. Knoedl.

[113] OMB, "Statistical Policy Directive No. 1: Fundamental Responsibilities of Federal Statistical Agencies and Recognized Statistical Units," 79 *Federal Register* 71610-71616, December 2, 2014, p. 71611. CIPSEA is codified at Title 44, Sections 3561-3583, of the *U.S. Code* and was originally enacted as part of the E-Government Act of 2002 at P.L. 107-347, 116 Stat. 2962. The law was later amended in 2018 by P.L. 115-435, 132 Stat. 5544.

[114] For more information on the development of statistical limitation techniques, see "What Is Considered to Be "Identifiable Form"?" below.

[115] 13 U.S.C. §9(a)(1) and (3). The limits in Section 9(a) do not apply to censuses of governments under chapter 5 of Title 13. See 13 U.S.C. §9(b).

[116] 13 U.S.C. §9(a)(2).

[117] 5 U.S.C. §552a(c).

To help administer the Privacy Act, OMB requires agencies to designate SAOPs. SAOPs, in cooperation with CIOs, are charged with agency implementation of these requirements. This section further explores agency requirements and roles in Privacy Act implementation.

Systems of Records Notices (SORNs)

For purposes of the Privacy Act, an agency may control a group of records where information is retrievable by an individual's name or other unique identifiers. As noted earlier, this group of records is referred to as a *system of records*.[118] When an agency seeks to establish a new system of records or make significant changes to an existing system of records, the act requires the agency to submit a proposal to OMB and Congress.[119] OMB explains that a significant change that would require submission of a revised SORN could include, for example:

- a substantial increase in the number, type, or category of individuals about whom the records are maintained in the system, or a change that expands the types or categories of records in the system;
- a change that modifies the scope of the system or the purpose for which the information is maintained; and
- a new routine use or significant change to an existing routine use.[120]

After review and potential comments from OMB, the agency publishes a SORN in the *Federal Register* and provides 30 days for the public to submit written views on the proposed use of the system.[121] A typical SORN must include information such as:

- the name and location of the system;
- the categories of records and individuals on whom records are maintained;
- each routine use of the records contained in the system, including the categories of users and the purpose of such use; and
- the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.[122]

As described above, certain systems of records may be exempted from selected Privacy Act requirements by an agency head based on the system's contents and subject to notice in the *Federal Register*.[123]

---

[118] 5 U.S.C. §552a(a)(5).

[119] 5 U.S.C. §552a(r). The proposal is to enable "an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals." See also OMB, "Circular No. A-108," p. 14.

[120] OMB developed a list of examples of significant changes requiring a revised SORN at OMB, "Circular No. A-108," pp. 5-6.

[121] 5 U.S.C. §552a(e)(11). OMB guidance indicates that a SORN is considered in effect upon publication in the *Federal Register* with the exception of "any new or significantly modified routine uses." OMB further explains, "Agencies shall publish notice of any new or significantly modified routine use sufficiently in advance of the proposed effective date of the routine use to permit time for the public to comment and for the agency to review those comments. In no circumstance may an agency use a new or significantly modified routine use as the basis for a disclosure fewer than 30 days following Federal Register publication." OMB, "Circular No. A-108," p. 7. For a brief description of the OMB director's government-wide roles under the Privacy Act, see OMB, "Circular No. A-108," p. 31.

[122] 5 U.S.C. §552a(e)(4). See also OMB, "Circular No. A-108," p. 16. OMB provides SORN templates in Appendices II, III, and IV of Circular No. A-108.

[123] 5 U.S.C. §§552a(j) and 552a(k). For discussion of statutory provisions that explicitly exempt or allow agencies to exempt certain categories of records (or information within records) from certain Privacy Act provisions, see DOJ, *Overview of the Privacy Act of 1974*, pp. 338-372, and OMB, "Circular No. A-108," p. 25.

The Federal Privacy Council maintains an online SORN dashboard, which pulls SORNs from the *Federal Register* and allows for targeted searching of SORNs for "government privacy analysts and privacy lawyers to make it easier."[124] Given the development of this additional tool to search SORNs, Congress may consider whether SORNs are sufficiently accessible and understood by the public in their current format.

Privacy Impact Assessments (PIAs)

Adjusting government processes and aspects of the Privacy Act to the electronic age, Section 208 of the E-Government Act of 2002[125] requires federal agencies to conduct PIAs to ensure sufficient protections for the privacy of personal information when the information is in an identifiable form. Per statute, PIAs are to be reviewed by the agency CIO, or equivalent official, as determined by the head of the agency.[126] Elements required to be addressed in a PIA include:

- what information is to be collected,
- why the information is being collected,
- the information's intended agency use,
- with whom the information will be shared,
- what notice or opportunities for consent would be provided to individuals regarding information collection and sharing,
- how the information will be secured, and
- whether a system of records is being created.[127]

Further, the act defines *identifiable form* as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."[128] In the accompanying OMB Memorandum M-03-22, a PIA is required to be performed and "updated as necessary" when a change creates new privacy risks, including, for example, (1) when agencies convert paper-based records to electronic systems; (2) when functions applied to an existing information collection change anonymous information into information in identifiable form; or (3) when agencies adopt or alter business processes to allow for the merging, centralization, or matching of information with other databases.[129]

[124] GSA and Federal Privacy Council, "SORN Dashboard: About," https://sorndashboard.fpc.gov/about. The Federal Privacy Council is further discussed in the "Federal Privacy Council" section of this report.

