A Privacy Act Primer

The federal government is entrusted with the personal information of millions of people as part of its daily functions. From military enrollment data to data about Medicaid recipients to tax information—the federal government collects, uses, and stores administrative data in hundreds of databases. Given the sensitivity of these data assets, the federal government is subject to a stringent set of confidentiality requirements outlined by the Privacy Act of 1974. The Privacy Act has recently become the subject of litigation in response to the federal government's demands for personal information from the states and their vendors.

On March 20, 2025, President Donald J. Trump signed Executive Order 14243 (EO'), titled "Stopping Waste, Fraud and Abuse by Eliminating Information Silos." *See*, **Exec. Order No. 14243, 90 FR 13681**. The EO directs federal agencies to "take all necessary steps" to ensure that the federal government "has unfettered access to comprehensive data from all State programs that receive Federal funding, including, as appropriate, data generated by those programs but maintained in third-party databases." *Ibid.* The USDA subsequently attempted to enforce this EO by demanding **Supplemental Nutritional Assistance Program (SNAP) data** from the states and third-party benefit processors. This request drew swift criticism and privacy advocates have challenged these actions in **court**, arguing that both the EO and the actions taken by the USDA to enforce it violate the Privacy Act.

In light of renewed attention to the Privacy Act, this brief aims to provide a primer on this critical statute governing the confidentiality of federal records by offering a concise overview of its core components and sections relevant to data sharing and integration.

Disclaimer: This resource is not intended to constitute legal advice, nor is it a substitute for consulting with legal counsel. All information and content are for general informational purposes only. Readers should always consult with their attorney for specific legal advice.

WHY?

The Privacy Act provides safeguards around how the federal government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act was promulgated in 1974 and was enacted as a response to the Watergate scandal and the government's surveillance activities of anti-war protestors.

The Privacy Act in Historical Context: The Privacy Act was one of the earliest efforts to set boundaries around the government's use of personal information. The Privacy Act was passed five years before the **Belmont Report** established ethical principles for research involving human subjects. At the time the Privacy Act was promulgated, there were still no formal protections recognized for the real-world harms that could result from misusing personal data, especially for marginalized communities. While the Privacy Act was a direct response to surveillance abuses espoused by Watergate, the scandal unfolded against a more expansive backdrop of public distrust. Just two years earlier, the **Tuskegee syphilis study** had finally ended, and only 30 years had passed since the forced **internment of Japanese Americans**. The Privacy Act was the culmination of Americans' collective realization of the scope of unchecked government surveillance and data collection.

Continued on next page

A Privacy Act Primer

WHAT?

The Privacy Act of 1974 protects the confidentiality of personally identifiable information of citizens and permanent residents contained in systems of records maintained by federal agencies. Pub Law No. 93-579, 5 U.S.C. § 552a (2018). The Privacy Act defines a record as "any item, collection, or grouping of information about an individual that is maintained by an agency..."5 U.S.C. § 552a(a)(4). A system of records means a group of records under the control of an agency that must be retrievable by a personal identifier. 5 U.S.C. § 552a(a)(5). The Privacy Act does not protect the personal information of the deceased, corporations, and organizations. *See*, OMB 1975 Guidelines, 40 Fed Reg. at 28, 951.

What about the data of people who are not U.S. citizens or permanent residents? The Privacy Act does not apply to records that are solely about non-resident foreign nationals. However, if a record system includes both citizens and non-citizens, the parts that relate to U.S. citizens and permanent residents must comply with the Privacy Act. Federal agencies are encouraged, but not required, to treat the entire system, including records about noncitizens, as if the Privacy Act applies. *See*, OMB 1975 Guidelines, 40 Fed. Reg. at 28951.

WHO?

The Privacy Act applies to federal agencies. The Privacy Act defines "agency" as "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." 5 U.S.C. § 552a(a)(1), 5 U.S.C. § 552(f)(1). Notably, the Privacy Act does not apply to local, state, tribal, or territorial governments.

HOW?

Before any federal agency can collect or share information, it must first inform the public by publishing a *system of records notice* (SORN). 5 U.S.C. §§ 552a(a)(3), (e)–(f). A SORN describes the contents of records held in an agency's system and the processes and procedures for individuals to access or contest any personal information contained in that system. The federal government is required to publish SORNs in the Federal Register for a public comment period before beginning data collection processes. 5 U.S.C. § 552a(e)(4), (a)(5).

