apdu
ASSOCIATION of PUBLIC DATA USERS

Primer on the Privacy Act of 1974

By Bethanne Barnes and Maya A. Bernstein

When Congress passed the Privacy Act of 1974, it wanted the government to treat individuals fairly when collecting data about them. The law does this by:

1. **Making agencies responsible** for managing identifiable records fairly and protecting them from being used or shared without authorization.
2. **Granting rights to individuals,** like the right to know what records the government has about them, to see those records, request amendments, and take legal action.

The Privacy Act is more than just a law about who can see a file. Fairness in every aspect of managing records about individuals is woven into the law. The Act regulates covered information throughout its lifecycle. This means it controls the agency's collection, maintenance, use, disclosure, and eventual archiving or disposal of records.

This Primer provides a basic guide to the principles and protections in the Privacy Act. It is not legal advice and does not discuss every provision. It should give you an understanding of where the Privacy Act protections are strong and where they are weaker.

Why Did Congress Enact the Privacy Act?

The Privacy Act of 1974 ("the Act") emerged from a perfect storm of political scandal and new technology. By the early 1970s, the federal government gained a unique ability to keep massive, computerized databases. This sparked fears that the executive branch could build permanent, secret files on citizens without anyone watching.[1]

These fears grew after the 1972 Watergate break-in and revelations of J. Edgar Hoover's extensive private files on political figures.[2] At the same time, some politicians proposed aggressive new policies that would let the government pool personal data across agencies without any privacy rules. These events showed a dire need for a new law to control how the government keeps records.

The Act was ultimately fueled by a landmark 1973 advisory committee report to the Secretary of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens* (HEW Report).[3] This report set out a **Code of Fair**

1 See Rebecca S. Krauss, *Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants* (2011), U.S. Census Bureau. https://www2.census.gov/library/working-papers/2011/dir/kraus-01.pdf.

2 The New York Times reported that President Nixon was recorded as saying that he avoided firing J. Edgar Hoover, head of the FBI, for fear of reprisal. *Wines, Michael (June 5, 1991).* "Tape Shows Nixon Feared Hoover". The New York Times. See also Lukas, J. Anthony (January 1, 1976). *Nightmare: The Underside of the Nixon Years*. Viking Press. pp. 22–26 (reporting on Nixon abuses of the Internal Revenue Service).

3 Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare. 1973. *Records, Computers, and the Rights of Citizens*; Report. MIT Press. http://archive.org/details/recordscomputers00unit.

Information Practice for the first time. As the Watergate and impeachment hearings were playing on TV, Congress moved quickly to turn these principles into law. Following other, related legislation,[4] the Act was passed as a bipartisan compromise and signed into law by President Gerald Ford on December 31, 1974, ending the era of secret federal record systems.

The Heart of Privacy: the Code of Fair Information Practice

The **Code of Fair Information Practice** was the core recommendation of the HEW Report, arguably the most influential federal advisory committee report ever produced. The Code formed the basis of the Privacy Act and every other privacy law in the United States and around the world. It included five tenets that set the standard for protecting personal data, and has been used internationally to guide decisions about personal information. The Code has been reformulated many times and is sometimes called the "Fair Information Principles" or "Fair Information Practice Principles" (FIPPs).[5]

CODE OF FAIR INFORMATION PRACTICE

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for individuals to find out what information about them is in a record and how it is used.
- There must be a way for individuals to prevent information about them obtained for one purpose from being used or made available for other purposes without their consent.
- There must be a way for individuals to correct or amend a record of identifiable information about them.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Who Must Comply with the Privacy Act?

Federal executive branch agencies must comply with the Act, but what is an *agency*? The Act uses the same definition as the Freedom of Information Act (FOIA):

> [T]he term 'agency' means any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government (including the Executive Office of the President), or any independent regulatory agency.[6]

That is, an ***agency*** is a cabinet agency (such as the Department of Homeland Security, not Customs and Border Protection) or the highest level of any non-cabinet agency (such as the Equal Employment Opportunity Commission).

4 The Fair Credit Reporting Act (1970) Title VI of Pub. L. 91-508, 84 Stat. 1114, 1127, codified at 15 U.S.C. § 1681 *et seq,* regulated the credit industry, and the Family Educational Rights and Privacy Act Pub, L. 93-380, 88 Stat. 571 (1974) regulated education records.