[125] P.L. 107-347; 116 Stat. 2899. Section 208 of the E-Government Act of 2002 is located in chapter 35 of Title 44, Section 3501 note, of the *U.S. Code*. Chapter 35 of Title 44 focuses on OMB coordination of federal information policy, as opposed to the broader administrative procedure statutes of Title 5 of the *U.S. Code*, where provisions associated with FOIA and the Privacy Act are located. The act's Title 44 location underscores the role of OMB to guide information policy as informed by the Privacy Act.

[126] 44 U.S.C. §3501 note; P.L. 107-347, 116 Stat. 2922.

[127] 44 U.S.C. §3501 note. Example PIA templates may be viewed at Consumer Financial Protection Bureau, "Privacy Impact Assessment Template," https://files.consumerfinance.gov/f/documents/cfpb_pia-template.pdf, and U.S. Department of Commerce, *Privacy Impact Assessment Template*, https://www.osec.doc.gov/opog/privacy/PIA_Template.pdf.

[128] 44 U.S.C. §3501 note; P.L. 107-347, 116 Stat. 2923.

[129] OMB, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," M-03-22, September 26, 2003, p. 4, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2003/m03_22.pdf.

In 2010, OMB provided additional guidance on PIAs for agency use of third-party websites and applications.[130] Congress might evaluate whether the current statute and guidance environment provide adequate considerations given the changes in information management since the law's passage in 2002. Additionally, Congress may inquire whether agency staff has sufficient training or guidance from OMB to understand when new collections, format changes, or modifications to information could create privacy risks that would necessitate an updated PIA.

Senior Agency Officials for Privacy

While CIOs are established by law, OMB administratively directed agencies to designate SAOPs.[131] In combination, CIOs and SAOPs have key roles in the administration and oversight of agency activities covered by the Privacy Act, including information disclosure, privacy, and statistical policy. In 2016, as directed by Executive Order 13719, OMB issued Memorandum M-16-24, which further defined the designation process and role for an SAOP.

Under OMB Memorandum M-16-24, an SAOP is to be a senior official at the Deputy Assistant Secretary or equivalent level who is "positioned highly enough within the agency to regularly engage with other agency leadership, including the head of the agency."[132] In addition, the SAOP is to have the necessary skills, knowledge, expertise, and agency authority to lead and direct the agency's privacy program and related privacy functions.[133] Notably, OMB Memorandum M-16-24 does not prohibit an agency CIO from serving as the SAOP, meaning that in some agencies, the CIO may serve in both positions.[134]

OMB explains that the SAOP role is also responsible for an agency's policy making functions, compliance, and risk management for privacy. The SAOP is to lead and address the agency's evaluation of the privacy implications of legislative proposals, congressional testimony, and other materials. In addition to monitoring compliance with the Privacy Act and FISMA as directed in separate OMB guidance,[135] the SAOP is to oversee, coordinate, and facilitate agency compliance

[130] Kevin Neyland, *Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications*, OMB, December 29, 2011, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/inforeg/inforeg/info_policy/model-pia-agency-use-third-party-websites-and-applications.pdf.

[131] 44 U.S.C. §3506(a)(2); OMB, "Designation of Senior Agency Officials for Privacy," M-05-08, February 11, 2005, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2005/m05-08.pdf.

[132] OMB, "Role and Designation of Senior Agency Officials for Privacy," M-16-24, September 15, 2016, p. 2, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m_16_24_0.pdf.

[133] Appendix II of OMB Circular A-130 details the many components of an agency's privacy program. See OMB, "Circular No. A-130," Appendix II – 1-20.

[134] The creation of other officials within agencies, such as chief data officers, raises additional questions regarding the relationship and hierarchy of the CIO to these other officials. For more information on the role of chief data officers as it relates to CIOs, see CRS In Focus IF12299, *The OPEN Government Data Act: A Primer*, by Meghan M. Stuessy.

[135] 44 U.S.C. §§3551-3559; OMB, M-05-08.

with the Paperwork Reduction Act (PRA),[136] the E-Government Act of 2002,[137] and OMB Circulars A-130 and A-108,[138] among other statutes and guidance.