Continued on next page

Penn Social Policy & Practice University of Pennsylvania

ACTIONABLE INTELLIGENCE FOR SOCIAL POLICY (AISP)

University of Pennsylvania, 3701 Locust Walk, Philadelphia, PA 19104 • dejak@upenn.edu

A Privacy Act Primer

COMMON EXCEPTIONS TO CONSENT REQUIREMENT

In general, under the Privacy Act, federal agencies are prohibited from sharing personally identifiable information unless that person provides written consent. 5 U.S.C. § 552a(b). However, there are some notable exceptions to the consent requirement that are pertinent to data sharing and integration:

Need to Know within Agency: The Privacy Act allows employees within an agency who regularly handle certain records to access them when needed to perform their official duties. 5 U.S.C. § 552a(b)(1). For example, a revenue agent for the IRS conducting an official audit of a taxpayer's business needs access to the IRS data in connection with her official duties and has a legitimate "need to know."

Routine Use: The Privacy Act allows records to be shared without consent if the record is used for "a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7), (b)(3). Stated plainly, if an agency originally collected a record for one purpose, such as administering a program, the agency is only allowed to share it for another reason that fits with the original purpose. It cannot share the record for an unrelated purpose or reason, such as law enforcement. Significantly, before an agency can share information under the routine use exception, it must publicly list each routine use in the Federal Register, including the categories of users and the purpose of each use, and allow time for a public comment period. 5 U.S.C. § 552a(e)(4); see also, *Fattahi v. Bureau of Alcohol, Tobacco & Firearms*, 328 F.3d 176 (4th Cir. 2003); *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 547-50 (3d Cir. 1989).

A common question that arises is, what is the difference between the "routine use" exception and the "need to know" exception? This table summarizes key differences.

Feature	Need to Know (b)(1)	Routine Use (b)(3)
Who can get the data?	Internal agency employees	External parties (or other federal/state entities)
Use conditions	Must be for job duties	Must be related to the original purpose
Public notice required?	No	Yes (via SORN)
Main Purpose	Support internal agency functions	Facilitate cooperation for uses consistent with program goals
Example	An IRS agent accesses taxpayer return data to conduct an audit	The IRS shares taxpayer information (outside of the department) with the Department of Education to confirm eligibility for student loan repayment programs and the IRS publishes this use in a SORN

Continued on next page

A Privacy Act Primer

Census: The Privacy Act allows records to be shared without consent to the Bureau of Census for "planning or carrying out a census or survey or related activity." 5 U.S.C. § 552a(b)(4).

Statistical Research: The Privacy Act allows an agency to share records without consent if the information is used only for statistical research or reporting and if the data does not identify any individual person. Before sharing, the data recipient must agree in writing to only use the data for that purpose. 5 U.S.C. § 552a(b)(5).

Other exceptions: The Privacy Act also allows disclosures for FOIA requests (§ 552a(b)(2)), for the health and safety of an individual (§ 552a(b)(8)), to the National Archives and Records Administration (§ 552a(b)(6)), for federal civil and criminal law enforcement activity that is written, specific and lawful (§552a(b)(7)), to Congress (§ 552a(b)(9)), to the Comptroller General (§ 552a(b)(10)), per court order (§ 552a(b)(11)), and to a consumer reporting agency. (§ 552a(b)(6)).

THE COMPUTER MATCHING ACT OF 1988

The Privacy Act was amended with the Computer Matching and Privacy Protection Act of 1988 which added several new provisions. See, 5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o), (p), (q), (r), (u). Notably, this Act restricts data sharing between government agencies by limiting "matching programs." 5 U.S.C § 552a(a)(8). Federal agencies cannot run matching programs on systems of records unless there is a written agreement between the agencies. 5 U.S.C. § 552a(o). There are requirements for what the agreement must contain, which include conditions, safeguards and procedures for disclosure of the data. 5 U.S.C. § 552a(p), (q), (r), (u) (2018).

CONCLUSION

As federal efforts to access state and third-party data intensify, understanding the Privacy Act of 1974 is more critical than ever. This foundational law establishes essential guardrails for how federal agencies collect, use, and disclose personal information. Before turning over data, state and local governments should take proactive steps to ensure legal compliance. It is critical to distinguish between using data to administer programs and services as intended, and using that same data for enforcement—such repurposing risks undermining trust and turning essential government functions into tools of surveillance or punishment. These include carefully reviewing whether a federal request aligns with the Privacy Act and other applicable laws, establishing internal protocols for evaluating data-sharing requests, and consulting legal counsel.

ADDITIONAL RESOURCES

Electronic Privacy Information Center. (n.d.). *The Privacy Act of 1974*. Retrieved from, https://epic.org/the-privacy-act-of-1974/

U.S. Department of Housing and Urban Development. *Computer Matching Agreement Guidance and Overview*. (n.d.). Retrieved from, https://www.hud.gov/sites/dfiles/OCHCO/documents/HUDCMAOverview.pdf

Winn, P. A. (2022, October 12). Overview of the Privacy Act of 1974 (2020 edition). Office of Privacy and Civil Liberties.