5 For a nice discussion of the variety of formulations, refer to Robert Gellman, "Fair Information Practices: A Basic History, v 2.232" (July 28, 2025), *available at* https://bobgellman.com/rg-docs/rg-FIPshistory.pdf (visited Jan 3, 2026). See also Memorandum Dept. of Homeland Security (DHS, 2008) *Privacy Policy Guidance Memorandum 2008-01: the Fair Information Practice Principles* https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.

6 5 U.S.C. § 552a(a)(1).

This definition does not include, and the Privacy Act generally does not cover:

- Components of the Executive Office of the President whose only job is to advise and assist the President (for example, the National Security Council)
- Congress
- The judicial branch
- State, local, tribal, or territorial governments[7]

Who Has Privacy Act Rights? Who Does the Privacy Act Protect?

The Act protects natural, living *individuals*. An ***individual*** is defined as:

> a citizen of the United States or an alien lawfully admitted for permanent residence.

These are called ***U.S. persons***. The definition excludes:

- Deceased persons
- Non-US persons (i.e., visitors and others not admitted for permanent residence)[8]
- Organizations (including for-profit corporations and not-for-profit entities)

Systems of Records: What Records are Covered by the Privacy Act?

All Privacy Act rights and almost all agency responsibilities only apply if a *record* is in a *system of records*—a group of *records* that meets certain conditions described below.

So, what is a *record*? Under the Act, ***records*** are defined as:

> any item, collection, or grouping of information about an individual that is maintained by an agency … and that contains his name, or the identifying number, symbol or other identifying particular assigned to the individual.

In other words, a record is information about an individual connected to an identifier.[9]

7 States and local governments are subject to parts of the Act that limit when a federal, state, or local government may require individuals to submit social security numbers (SSNs) and list the elements of notice that are required upon collection. Pub. L. 93-579, § 7 (1974). They are also covered by amendments dealing with ***matching programs*** — computerized comparisons of records to make decisions about eligibility for federally funded benefit or loan programs, or certain computerized comparisons of federal employees. See 5 U.S.C. § 552a(a)(8), (o), (p), (q), (r), and (u).

8 In practice, many agencies administratively grant access and amendment rights to all individuals regardless of immigration status. Refer to APDU's Issue Brief, *Managing "Mixed Systems" of Records Under the Privacy Act of 1974*, available at https://apdu.org/apdu-in-action/data-privacy-resources.

9 Some records may refer to two or more individuals, for example, a married couple. The part that is a record with respect to any individual is only the part of the record *about* that individual. Compare *Voelker v. IRS*, 646 F.2d 332, 334 (8th Cir. 1981) (requiring agency to provide individual with access to entire record, even though some information in that record "pertained" to a third party), with *Sussman v. U.S. Marshals Service*, 494 F.3d at 1121 n.9 (interpreting subsection (d)(1) "to give parties access only to their own records, not to all information pertaining to them that happens to be contained in a system of records"; "[f]or an assemblage of data to qualify as one of [plaintiff's] records, it must not only contain his name or other identifying particulars but also be about him"). *See also Aguirre v. SEC*, 671 F. Supp. 2d 113, 121 (D.D.C. 2009), *Nolan v. DOJ*, No. 89-A-2035, 1991 WL 36547, at *3 (D. Colo. Mar. 18, 1991), *aff'd*, 973 F.2d 843 (10th Cir. 1992), and *DePlanche v. Califano*, 549 F. Supp. 685, 693-98 (W.D. Mich. 1982). For more detail, refer to Department of Justice *Overview of the Privacy Act, 2020 edition*: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition.

The identifier can be almost anything that could be used to pinpoint the record (such as name, Social Security Number, or address), but it does not have to be unique to an individual. In addition to names and account numbers, the Act specifically lists fingerprints, voice prints, and photographs as possible identifiers. For example, Rosa Lee, while not a unique name, could be an identifier, as could Rosa Lee's social security number, a photo of her face, or even a photo of her unusual tattoo.

Note, the record must be *maintained* by an *agency*[10] and be about an *individual*.

Examples of materials that would not qualify as Privacy Act records include restricted-access files that contain detailed individual observations—including sensitive data like age, sex, ZIP code, or medical history—but identify each observation using a randomly assigned number that no longer links back to a person. It does not matter if the files are generated from administrative records or survey responses. These files would not qualify as records because at this point the data are not connected to an identifier.

