

# **PRIVACY ACT**

## **Administrative Conference of the United States**

### **ABA Section on Administrative Law and Regulatory Practice**

**Online at:**

**[https://sourcebook.acus.gov/wiki/Privacy\\_Act/view](https://sourcebook.acus.gov/wiki/Privacy_Act/view)**  
**(emphasis added)**

#### **Overview**

The Privacy Act of 1974 represents the Congressional response to concerns about government uses of information collected about private individuals. The Privacy Act gives individuals greater control over the gathering, dissemination, and accuracy of information collected about themselves by agencies. *Miller v. United States*, 630 F. Supp. 347 (E.D.N.Y. 1986). The main purpose of the Privacy Act is to forbid disclosure unless it is required by the [Freedom of Information Act](#) (FOIA). *Lovell v. Alderete*, 630 F.2d 428 (5th Cir. 1980). **To protect individual privacy, the Privacy Act constrains executive branch recordkeeping, defines the individual's right to access certain records, limits agency disclosure of records containing an individual's private information, establishes safeguards to protect records concerning individuals, and provides remedies for agency violation of the Privacy Act's provisions.**

#### **Scope**

The Privacy Act covers records maintained by agencies as defined in FOIA. It applies to Cabinet-level departments, independent regulatory agencies, military departments, and government corporations. [§ 552a\(a\)\(1\)](#). It does not apply to the legislative branch, national banks (*United States v. Miller*, 643 F.2d 713 (10th Cir. 1981)), or Amtrak (*Ehm v. National R.R. Passenger Corp.*, 732 F.2d 1250 (5th Cir. 1984), *cert. denied*, 469 U.S. 982 (1984)). See *Alexander v. FBI*, 971 F. Supp. 603, 606-07 (D.D.C. 1997) (recognizing that the definition of "agency" under Privacy Act is same as in FOIA and that courts have interpreted that definition under FOIA to exclude the President's immediate personal staff and units within Executive Office of the President whose sole function is to advise and assist the President, but, nevertheless rejecting such limitation with regard to "agency" as used in the Privacy Act due to the different purposes that the two statutes serve); *Shannon v. Gen. Elec. Co.*, 812 F. Supp. 308, 313, 315 n.5 (N.D.N.Y. 1993) (stating there

is “no dispute” that General Electric (GE) falls within the definition of “agency” subject to requirements of the Privacy Act where, pursuant to a contract, it operated a Department of Energy-owned lab under the supervision, control, and oversight of the Department and where, by terms of the contract, GE agreed to comply with the Privacy Act).

A record is a collection or grouping of information about an individual that, for example, may include educational, financial, or biographical information, together with personal identifiers such as names, photos, numbers, or fingerprints. 5 U.S.C. § 552a(a)(4). The Privacy Act does not apply to all government records and documents that may contain an individual’s name or other private information. For example, it does not include the private notes of a supervisor if such notes are not used by the agency to make decisions. *Johnston v. Horne*, 875 F.2d 1415 (9th Cir. 1989). But such notes may become subject to the Privacy Act if they become part of an agency’s decision. *Chapman v. NASA*, 682 F.2d 526 (5th Cir. 1982), *cert. denied*, 469 U.S. 1038 (1984). The Act also does not apply to information in documents obtained from independent sources of information, even though identical information may be in an agency’s system of records. *Thomas v. U.S. Dep’t of Energy*, 719 F.2d 342 (10th Cir. 1983).

**The Privacy Act focuses on “systems of records” established, maintained, or controlled by an agency. A “system of records” is a group of any records where individual names or other individual identifiers can be used to retrieve the information. 5 U.S.C. § 552a(a)(5). Agencies may maintain records covered by the Privacy Act only when they are relevant and necessary to accomplish the agency’s purpose. 5 U.S.C. § 552a(e)(1).**

The Court of Appeals for the District of Columbia Circuit addressed the “system of records” definition in the context of computerized information in *Henke v. U.S. Dep’t of Commerce*, 83 F.3d 1453 (D.C. Cir. 1996), and noted that “the [Office of Management and Budget] guidelines make it clear that it is not sufficient that an agency has the capability to retrieve information indexed under a person’s name, but the agency must in fact retrieve records in this way in order for a system of records to exist.” *Id.* at 1460 n.12. The D.C. Circuit looked to Congress’ use of the words “is retrieved” in the statute’s definition of a system of records and focused on whether the agency “in practice” retrieved information. *Id.* at 1459-61.