Lastly, the SAOP is also to manage and review privacy risks associated with any agency activities that involve "the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems."[139]

The Privacy Act originally required the President to submit a biennial report to Congress about Privacy Act implementation and administration, although this requirement was repealed.[140] OMB explains that in place of this report, OMB now reports to Congress on agencies' compliance with privacy requirements through the annual FISMA report, which is informed by and populated with information collected from SAOPs.[141]

Federal Privacy Council

The Federal Privacy Council was established in 2016 by Executive Order 13719 and includes the SAOPs of 25 agencies as its members. As part of its responsibilities, the council is to coordinate with the Federal CIO Council to promote consistency and efficiency across the executive branch with regard to privacy and information security issues.[142] In addition, the council is to develop recommendations on policy for OMB; coordinate and share best practices with regard to protecting privacy; and assess and recommend how to address the hiring, training, and professional development needs of the federal government with respect to privacy matters.[143]

Issues for Congress: The Privacy Act and the Future of Privacy Policy

In the Privacy Act's 1974 enumeration of findings and purposes, Congress found that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."[144] In many ways, the Privacy Act represents an expansion of the concept of privacy beyond "a narrow-

[136] 44 U.S.C. §§3501-3521. The PRA was originally enacted in 1980 (see P.L. 96-511; 94 Stat. 2812) and reauthorized in 1995 (see P.L. 104-13; 109 Stat. 163).

[137] P.L. 107-347, 116 Stat. 2922. The E-Government Act of 2002 contained the original 2002 version of CIPSEA in Title V. However, agency roles related to the implementation and oversight of CIPSEA may be shared or have shifted over time. Under Title 44, Section 3506(a)(2), of the *U.S. Code*, for example, the CIO has responsibilities for implementation of federal information policy (Subchapter I), but it appears that in the statutory text, for purposes of CIPSEA (Subchapter III), implementation rests with the OMB director and the agency head (see 44 U.S.C. §3562 and §3576).

[138] OMB, "Circular No. A-130;" and OMB, "Circular No. A-108."

[139] OMB, M-16-24, p. 4. These terms are also used in the context of the information life cycle. For more information about the information life cycle, see CRS Report R47058, *Access to Government Information: An Overview*, by Meghan M. Stuessy.

[140] See 5 U.S.C. §552a(s) and 31 U.S.C. §1113 note.

[141] OMB, M-16-24, p. 28.

[142] Executive Order 13719, "Establishment of the Federal Privacy Council," 81 *Federal Register* 7685, February 12, 2016, §4(d).

[143] Additional information on the Federal Privacy Council and its activities may be found at https://www.fpc.gov.

[144] Privacy Act of 1974, §2 (P.L. 93-579, December 31, 1974; 88 Stat. 1896).

property-based concept of individual control" and the beginnings of understanding privacy based on the content of the information itself rather than its paper or electronic format.[145]

In deciding the future of privacy policy for new formats and uses, the FIPPs may be useful as Congress considers the adequacy of the Privacy Act in safeguarding the privacy of individuals while facilitating effective and efficient operation of government agencies and programs. As summarized by DOJ:

> [T]he authors of the HEW Report argued that the concept of privacy needed to be reimagined to recognize the mutual interests that institutions and individuals shared in the fair and appropriate management of personal information. This meant that instead of a property-based concept of individual control, what was needed was a governance framework designed to ensure the trust of the stakeholders in the information.[146]

As technology advances, opportunities for use and misuse of systems of records may be present in ways not considered during the original design and implementation of the Privacy Act. Congress has passed legislation providing further direction on the sharing and storage of information maintained on individuals. Examples of legislation that interact with the Privacy Act include provisions associated with the Computer Matching and Privacy Protection Act (CMPPA),[147] FISMA,[148] and the CIPSEA 2018 amendments, which were included in Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (FEBPA).[149]

As Congress reviews the Privacy Act, it might consider evaluating the effectiveness of the law and its implementation based on multiple considerations and across many contexts. This report highlights the FIPPs of individual participation, minimization, and purpose specification and use limitation and examines the potential issues related to the Privacy Act for each of these principles.[150]

Individual Participation

As previously discussed, the Privacy Act permits individually identifiable information to be disclosed without an individual's written consent pursuant to 12 statutory exceptions. Although Congress has sought to modernize the process of soliciting an individual's written consent, questions remain regarding not only whether individuals are sufficiently informed about how their information is being used but if appropriate precautions are being taken to validate an individual's identity. The principle of individual participation may be one concept used to explore different models of consent in government and digital identity authentication issues.

---

[145] DOJ, *Overview of the Privacy Act of 1974*, p. 2, and 44 U.S.C. §3301(a). See also the Presidential and Federal Records Act Amendments of 2014 at P.L. 113-187, 128 Stat. 2003 (2014).

[146] DOJ, *Overview of the Privacy Act of 1974*, p. 2.

[147] P.L. 100-503, 102 Stat. 2507, and subsequent amendments to its provisions. This law inserted many new requirements in provisions associated with the Privacy Act. See also CRS In Focus IF12053, *Federal Data Integration and Individual Rights: The Computer Matching and Privacy Protection Act*, by Natalie R. Ortiz.

[148] 44 U.S.C. §§3551-3559, P.L. 107-347, 116 Stat. 2946.

[149] P.L. 115-435, 132 Stat. 5529. CIPSEA is located at Title 44, Sections 3561-3583, of the *U.S. Code* and was originally enacted in P.L. 107-347, 116 Stat. 2962. FEBPA's Title III enacted the CIPSEA 2018 amendments in P.L. 115-435, 132 Stat. 5544. Please note that although OMB refers to FEBPA as the "Evidence Act" (see OMB, "Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance," M-19-23, July 10, 2019, https://www.whitehouse.gov/wp-content/uploads/2019/07/M-19-23.pdf), Congress did not indicate the use of such a short title in enacting the law.