A ***system of records*** is defined as:

> a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

So, a system of records is a group of the above-defined records that **is retrieved by an identifier**. To qualify as a system of records, the agency must retrieve records by the identifier. It is not enough for the records to have identifiers or be retrievable; the agency must actually use those identifiers to pull up records. For example, if the agency only retrieves the photo of Rosa Lee's unusual tattoo by searching by the name of the company that provided the tattoo, Rosa's record will not qualify as being in a system of records. This is true even if her name and other personal information were included in the record retrieved. The retrieval must use the personal identifier.

Note that a system of records is a **logical description** of records and not a physical one. Records in a system of records may be stored in one file drawer or many, in a single database, or in multiple electronic systems across an agency or even across government.[11] A system of records may also be a subset of a larger group of records or database. The key criterion is that the records are bound together logically.

Examples of records that are not covered by the Privacy Act:

- Records retrieved by date, by state, by subject, or by another mechanism that is not an individual identifier.
- An IT system that simply holds personal information (more criteria must be met, it's not enough just to be an IT system, or just to include personal information).

TO BE A SYSTEM OF RECORDS IT MUST:

1. Be a logical description (not a physical one) of a group of records, which are…
   - Information
   - Maintained by an agency (Federal Executive Branch Agencies (and their contractors) EXCEPT for the immediate office of the President and its advisory offices)
   - About (reflects a quality or characteristic)
   - An individual (U.S. person, defined as a living citizen or Legal Permanent Resident)
   - That is attached to an identifier (almost anything that could be used to pinpoint the record, e.g., name, ID, photo)
2. Actually use the identifier to retrieve records.

10 ***Maintain*** is defined in the Act and includes "maintain, collect, use, or disseminate. ***Agency*** includes federal contractors who are required to manage records covered by the Privacy Act; the Federal Acquisition Regulation dictates language that must be used in contracts (48 C.F.R. § 24.104).

11 The concept of a government-wide system of records is a "legal fiction" created by OMB to allow one agency (with authority over the records) to issue a SORN that guides all agencies managing similar records.

What Responsibilities Does an Agency Have?

Agency responsibilities under the Privacy Act are designed to ensure the fair management of records from start to finish. These rules put the Code of Fair Information Practice into action.

RECORD COLLECTION AND STEWARDSHIP

Agencies are limited in how they gather and maintain information to protect privacy and minimize government overreach:

- **Authority and Minimization:** Agencies must collect only information "relevant and necessary" to carrying out a purpose required by statute or executive order.[12]
- **First-Hand Collection:** Agencies must collect information directly from the individual "to the greatest extent practicable."[13]
- **Individual Consent:** Agencies must get written consent before disclosing a record unless a specific statutory exception applies.[14]
- **Standards of Quality:** Before using a record to make a decision about someone (or sharing the record externally) agencies must make reasonable efforts to assure the record is accurate, relevant, timely, and complete.[15]
- **Rules of Conduct:** Agencies must set and enforce rules of conduct for everyone involved in designing, developing, or operating a system of records.[16]
- **Security Safeguards:** Agencies must set up administrative, technical, and physical protections to keep records confidential and safe from threats that could cause substantial harm, embarrassment, inconvenience, or unfairness to individuals.[17]
- **Matching Programs:** An agency must establish a formal agreement before it uses a computer to "match" a system of records with another (or with state or local government data) for specific reasons, including verifying benefits eligibility. This triggers significant due process controls, though numerous exceptions exist.
- **Keeping Logs:** Agencies must keep an ***accounting of disclosures***, or log, when they share records, except in cases where the information is shared internally or under FOIA. This log includes the date, nature, and purpose of each disclosure, and who received it. The agency must keep the log for at least five years.[18] While rarely requested and often overlooked, this log is essential to trace who has received records. For example, when something goes wrong, it allows individuals to identify the source of unauthorized disclosures.

12 5 U.S.C. § 552a(e)(1).

13 5 U.S.C. § 552a(e)(2).

14 5 U.S.C. § 552a(b).

15 5 U.S.C. § 552a(e)(5) and (e)(6).

16 5 U.S.C. § 552a(e)(9).

17 5 U.S.C. § 552a(e)(10).

18 5 U.S.C. § 552a(c)(1) and (c)(20).