## **Access to Records**

**Where the agency is authorized to keep records covered by the Privacy Act, an individual has a right of access to records concerning him or her. This is a central protection of the Privacy Act for individuals. The individual has a right to:**

- **Copy any or all of the record (§ 552a(d)(1));**
- **Request amendment of the record (§ 552a(d)(2)) and file a concise statement of disagreement if the agency refuses to amend the record that will be provided to all persons to whom the record is disclosed (§ 552a(d)(4)); and**
- **Request an accounting from the agency on the date, nature, and purpose of each disclosure of the record (§ 552a(c)).**
- **The individual has an absolute right to access and need not provide any reason for seeking access. *FTC v. Shaffner*, 626 F.2d 32 (7th Cir. 1980).**

## Agency Requirements

For each system of records an agency maintains, it must:

- **Publish in the *Federal Register* the name and location of the system; the categories of individuals contained in the system; the routine use of the records; agency policies concerning the records including storage, retrieval, access, retention, and disposal; the person, including title and address, responsible for the system; the method used to notify individuals how to gain access to records about themselves; and the sources or records in the system.** Any new use of the system must be noticed for comment 30 days prior to implementing the new use. Exempt systems must also be noticed. *See, e.g.*, 5 U.S.C. § [552a\(b\)\(3\)](#), (e)(4), and (e)(11);
- **Maintain records in the system accurately, completely, and timely to ensure fairness to the individuals** (§ 552a(e)(5));
- **Establish rules and training for persons designing, developing, operating, or maintaining the system to ensure compliance with the Privacy Act and the agency's implementing policies** (§ 552a(e)(9));
- **Establish safeguards for the protection of records** (§ 552a(e)(10)); and
- **Inform government contractors of their duties under the Privacy Act** (§ 552a(m)).

When the agency collects information that “may result in adverse determinations about an individual’s rights, benefits, and privileges under Federal programs,” the Privacy Act requires the information to be collected, to the “greatest extent practicable,” directly from the affected individual. 5 U.S.C. § 552a(e)(2). When requesting such information from individuals, the agency must disclose: (1) the authority under which collection is authorized; (2) the principal purposes for which the information is needed; (3) the routine use of the information; and (4) consequences, if any, of not providing the information. 5 U.S.C. § 552a(e)(3).

**The Privacy Act mandates that information maintained in agency records be as relevant and as necessary as possible to accomplish the agency’s purpose. It must also undertake to maintain the information with such accuracy and completeness as is reasonably necessary to assure fairness to the individual.** In *Doe v. United States*, 821 F.2d 694 (D.C. Cir. 1987), the court sitting en banc held that an agency may satisfy this requirement by supplementing the information an individual considers damaging with the individual’s explanation or disagreement with the accuracy of the information. The court found that the agency made a reasonable effort to determine the accuracy of the information and that an adjudication of the disputed facts was not necessary for the agency’s purposes. The court said that in some cases, fairness may require a record to contain both versions of a disputed fact.

**Agencies are prohibited from maintaining records describing how an individual exercises First Amendment rights, unless such records are authorized by statute or are pertinent to and within the scope of authorized law enforcement activity.** 5 U.S.C. § 552a(e)(7). **Such records are subject to the Privacy Act even if not kept in “a system of records.”** *Clarkson v. IRS*, 678 F.2d 1368, 1373-77 (11th Cir. 1982), *cert. denied*, 481 U.S. 1031. *Cf. Pototsky v. U.S. Dep’t of Navy*, 717 F. Supp. 20 (D. Mass. 1989). Guidelines from the Office of Management and Budget (OMB) call for the broadest reasonable interpretation of the prohibition.

## **Exemptions from Access**

The Privacy Act provides general (§ 552a(j)) and specific (§ 552a(k)) exemptions. These are exemptions allowing an agency to deny access to the record by the individual to whom the record pertains. The two types of exemptions are different in nature and consequences and are discretionary on the agency's part. To be effective, the agency must first determine that a record or system of records meets the criteria for exemption under the Privacy Act and then publish the exemption as a rule under the [Administrative Procedure Act's](#) (APA) notice-and-comment provisions. Failure to set out reasons demonstrating that the exemption meets the requirements of the Privacy Act may leave the records subject to the Privacy Act. *Exner v. FBI*, 612 F.2d 1202 (9th Cir. 1980). The exemptions do not authorize the agency to use the record in a manner other than the manner originally set out in the *Federal Register* establishing the system of records. *Doe v. Naval Air Station*, 768 F.2d 1229 (11th Cir. 1985).