[150] Clint Brass, Specialist in Government Organization and Management, contributed to this section of the report. See also Federal Privacy Council, "Fair Information Practice Principles (FIPPs)."

Examining Written Consent[151]

Recalling the *routine use* exception, which was included to allow individually identifiable information disclosures considered to be compatible with the original information collection, DOJ cautions that the exception, "because of its potential breadth, is one of the most controversial provisions in the Act."[152]

While the routine use exception may allow agencies to more efficiently share information on individuals, potentially facilitating streamlined interactions with the government, individuals who consent to the use of their information may be unaware of how agencies could repurpose the information. Congress may consider whether the level of information individuals receive when providing written consent through the Privacy Act or through agency publication of SORNs is commensurate with the sensitivity of the information. Congress may also consider whether agencies adequately consider and justify compatible uses of existing information.

In other contexts, processes exist to educate individuals on the collection and use of their information. For example, the CMPPA, which complies with the Privacy Act's disclosure provisions, requires a federal agency to have procedures for notifying individuals that information they provide to it may be compared to other information maintained by other agencies through matching programs.[153]

This notice can be *direct*, such as some form of contact between the government and the subject at the time an individual applies for a federal benefit or in a notice that arrives with the benefit, or *constructive*, where the notice, routine use disclosure, or matching program is published in the *Federal Register*.[154] Congress may consider if there are certain information uses that should rely on direct (rather than constructive) notice for purposes of providing consent under the Privacy Act.

Ascertaining Identity[155]

Agencies have interpreted the Privacy Act's written consent requirement to mean a signed document that may be either notarized or submitted to the agency under penalty of perjury.[156] However, these previously accepted methods of identity validation have been reexamined as Congress and the executive branch explore providing government services and access to individuals through electronic means. In recent years, Congress and the executive branch have worked to digitize and streamline processes where members of the public interact with the federal

[151] Natalie R. Ortiz, Analyst in Government Organization and Management, contributed to this section of the report.

[152] 5 U.S.C. §552a(a)(7); and DOJ, *Overview of the Privacy Act of 1974*, p. 95.

[153] P.L. 100-503, 102 Stat. 2507, and subsequent amendments to its provisions. 5 U.S.C. §552a(o)(1)(D). *Matching program* is defined as *any* computerized comparison of two or more automated systems of records or a system of records with nonfederal records for one of the purposes specified by the CMPPA (5 U.S.C. §552a(a)(8)). For more information on the CMPPA, see CRS In Focus IF12053, *Federal Data Integration and Individual Rights: The Computer Matching and Privacy Protection Act*, by Natalie R. Ortiz. Another example where individuals are educated on the collection and use of their information may be found in HIPAA's "Common Rule." For more information on the Common Rule, see CRS In Focus IF11043, *Updated Common Rule: Key Changes for Research Using Stored Biospecimens*, by Amanda K. Sarata.

[154] *Federal benefit program* for the purposes of the CMPPA is defined as "any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals" (5 U.S.C. §552a(a)(12)).

[155] Dominick A. Fiorentino, Analyst in Government Organization and Management, and Natalie R. Ortiz, Analyst in Government Organization and Management, contributed to this section of the report.

[156] OMB, M-21-04; and NARA, "Guide to Making a Privacy Act Request: What Is a Privacy Act Certification of Identity?," https://www.archives.gov/privacy/guide.html.

government. For example, in 2015, Congress required GSA to develop and implement a "single sign-on trusted identity platform" for individuals accessing public agency websites, which has become known as Login.gov.[157]

In an August 22, 2017, announcement, GSA described Login.gov as "a single sign-on solution for government websites that will enable citizens to access public services across agencies with the same username and password."[158] Further, Login.gov aims to allow users to "securely sign in to participating government websites and securely verify their identity" in accordance with NIST guidelines for providing different levels of identity and authenticator assurance.[159]

Login.gov came under scrutiny in a March 2023 GSA inspector general report and as the subject of a March 2023 House Committee on Oversight and Accountability subcommittee hearing.[160] The report found that Login.gov improperly advertised the level of confidence its digital processes could provide in validating an individual's identity. With regard to the Privacy Act, Congress may continue to consider the role and ability of the federal government to provide identity authentication in digital formats, the adequacy of processes to ascertain identity in the context of written consent, and opportunities to improve agency implementation.

Minimization

Given existing and emerging computer technologies at the time of its consideration, the Privacy Act included numerous safeguards to avoid privacy-related harms to the public and considered the need to update privacy protections for digital information. Especially in a digital context, the principle of minimization—that is, reducing the collection and use of individually identifying information and maintaining it only for as long as is necessary to accomplish a legally authorized purpose—takes on new meaning. The ability of digitized information to be available outside of physical filing cabinets or libraries may make the information more convenient, but such formats also reduce the ability to control the use of the information after its release. In particular, the phenomenon of the *mosaic effect* and the ability to recombine seemingly de-identified data into PII shows how the principle of minimization may relate to the Privacy Act and its implementation.