TRANSPARENCY AND NOTICE

Agencies must manage their records "in the sunshine" by providing clear information about what they are doing or plan to do:

- **General and Direct Notice**: Agencies must publish a public notice of their systems of records (called a System of Records Notice or SORN) in the *Federal Register.* They must also give direct notice to the individuals when they collect data from them.[19]
- **Compulsory Process Notice:** Agencies must try to notify an individual if their records are made part of a compulsory process, like a court order or subpoena.[20]
- **Access and Amendment:** Agencies must allow individuals to see records about themselves. Agencies must also allow individuals to request amendments (e.g., corrections) to records that are not accurate, relevant, timely, or complete.[21]
- **Procedural Transparency:** Agencies must publish the exact steps an individual must follow to ask for their records or request amendments.[22]

Note: Agencies may exempt certain records from some of these rules (refer to page 9).

What Rights Does an Individual Have Under the Privacy Act?

Individuals' rights generally mirror the federal agencies' responsibilities. For example, if an agency must provide a notice, the individual has the right to receive that notice. We summarize below the most important rights and limitations.[23]

NOTIFICATION

As referenced above, the Privacy Act requires two notices to individuals about the records being collected and how the agency uses and discloses those records:

- **A general notice** about the existence and character of the records (via a SORN)
- **A direct notice** provided to the individual when the government collects the data

However, it is important to note that the agency is not required to notify an individual directly when it adds or changes disclosures for records it has already collected and usually does not. In the case of significant additions or changes, the agency must provide public notice by publishing an update to the SORN in the *Federal Register*. This means that to find the most current information about how their information is used or shared, individuals must check the *Federal Register.*

19 5 U.S.C. § 552a(e)(4) and (e)(3).

20 5 U.S.C. § 552a(e)(8).

21 5 U.S.C. § 552a(d)(1) and (d)(2).

22 5 U.S.C. § 552a(e)(4)(G) and (e)(4)(H).

23 Under the Act, an agency may allow a person qualified as a parent to act on behalf of a minor, or a guardian to act on behalf of any individual who has been declared by a court of competent jurisdiction to be incompetent due to physical or mental incapacity or age. The agency does not have to grant these rights.

ACCESS AND AMENDMENT

Individuals have the right to see, review, and obtain copies of records about themselves and to see who else has received them (the accounting of disclosures). They may also request amendment if something is not accurate, relevant, timely, or complete.

Requesting an amendment doesn't guarantee that it will be made. If the agency **does not** amend the record, individuals have the right to:

- **Request an independent review** by another agency official (an appeal).
- **Add a statement of disagreement**—their own brief explanation—to the file. The agency must include that explanation in all future disclosures of the record. The agency may include its own explanation for not making the requested amendment.
- **File a civil lawsuit** to challenge in court the agency's refusal to amend the record.

If the agency **does** make a requested amendment, it must send the amended record to everyone who received it before. Note that an individual cannot change a decision about rights or benefits (like a denied application) through the amendment process. Individuals must use the specific program's appeal process to challenge those outcomes.

What About First Amendment Activities?

The Privacy Act does not allow agencies to collect information describing how individuals exercise their First Amendment rights in any context unless:

- **A law requires it:** A specific federal statute says the agency must collect it.
- **The individual allows it:** The individual has given their specific consent.
- **It is for valid law enforcement:** The collection is a part of an authorized law enforcement activity.

This is one of the few protections of the Act that does not require a system of records.

When May an Agency Disclose Privacy Act Records?

A disclosure occurs any time an agency shares information from a Privacy Act record in any form, including letting someone see a record by any method. With some exceptions, agencies may not disclose records without first getting the individual's written consent.[24]

Congress created 13 *exceptions* to this rule for times when getting consent is impractical. They are summarized in the following table:

24 Refer to 5 U.S.C. § 552a(b). The OMB 1975 Guidelines caution that "the consent provision was not intended to permit a blanket or open-ended consent clause, i.e., one which would permit the agency to disclose a record without limit," and that, "[a]t a minimum, the consent clause should state the general purposes for, or types of recipients [to,] which disclosure may be made." 40 Fed. Reg. at 28,954.