A general exemption denies access by an affected individual under virtually all the Privacy Act's provisions and is available for records maintained by the Central Intelligence Agency or by an agency whose principal functions are criminal law enforcement. The general exemption may not be used to exempt records compiled for a noncriminal or administrative purpose even if they are also a part of a system of records maintained by an agency qualified to assert the exemption. *Vymetalik v. FBI*, 785 F.2d 1090, 1095 (D.C. Cir. 1986).

The specific exemptions (§ 552a(k)(1)(7)) are available to any agency if the head of the agency promulgates rules pursuant to the notice-and-comment provisions of the [APA](#), 5 U.S.C. § 553. The specific exemption is from a particular provision of the Privacy Act. The seven exemptions allowed are:

- [FOIA \(b\)\(1\) exemptions](#) (matters to be kept secret in the interest of national defense or foreign policy and properly classified by executive order);
- Investigatory material compiled for law enforcement purposes that does not fall within the general exemption;
- Material maintained to provide protective service to the President or pursuant to 18 U.S.C. § 3056;
- Confidential investigatory records relating to employment or contracts;
- Statistical records required by statute;
- Testing and examination material related to federal employment; and
- Evaluations related to military promotions obtained confidentially.

**An individual may sue to challenge a denial of access to records based on the general or specific exemptions, and the court will determine the substantive and procedural propriety of the agency's assertion of the exemption.** *Zeller v. United States*, 467 F. Supp. 487 (E.D.N.Y. 1979).

## **Restrictions on Disclosure**

**The Privacy Act prohibits disclosure of any record covered by the Privacy Act without the written request or prior written consent of the person whom the record concerns. 5 U.S.C. § 552a(b). The restriction on disclosure applies to any person or agency and includes any means of communication—written, oral, electronic, or mechanical [Responsibilities for the Maintenance of Records About Individuals by Federal Agencies](#), 40 Fed. Reg. 28948, 28953 (July 9, 1975). Information obtained (or released) through sources independent of agency records is not “disclosure” under the Privacy Act.**

The general rule of nondisclosure is subject to 12 exceptions (§ 552a(b)(1)(12)). They are:

- Internal agency use on a need to know basis;
- Proper requests under FOIA;
- Routine use;
- Census Bureau activities;
- Statistical research where the recipient has given written assurance that records are not individually identifiable;
- National Archives preservation;
- Information to Congress;
- Information to the Comptroller General in performing Government Accountability Office (GAO) duties;
- Showing of compelling circumstances affecting the health or safety of an individual;
- Pursuant to court order (subpoenas issued by clerks of courts are not “orders” *Stiles v. Atlanta Gas Light Co.*, 453 F. Supp. 798, 800 (N.D. Ga. 1978));
- To a consumer reporting agency in accordance with 31 U.S.C. § 3711(f); and
- Use by “any governmental jurisdiction . . . for a civil or criminal law enforcement activity” as long as a written request (1) is made by the head of the agency seeking the record, (2) specifies the portion of the record sought, and (3) describes the relevant enforcement activity. *See Doe v. Naval Air Station*, 768 F.2d 1229 (11th Cir. 1985).

“Routine use,” considered generally the most important exception, is defined as “the use of such record for a purpose that is compatible with the purpose for which it was collected.” 5 U.S.C. § 552a(a)(7). Each routine use is identified in the *Federal Register* notice upon establishment or revision of each system of records. 5 U.S.C. (§ 552a(e)(4)(D)). This exception permits nonconsensual intra- or interagency transfer of what is generally described as “house-keeping” information. Because the language is broad, the potential for abuse is considered great, and the courts have strictly required that the use be clearly and specifically identified in the rule adopted by the agency identifying the system of records. *Covert v. Harrington*, 876 F.2d 751 (9th Cir. 1989); *Doe v. Stephens*, 851 F.2d 1457 (D.C. Cir. 1988); *Zeller v. United States*, 467 F. Supp. 487 (E.D.N.Y. 1979). The Supreme Court has found that the Privacy Act’s provisions restricting disclosure, even while allowing disclosure for “routine uses,” are sufficient to protect persons’ constitutional right to informational privacy, if such a right exists. *NASA v. Nelson*, 562 U.S. 134, 153-55 (2011).

## **Review, Relief, Remedies**

The Privacy Act provides that each agency shall promulgate rules that establish, among other things, procedures of notice, disclosure, and review of requests. 5 U.S.C. § 552a(f). **In the event that the rules are not followed or that a dispute persists, there are four civil actions:**

- (1) a challenge for failure to provide access;**
- (2) a challenge for refusal to amend;**
- (3) a damages action for improper maintenance of the content of records; and**
- (4) a damages action for other breaches of the Privacy Act or regulations issued thereunder that adversely affect the individual. 5 U.S.C. § 552a(g)(1).**

**The latter two actions require proof of damages and are limited to actual damages. A cause of action for monetary damages requires a showing of an agency's intentional or willful failure to maintain accurate records and that the violation of the Privacy Act caused the actual damages complained of.** *Molerio v. FBI*, 749 F.2d 815, 826 (D.C. Cir. 1984). Because waivers of sovereign immunity are to be strictly construed, the Supreme Court held that "actual damages" do not include nonpecuniary damages. <https://tile.loc.gov/storage-services/service/ll/usrep/usrep566/usrep566284/usrep566284.pdf> Fed. Aviation Admin. v. Cooper], 566 U.S. 284 (2012).

Remedies for failure to grant access or refusal to amend are injunctive.

An individual bringing a claim under § 552a(g)(1) must demonstrate a causal connection between the alleged violation and the harm suffered but may not use the Privacy Act claim as the forum in which to prove the entitlement the individual claims was improperly denied. *Gizoni v. Sw. Marine, Inc.*, 909 F.2d 385 (9th Cir. 1990).

Criminal penalties are established for willful disclosure of records by those who know such disclosure is prohibited, willful maintenance of a system of records without meeting the appropriate notice requirements, and knowing and willful requests for records under false pretenses. 5 U.S.C. § 552a(i).

Each violation is classified as a misdemeanor, and the violator may be fined not more than \$5,000. There have been at least two criminal prosecutions for unlawful disclosure of Privacy Act-protected records. *See United States v. Trabert*, 978 F. Supp. 1368 (D. Colo. 1997) (finding the defendant not guilty; that the prosecution did not prove "beyond a reasonable doubt that defendant 'willfully disclosed' protected material"; and that the evidence presented constituted, "at best, gross negligence," and thus was "insufficient for purposes of prosecution under § 552a(i)(1)"); *United States v. Gonzalez*, No. 76-132 (M.D. La. Dec. 21, 1976) (guilty plea entered). *See generally In re Mullins (Tamposi Fee Application)*, 84 F.3d 1439, 1441 (D.C. Cir. 1996) (*per curiam*) (indicating the application for reimbursement of attorney fees where



independent counsel found no prosecution was warranted under the Privacy Act because there was no conclusive evidence of improper disclosure of information). In a case involving the destruction of records, [Gerlich v. DOJ](#), 711 F.3d 161 (D.C. Cir. 2013), the D.C. Circuit allowed a Privacy Act claim to proceed against senior officials at the Department of Justice on the ground that they created records about appellants in the form of annotations to their applications and internet printouts concerning their political affiliations. The court relied in part on a permissive spoliation inference in light of the destruction of appellants' records, because the senior department officials had a duty to preserve the annotated applications and internet printouts given that department investigation and future litigation were reasonably foreseeable.

**The Privacy Act provides a two-year statute of limitations. 5 U.S.C. § 552a(g)(5). The time begins to run when a reasonable person should have known of the alleged violation.** *Rose v. United States*, 905 F.2d 1257, 1259 (9th Cir. 1990); *Diliberti v. United States*, 817 F.2d 1259, 1262 (7th Cir. 1987).

## **Computer Matching**

The Privacy Act was amended in 1988 by the Computer Matching and Privacy Protection Act of 1988 ([Pub. L. No. 100-503](#)). OMB issued final guidance implementing the amendment's provisions on June 19, 1989. [Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988](#), 54 Fed. Reg. 25818 (June 19, 1989)). The amendments added § 552a(o)-(q) to establish procedural safeguards affecting agencies' use of Privacy Act records when performing computerized matching programs. The amendments require agencies to conclude written agreements specifying terms and safeguards under which matches are to be done. They provide procedures for individuals whose information is contained in the affected records to use to prevent agencies from taking adverse actions unless they have independently verified the results of matching and given the individual advance notice. Oversight is established by requiring *Federal Register* notice of matching agreements, reports to OMB and Congress, and the establishment of internal "data integrity boards" to oversee and coordinate the agency's implementation of matching programs.

## **Relationship to the FOIA**

Two provisions relate to FOIA. 5 U.S.C. [§ 552](#). Section 552a(b)(2) exempts agencies from the requirement of obtaining an individual's consent to release of information subject to disclosure under FOIA. In 1984, Congress added provisions delineating an individual's access rights to records exempt from disclosure under FOIA or the Privacy Act. An agency must give an individual access to a record if it is accessible under either act irrespective of whether it might be withheld under the other. 5 U.S.C. § 552a(t). This gives maximum access to records by an individual whose personal information is contained therein. An accounting of the number of FOIA releases of Privacy Act information is not required. 5 U.S.C. § 552a(c)(1). If released under FOIA, the agency is relieved from ensuring the accuracy, completeness, timeliness, and relevance of the record. 5 U.S.C. § 552a(e)(6). If the system of records is made necessary by FOIA, the agency may exempt the system from the Privacy Act. 5 U.S.C. § 552a(k)(1).

## **Social Security Numbers**

**The Privacy Act restricts use of an individual's Social Security account number.** [Pub. L. No. 93-579](#), § 7 (not codified as part of 5 U.S.C. § 552a). This provision applies to state and local governments, as well as to the federal government and makes it unlawful to deny any right, benefit, or privilege based on an individual's failure to disclose the Social Security account number, unless the disclosure was required by any federal, state, or local system of records in operation before January 1, 1975, or the disclosure is required by federal law. Since enactment, Congress has required disclosure in the Tax Reform Act of 1976 ([Pub. L. No. 94-455](#)), the Deficit Reduction Act of 1984 ([Pub. L. No. 98-369](#)), and the Debt Collection Act of 1982 ([Pub. L. No. 97-365](#)). In the Tax Reform Act of 1976, Congress declared it to be U.S. policy to use Social Security account numbers "in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law." Pub. L. No. 94-455, amending 42 U.S.C. § [405\(c\)\(2\)](#).

## **Oversight**

The Privacy Act requires OMB to develop guidelines and regulations for its implementation and to provide continuing assistance and oversight. The OMB guidelines are entitled to the usual deference accorded the interpretations of the agency charged with administration of a statute. *Albright v. United States*, 631 F.2d 915, 919 n.5 (D.C. Cir. 1980); *Quinn v. Stone*, 978 F.2d 126, 133 (3d Cir. 1992). However, a few courts have rejected particular aspects of the OMB guidelines as inconsistent with the statute. *See, e.g., Kassel v. U.S. Dep't of Veterans Affairs*, No. 87-217-S, slip op. at 24-25 (D.N.H. Mar. 30, 1992) (subsection (e)(3)); *Doe v. Chao*, 540 U.S. 614, 627 n.11 (2004) (disagreeing with dissent's reliance on OMB interpretation of damages provision since the Court does "not find its unelaborated conclusion persuasive").

The vast majority of OMB's Privacy Act guidelines are published in [Privacy Act Implementation Guidelines and Responsibilities](#), 40 Fed. Reg. 28948 (1975). However, these original guidelines have been supplemented in particular subject areas over the years, including:

- [Appendix I to OMB Circular No. A-130](#), most recently revised at [81 Fed. Reg. 49689](#) (July 28, 2016)).
- [Implementation of the Privacy Act Supplemental Guidance](#), 40 Fed. Reg. 56741 (Dec. 4, 1975) (system of records definition, routine use and intra-agency disclosures, consent and congressional inquiries, accounting of disclosures, amendment appeals, rights of parents and legal guardians, relationship to FOIA).
- [Guidelines on the Relationship of the Debt Collection of 1982 to the Privacy Act of 1974](#), 48 Fed. Reg. 15556 (Apr. 11, 1983) (relationship to Debt Collection Act).
- [Guidance on the Privacy Act Implications of "Call Detail" Programs to Manage Employees' Use of the Government's Telecommunications Systems](#), [52 Fed. Reg. 12,990-93](#) (Apr. 20, 1987) ("call detail" programs).
- [Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988](#), [54 Fed. Reg. 25,818](#) (June 19, 1989) (computer matching).
- [The Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act of 1974](#), [56 Fed. Reg. 18,599](#) (proposed Apr. 23, 1991) (computer matching);



- [Management of Federal Information Resources](#), 61 Fed. Reg. 6428 (1996) (“Federal Agency Responsibilities for Maintaining Records About Individuals”).

Thus, when researching in this area, it may be important to check subsequent supplements.

## **Source Note**

The legislative history of the original Act is exhaustively collected in [Legislative History of the Privacy Act of 1974, S. 3418 \(Pub. L. No. 93-579\): Source Book on Privacy](#) (1976).

The Department of Justice’s [Overview of the Privacy Act of 1974](#) is updated periodically and discusses the extensive case law under the Privacy Act.