Mosaic Effect[161]

Data access and sharing may still involve significant risks even with seemingly de-identified data. OMB has warned of the *mosaic effect*, a problem that could occur as multiple versions of public and private information on individuals become accessible on the internet or through other channels. In a 2013 memorandum to agencies, OMB explained:

[157] 6 U.S.C. §1523(b)(1)(D).

[158] Joel Minton and Tom Mills, "Government Launches Login.Gov to Simplify Access to Public Services," GSA, August 22, 2017, https://18f.gsa.gov/2017/08/22/government-launches-login-gov/.

[159] GSA, "Login.gov: About Us," https://www.login.gov/about-us.

[160] See CRS In Focus IF12395, *Login.gov: Administration and Identity Authentication*, by Dominick A. Fiorentino, Natalie R. Ortiz, and Meghan M. Stuessy. See also GSA, Office of Inspector General, *GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards*, March 7, 2023, https://www.gsaig.gov/content/gsa-misled-customers-logingovs-compliance-digital-identity-standards; and U.S. Congress, House Committee on Oversight and Accountability, Subcommittee on Government Operations and the Federal Workforce, *Login.gov Doesn't Meet the Standard*, 118th Cong., 1st sess., March 29, 2023, https://oversight.house.gov/hearing/login-gov-doesnt-meet-the-standard/.

[161] Taylor R. Knoedl, Analyst in American National Government, contributed to this section of the report.

> The mosaic effect occurs when the information in an individual dataset, in isolation, may not pose a risk of identifying an individual (or threatening some other important interest such as security), but when combined with other available information, could pose such risk. Before disclosing potential PII or other potentially sensitive information, agencies must consider other publicly available data—in any medium and from any source—to determine whether some combination of existing data and the data intended to be publicly released could allow for the identification of an individual or pose another security concern.[162]

The ubiquity of digital information has created increased privacy risks, and there appears to be no consensus on whether the shared or combined information can be destroyed in the same manner as paper records. Digital formats raise new questions regarding how information could or should be released and how agencies prospectively determine privacy risks after its disclosure.

OMB advises that agencies should perform privacy analysis at each stage of the information's life cycle.[163] In this analysis, the agency must review the information that is collected or created for valid release restrictions and determine if the information can be made publicly available without jeopardizing privacy.[164] However, OMB warns agencies to consider the mosaic effect and conduct risk-based analyses in making their determinations, but OMB defers to NIST security standards for further implementation guidance.[165]

What Is Considered to Be "Identifiable Form"?

The Privacy Act and associated OMB guidance state how agencies should control and restrict the use, sharing, or dissemination of information on individuals in identifiable form. However, the Privacy Act itself does not define what is to be considered identifiable form. The statistical and computing technologies available at the time the Privacy Act was considered have markedly changed in the decades since its enactment. Where information was previously dispensed in analog and paper formats, the ability to share and re-share information in digital and electronic formats may complicate current understandings of privacy.

OMB considers PII to consist of information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual.[166] Relatedly, the E-Government Act of 2002 specifies that *identifiable form* means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.[167] However, each of these definitions hinges on a common understanding of when linking information can reveal an individual or what manipulations to information could reveal an individual from seemingly de-identified data.

---

[162] OMB, "Open Data Policy-Managing Information as an Asset," M-13-13, May 9, 2013, pp. 4-5, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2013/m-13-13.pdf. See also OMB, "Guidance for Agency Use of Third-Party Websites and Applications," M-10-23, June 25, 2010, p. 8, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-23.pdf.

[163] For more information about the information life cycle, see CRS Report R47058, *Access to Government Information: An Overview*, by Meghan M. Stuessy.

[164] OMB, M-13-13, pp. 9-10.

[165] When considering security-related restrictions to release, OMB advises agencies to focus on information confidentiality, integrity, and availability as factors to their risk management frameworks. These factors are further explored in NIST, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.

[166] OMB, "Circular No. A-130," p. 33.

[167] Section 208 of the E-Government Act of 2002 is located at 44 U.S.C. §3501 note; P.L. 107-347, 116 Stat. 2921.

In addition to appropriate agency governance, developments in computer science and statistics have created new methods of protecting PII while facilitating ethical use of the information.[168] These methods—which may involve manipulating the information, creating secure ways of matching information, or creating artificially manufactured data, among others—are known as privacy-enhancing technologies (PETs). Similarly, researchers are working to create utility metrics to measure how the release of limited or obscured information impacts the accuracy or validity of analysis that uses such information.[169] Application of these new technologies may enable agencies to achieve greater understanding of programmatic impacts and efficiencies while still hewing to the principle of information minimization.

In March 2023, components of the Office of Science and Technology Policy released a "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics" describing strategic priorities and recommending actions for agencies to adopt PETs. They define PETs as "a broad set of technologies that protect privacy by removing personal information, by minimizing or reducing personal data, or by preventing undesirable processing of data, while maintaining the functionality of a system."[170] However, agency adoption of PETs may be influenced by factors such as cost and scalability, information loss after manipulation, or tradeoffs between accuracy and utility of the information.[171]

Purpose Specification and Use Limitation

While government information can be inherently valuable for researchers, members of the public, and other agencies or governments, uncontrolled access to information may also put individual privacy at risk. Under the principle of purpose specification and use limitation, agencies are to balance the utility of the information against threats to privacy by providing notice of the specific purpose and use of individually identifying information.

The Privacy Act's multi-stakeholder approach to governance of information, in DOJ's view, seeks to balance the "need for other legitimate secondary users, such as public health authorities, financial oversight agencies, law enforcement and national security agencies—indeed any stakeholder with a legitimate need to use the information in the public interest—to access and appropriately use the information."[172] Congress may wish to revisit this principle with respect to

[168] NIST has described how components of agency governance can blend together as components of a privacy engineering plan for federal systems. NIST describes that existing privacy laws, as guided by the FIPPs, can inform risk assessments and risk management frameworks. This agency understanding of risk, then, can be documented and managed by the agency through PIAs and privacy engineering and security objectives. For more information, see Sean Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NIST, January 2017, https://nvlpubs.nist.gov/nistpubs/ir/2017/nist.ir.8062.pdf. See also Simson Garfinkel et al., *De-Identifying Government Datasets: Techniques and Governance*, NIST, September 2023, https://csrc.nist.gov/pubs/sp/800/188/final.

[169] Claire McKay Bowen, "Utility Metrics for Differential Privacy: No One-Size-Fits-All," NIST, October 29, 2021, https://www.nist.gov/blogs/cybersecurity-insights/utility-metrics-differential-privacy-no-one-size-fits-all.

[170] National Science and Technology Council, Fast-Track Action Committee on Advancing Privacy-Preserving Data Sharing and Analytics, *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics*, March 2023, p. 4, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf. The document further specifies that key technical approaches include k-anonymity, secure multiparty computation, homomorphic encryption, differential privacy, zero knowledge proofs, synthetic data, federated learning, and trusted execution environments. A chart explaining these approaches is located on page 15 of the document.

[171] Fast-Track Action Committee on Advancing Privacy-Preserving Data Sharing and Analytics, *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics*, p. 15.

[172] DOJ, *Overview of the Privacy Act of 1974*, p. 3.

efforts to limit agency information collections and the ability of government entities to store individually identifying information.

Information Collections and the Paperwork Reduction Act[173]

Congress enacted the PRA primarily to address a concern that the federal government was requiring businesses, individuals, and other entities to spend too much time filling out paperwork at the behest of federal agencies.[174] The PRA requires agencies to justify a proposed public information collection by evaluating the need and the burden of the information collection, among other criteria.[175] The act also empowers the OMB director to review and approve information collections.[176]

With regard to the principle of purpose specification and use limitation, in addition to agency justification of the information collection, the agency must ensure that each information collection is inventoried and informs the respondent of the reasons the information is being collected, how it is to be used, and whether responses to the information collection are voluntary or mandatory.[177]

The PRA also requires the OMB director, in consultation with other federal officials, to develop and maintain a plan to reduce information burdens on the public, including "through the elimination of duplication and meeting shared data needs with shared resources."[178] Relatedly, a Senate committee report on the PRA stated that "sharing information among government agencies also serves the goal of minimizing the burden imposed on the public by government collection of information" while reiterating that such disclosures need to be consistent with other laws, such as the Privacy Act.[179]

Because the PRA empowers the OMB director to approve of information collections and seek ways to eliminate information collection duplication, Congress may consider the role of OMB in understanding and adjudicating information collection requests and also whether agencies and OMB are able to adequately inform the public of new uses of the information they provide. Congress may also seek to examine whether agencies are striking an appropriate balance between

[173] Natalie R. Ortiz, Analyst in Government Organization and Management, contributed to this section of the report.

[174] 44 U.S.C. §§3501-3521. The PRA was originally enacted in 1980 (see P.L. 96-511; 94 Stat. 2812) and reauthorized in 1995 (see P.L. 104-13; 109 Stat. 163). For more context on the PRA, see CRS In Focus IF11837, *The Paperwork Reduction Act and Federal Collections of Information: A Brief Overview*, by Maeve P. Carey.

[175] 44 U.S.C. §3506(c)(1)(A). In practice, the terms *information collection* and *collection of information* with regard to the PRA are used interchangeably. The PRA defines *collection of information* in part to mean obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public of facts or opinions by or for an agency, regardless of form or format, calling for either (1) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, 10 or more persons other than agencies, instrumentalities, or employees of the United States; or (2) answers to questions posed to agencies, instrumentalities, or employees of the United States that are to be used for general statistical purposes. The full definition of *collection of information* is located at Title 44, Section 3502(3), of the *U.S. Code*. For the purposes of the PRA, *burden* is defined as "the time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency, including the resources expended for (A) reviewing instructions; (B) acquiring, installing, and utilizing technology and systems; (C) adjusting the existing ways to comply with any previously applicable instructions and requirements; (D) searching data sources; (E) completing and reviewing the collection of information; and (F) transmitting, or otherwise disclosing the information." The definition of *burden* under the PRA is located at Title 44, Section 3502(2), of the *U.S. Code*.

[176] 44 U.S.C. §3504(a)(1)(B)(i); 5 C.F.R. §1320.8(b)(3); 44 U.S.C. §3507(a)(2).

[177] 44 U.S.C. §3506(c)(1)(B).

[178] 44 U.S.C. §3503(a)(3)(B)(i).

[179] U.S. Congress, Senate Committee on Governmental Affairs, *Paperwork Reduction Act of 1995*, report to accompany S. 244, 104th Cong., 1st sess., S.Rept. 104-8, p. 29, https://www.congress.gov/104/crpt/srpt8/CRPT-104srpt8.pdf.

their need to collect information versus agency use of existing data resources to accomplish similar goals.

Exploring the Concept of a Data Clearinghouse[180]

Since the advent of the computing era, policymakers have intermittently considered the creation of a centralized clearinghouse to combine government data.[181] Proponents suggest that such a clearinghouse or "data warehouse" could provide access to agencies and researchers to foster learning, improve programs, and reduce the cost of studies. Critics, on the other hand, suggest that such access could come at the cost of individual privacy or allow the government or malicious actors to target individuals or groups. Such concerns prevented the creation of a national data center in 1965 and informed passage of the Privacy Act.[182] In considering the Privacy Act, the Senate Committee on Government Operations wrote:

> We believe that the creation of formal or de facto national data banks, or of centralized Federal information systems without certain statutory guarantees would tend to defeat these purposes, and threaten the observance of the values of privacy and confidentiality in the administrative process.[183]

Congress and the executive branch continued to consider ways to gain the value of such information for research and program evaluation purposes without sacrificing privacy. However, an absence of specific statutory authorization or concerns about public acceptance often led agencies to take restrictive and variable approaches to data sharing for statistical purposes.[184] Subsequently, some efforts to promote data sharing for exclusively statistical purposes were undertaken on a case-by-case basis.[185]

In 2016, Congress established the Commission on Evidence-Based Policymaking (CEP) to consider, among other things, whether "a data clearinghouse should be established to ensure federal data is available to policymakers, and also study how best to protect the privacy rights of individuals who interact with federal agencies."[186] CEP interpreted *clearinghouse* to mean "a data storage facility that permanently stores records from multiple databases from multiple agencies and, therefore, grows with each new data linkage."[187] CEP rejected the clearinghouse model,

---

[180] Clint Brass, Specialist in Government Organization and Management, contributed to this section of the report. For additional discussion, see CRS Insight IN11717, *Proposals for a National Secure Data Service, in Context*, by Meghan M. Stuessy and Clinton T. Brass.

[181] Rebecca S. Kraus, *Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants*, U.S. Census Bureau, August 1, 2011, https://www.census.gov/history/pdf/kraus-natdatacenter.pdf.

[182] Kraus, *Statistical Déjà Vu*, p. 39.

[183] U.S. Congress, Senate Committee on Government Operations, *Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information*, report to accompany S. 3418, 93rd Cong., 2nd sess., September 26, 1974, S.Rept. 93-1183 (Washington: GPO, 1974), p. 15.

[184] OMB, *Barriers to Using Administrative Data for Evidence-Building*, July 15, 2016, p. 5, https://obamawhitehouse.archives.gov/sites/default/files/omb/mgmt-gpra/barriers_to_using_administrative_data_for_evidence_building.pdf.

[185] Commission on Evidence-Based Policymaking, *The Promise of Evidence-Based Policymaking*, September 2017, p. 34, https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/Full-Report-The-Promise-of-Evidence-Based-Policymaking-Report-of-the-Comission-on-Evidence-based-Policymaking.pdf.

[186] P.L. 114-140, 130 Stat. 317; and U.S. Congress, House Committee on Oversight and Government Reform, *Evidence-Based Policymaking Commission Act of 2015*, report to accompany H.R. 1831, 114th Cong., 1st sess., July 16, 2015, H.Rept. 114-211, p. 4.

[187] CEP, *The Promise of Evidence-Based Policymaking*, p. 48.

however, citing "well-founded concerns about the potential privacy harm such a clearinghouse could raise."[188]

CEP's 2017 report suggested that advances in technology could support creation of a National Secure Data Service (NSDS), which could combine data without risking individual privacy or warehousing data through the application of de-identification methods and assigning expiration dates to data used by the NSDS.[189] In 2022, to further explore the creation of such a service, Congress instructed the director of the National Science Foundation, in consultation with the director of OMB, to create an NSDS demonstration project and authorized funds for the project for FY2023-FY2027.[190] Congress may wish to consider the nature of information management for privacy as it conducts oversight of the demonstration project.

Both statute and associated OMB guidance are to direct the administration of the NSDS demonstration project.[191] According to statute, the demonstration project may be operated directly or via a contract managed by the National Center for Science and Engineering Statistics. The statute also requires the demonstration project to "align" with the principles, best practices, and priority actions recommended by an advisory committee to the extent feasible.[192] Consistent with the purpose specification and use limitation principle, only authorized analysts are permitted to perform statistical queries necessary to answer approved project questions.[193] In December 2022, OMB released Memorandum M-23-04 providing for the establishment of a standard application process through which federal agencies, intergovernmental organizations, and researchers may apply to access confidential data assets.[194]

In terms of privacy protections, the demonstration project is to operate within the restrictions of CIPSEA and the Privacy Act. However, neither CIPSEA nor the Privacy Act specify when or how shared information or information concerning individuals is to be destroyed or whether such linkages are to be temporary instead of permanent. The director of the National Science Foundation is to further ensure that raw data and other sensitive inputs are not accessible to recipients of statistical outputs from the demonstration project and that no individual entity's data or information is revealed to any other party in an identifiable form.[195] Recalling the principle of minimization, the statute suggests that the demonstration project may use "the appropriate application of privacy-enhancing technologies and appropriate measures to minimize or prevent reidentification risks."[196] As Congress continues to oversee privacy and the pilot project, multiple FIPPs may be implicated.

[188] CEP, *The Promise of Evidence-Based Policymaking*, p. 48.

[189] CEP, *The Promise of Evidence-Based Policymaking*, p. 89.

[190] P.L. 117-167, §10375, 136 Stat. 1574. See also 42 U.S.C. §19085. This provision of P.L. 117-167 is located in Title III—National Science Foundation for the Future.

[191] 42 U.S.C. §19085(a).

[192] 42 U.S.C. §19085(b).

[193] 42 U.S.C. §19085(f)(1)(D).

[194] OMB, "Establishment of Standard Application Process Requirements on Recognized Statistical Agencies and Units," M-23-04, December 8, 2022, p. 1, https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-04.pdf.

[195] 42 U.S.C. §19085(f)(1)(A) and (B).

[196] 42 U.S.C. §19085(f)(2).

Appendix. Additional Resources

Table A-1. Fair Information Practice Principles (FIPPs), as Described by the Federal Privacy Council

Principle	Description
Access and Amendment	Agencies should provide individuals with appropriate access to personally identifiable information (PII) and appropriate opportunity to correct or amend PII.
Accountability	Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.
Authority	Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.
Minimization	Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.
Quality and Integrity	Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
Individual Participation	Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.
Purpose Specification and Use Limitation	Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
Security	Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
Transparency	Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

Source: Federal Privacy Council, "Fair Information Practice Principles (FIPPs)," https://www.fpc.gov/resources/fipps/.

Table A-2. 10 Exemptions from the Privacy Act

5 U.S.C. §552a Exemptions for Certain Records and Systems of Records

Citation	Description
(d)(5)	Information compiled in reasonable anticipation of a civil action proceeding;
(j)(1)	Information maintained by the Central Intelligence Agency;
(j)(2)	Material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or to apprehend criminals;
(k)(1)	Information that is currently and properly classified pursuant to an executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
(k)(2)	Investigatory material compiled for law enforcement purposes, other than criminal, that did not result in loss of a right, benefit or privilege under federal programs, or that would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
(k)(3)	Material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, *U.S. Code*, Section 3056;
(k)(4)	Material required by statute to be maintained and used solely as statistical records;
(k)(5)	Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
(k)(6)	Testing or examination material used to determine individual qualifications for appointment or promotion in federal government service, the release of which would compromise the testing or examination process;
(k)(7)	Material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

Source: CRS review of 5 U.S.C. §552a. See also U.S. Drug Enforcement Administration, "Exemptions," https://www.dea.gov/foia/privacy-act-exemptions; and U.S. Treasury, Financial Crimes Enforcement Network, "Privacy Act Exemptions," https://www.fincen.gov/privacy-act-exemptions.

Table A-3. 12 Exceptions to the Privacy Act

5 U.S.C. §552a Exceptions to the Written Consent Requirement

Citation	Description
(b)(1)	To those officers and employees of the agency which maintains the record, who have a need for the record in the performance of their duties;
(b)(2)	When disclosure is made under the Freedom of Information Act (FOIA);
(b)(3)	For an established routine use identified in the system of records notice (SORN) that has been published in the *Federal Register*;
(b)(4)	To the Census Bureau for purpose of planning or carrying out a census or survey;
(b)(5)	To a recipient who has provided the agency with adequate written assurance that the record will be used solely for statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
(b)(6)	To the National Archives and Records Administration (NARA) for historical preservation if the Archivist determines the record has historical value;
(b)(7)	To another agency or to an instrumentality of any governmental jurisdiction, within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
(b)(8)	To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
(b)(9)	To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any join committee of Congress or subcommittee of any such joint committee;
(b)(10)	To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accountability Office;
(b)(11)	Pursuant to the order of a court of competent jurisdiction;
(b)(12)	To a consumer reporting agency in accordance with Title 31, *U.S. Code,* Section 3711(e), related to debt collection.

Source: CRS review of 5 U.S.C. §552a. See also Department of Housing and Urban Development, "Privacy Act Exceptions: Information Disclosure Guidance," https://www.hud.gov/sites/dfiles/OCHCO/documents/PrivacyActExceptions.pdf.

Author Information

Meghan M. Stuessy
Analyst in Government Organization and Management

Disclaimer