Exception	Description	Implementation notes
Need to Know (b)(1)	To agency employees who have a need for the record in the performance of their duties	Most common. Permits disclosure anywhere within an agency, so long as the records are required to carry out authorized functions.
FOIA* (b)(2)	Records *required* to be released under The Freedom of Information Act. (5 U.S.C. § 552)	If FOIA requires disclosure, the Privacy Act permits it. If FOIA permits withholding (i.e., not disclosing the record), the Privacy Act mandates it. The Privacy Act removes the discretion the agency would otherwise have under FOIA.
Routine Use (b)(3)	*for a purpose compatible with the purpose for which [the record] was collected*	Refer to the discussion below.
Census (b)(4)	To the Bureau of the Census for its activities	For purposes of planning or carrying out a census or survey or related activity under Title 13.
Statistical Records (b)(5)	Recipient must provide reasonable advance assurance in writing that records will only be used for statistics and may only receive non-identifiable records.	Can be de-identified records or aggregate products. Rarely used due to researcher desire to link records across sources using individual identifiers.
National Archives (b)(6)	To the National Archives as required to transfer records of permanent historical value	Certain records are designated as being of permanent historical value on the agency's approved records retention schedule. These are transferred to the National Archives for permanent retention.
Law Enforcement (b)(7)	Written request by the head of a law enforcement agency (or delegate) for a specific record and specific authorized activity.	Cannot be used to "generate leads;" agency should have a particular case or matter it is pursuing and be able to identify the authority, purpose, and specific records it requires.
Health/Safety (b)(8)	Compelling circumstances affecting the health or safety of any individual.	Agency must immediately notify the subject's last known address of the disclosure.
Congress (b)(9)	Requests from either House or a Committee or Subcommittee.	Does not apply to individual Members for their own interest or for constituent work. Request must be signed by Speaker, Majority Leader, or Chairman. The Privacy Act does not apply once records are disclosed to Congress.
GAO (b)(10)	To Government Accountability Office (GAO) for GAO activities	To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the GAO. Privacy Act protections no longer apply after the record transfers.

*The Privacy Act itself never requires an agency to make a disclosure under any of the 13 exceptions; each specific disclosure can and should be evaluated on a case by case basis. However, other considerations apply: the Privacy Act explicitly recognized that the FOIA may require disclosure under the (b)(2) exception, and in the case of federal court orders under the (b)(12) exception, not responding puts agency officials in peril of contempt of court. Effectively, this makes FOIA (b)(2) and court orders (b)(12) the only exceptions under which an agency must disclose records.

Exception	Description	Implementation notes
CBO (b)(11)	To the Congressional Budget Office (CBO) for CBO Activities	To the Director of the CBO, or any authorized representative of the Director, in the course of performance of the duties of the CBO. Privacy Act protections no longer apply after the record transfers.
Court Order* (b)(12)	Pursuant to an order from a "court of competent jurisdiction."	Must be signed by a federal judge. Subpoenas are insufficient.
Consumer Reporting (b)(13)	To consumer reporting agencies under the Debt Collection Act	Information may be disclosed to a consumer reporting agency to aid in collecting past due debt to the federal government (other than taxes). See 31 U.S.C. § 3711(e).

*The Privacy Act itself never requires an agency to make a disclosure under any of the 13 exceptions; each specific disclosure can and should be evaluated on a case by case basis. However, other considerations apply: the Privacy Act explicitly recognized that the FOIA may require disclosure under the (b)(2) exception, and in the case of federal court orders under the (b)(12) exception, not responding puts agency officials in peril of contempt of court. Effectively, this makes FOIA (b)(2) and court orders (b)(12) the only exceptions under which an agency must disclose records.

WHAT IS A "ROUTINE USE" EXCEPTION?

A ***routine use*** is a disclosure of a record outside of the agency for a purpose "compatible with the purpose for which it was collected."[25] Under the Act, agencies may create or edit routine uses by publishing a SORN in the *Federal Register*. The agency must also allow at least 30 days for the public to comment and report to OMB and the Congress. While the agency must consider public comments, it is not required to acknowledge, summarize, or justify rejecting them, regardless of how many there are.

The language of a routine use must include both to whom and for what purpose the records will be disclosed. It should be narrowly tailored and should specify the portions of records that will be disclosed, if not the full record. It should not be overly broad or so vague that the purpose of disclosure is unclear, or it permits justification of inappropriate disclosures.

Refer to APDU's Issue Brief, *The "Routine Use" Exception in the Privacy Act of 1974*, for more information on routine uses.

EXCEPTIONS VS EXEMPTIONS

Exceptions and exemptions sound similar and are commonly confused. Here's the difference:

- Privacy Act exceptions give an agency legal permission to disclose a record without consent. They are **exceptions to the written consent rule**.
- Privacy Act exemptions allow an agency to "opt out" of portions of the entire law. **Exemptions remove rights**.

Note that both of these are different than **FOIA exemptions, which allow an agency to withhold records** that they would otherwise have to disclose.

When May an Agency Exempt Records From the Privacy Act?

To protect vital government interests, the Act allows agencies to "opt out" or *exempt* certain records from some of the Privacy Act protections. Agencies must go through a rulemaking process to get an exemption. These exemptions take away rights that an individual would normally have under the Privacy Act.

25 5 U.S.C. § 552a(b)(3).

GENERAL EXEMPTION

The general exemption applies to:

1. Records maintained by the **Central Intelligence Agency (CIA).**
2. Records that are **both** compiled for **criminal law enforcement** purposes and maintained by an agency whose **primary function** is criminal law enforcement.

Agencies that qualify may use this exemption to bypass most of the Act. However, they **may not** exempt themselves from:

- Getting written consent in advance for disclosures (subject to exceptions)
- Keeping an accounting of disclosures
- Ensuring the quality of records before disclosing to anyone other than an agency
- Following the rules on First Amendment activities
- Establishing rules of conduct for employees and security safeguards
- Publishing SORNs and routine uses for comment in the *Federal Register*
- Being subject to criminal penalties

SPECIFIC EXEMPTIONS

Specific exemptions apply to seven types of records:

Any of these types of records:	Can be exempted from any of these things:
■ Classified information	■ Giving access to the accounting of disclosures
■ Law enforcement records that do not meet the requirements of the general exemption^	■ Giving access to the records or entertaining amendments
■ Secret Service records in connection with protecting the President or other individuals	■ Collecting only information that is relevant and necessary
■ Personnel or military promotion records^	■ Including information in the SORN about how to access records or request amendments
■ Background investigations^	■ Making rules relating to access and amendment requests
■ Records required by statute to be used solely as statistical records	■ Listing where the information came from in the SORN
■ Civil service testing materials that would compromise testing objectivity or fairness	

^ These exemptions include safeguards. For background investigation or military promotion records, the agency may **only** exempt itself from granting access to information that would reveal the identity of a source who provided information under an express promise of confidentiality. For law enforcement records, the agency may exempt itself from **all** access requirements unless the record has resulted **in denial of a right, privilege, or benefit** that the individual would otherwise be entitled to, or eligible for, under federal law. In that case, the agency may **only** exempt information identifying a source who was expressly promised confidentiality.

SPECIAL EXEMPTION (D)(5)

The Act permits an agency to exempt records "compiled in reasonable anticipation of a civil action or proceeding." This includes both court cases and administrative hearings. Unlike other exemptions, the agency does not need to create a regulation to use this exemption.

Civil and Criminal Penalties

Agencies and their officials are legally accountable for their responsibilities under the Privacy Act, which provides for both civil and criminal penalties.

Individuals have the right to bring a civil action in federal district court if the agency:

- Refuses to amend a record
- Denies an individual access to their records
- Does not maintain accurate records, resulting in an unfair decision against the individual
- Fails to follow any other part of the Privacy Act, including associated rules

If the court rules in favor of the individual, the remedy may include corrective action or monetary compensation including attorney's fees and reasonable litigation costs.

The Department of Justice (DOJ) may bring criminal charges against an agency official, or a contractor maintaining a system of records on behalf of the agency, for:

- **Unauthorized Disclosure:** willfully disclosing records to someone not entitled to receive them, while knowing that disclosure is prohibited.
- **Maintaining Secret Records:** willfully maintaining a system of records without publishing a SORN.

DOJ may also bring charges against **any person** who knowingly and willfully requests or obtains a record under false pretenses. A person who commits one of these violations is guilty of a misdemeanor and may be fined up to $5,000.

Useful References

- The Privacy Act of 1974, as amended, codified at 5 U.S.C. § 552a
- Implementing Regulations: *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948 (July 9, 1975), available at https://www.govinfo.gov/content/pkg/FR-1975-07-09/pdf/FR-1975-07-09.pdf
- Department of Justice *Overview of the Privacy Act, 2020 edition*: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition
- OMB Circular A-108: *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf