apdu
ASSOCIATION of PUBLIC DATA USERS

Managing "Mixed Systems" of Records Under the Privacy Act of 1974

By Bethanne Barnes and Maya A. Bernstein

The Privacy Act of 1974 (the Act) sometimes creates a tension between the strict language of the law and the way things really work. The Act only protects ***U.S. persons***, i.e., citizens and lawful permanent residents (LPRs, or "green card" holders).[1] However, some *agencies*[2] serve both U.S. persons and non-U.S. persons in the same program. In those cases, agencies run ***mixed systems*** that contain *records*[2] on both populations. They do this for three main reasons:

- **Don't need to know:** Many program missions (such as postal services) do not require immigration status to function; they provide services regardless of status.
- **Broad Scope:** Some programs (such as customs enforcement) serve people from all over the world but stop tracking immigration status once the job is done.
- **Life Changes:** Status is not static. A refugee or visitor may become an LPR or citizen. These life changes don't automatically get updated in old records.

Agencies often can't tell who is a U.S. person, and therefore covered under the Act, because they rarely need real-time data on immigration status to run their programs.

The Cost of a Two-Tiered System

Treating two group's records differently in the same database is risky:

- **The "Secret System" Trap:** It is a criminal offense to keep a Privacy Act *system of records*[2] on U.S. persons without public notice (called a SORN). If an agency thinks its records are only about non-US persons and doesn't publish a SORN, they are in violation of the law the moment any person in that system gets a green card.
- **Verification Gridlock:** Without a master list of citizens against which agencies can quickly and legally check, agencies would have to require a burdensome proof of status for every request. This would be much too slow and expensive.
- **Bad Data:** Agencies rely on accurate, relevant, timely, and complete data to make life-altering decisions. If a group of people cannot review or correct their files, the agency is forced to make its decisions on less reliable information.

1 Refer to 5 U.S.C. § 552a(a)(2) ("the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence"). The Judicial Redress Act of 2015 enables citizens of certain foreign countries to bring suit under certain provisions of the Privacy Act in the same manner as U.S. Persons. Refer to 5 U.S.C. § 552a note.

2 For definitions and more context on agencies, records, and systems of records in the Privacy Act of 1974, refer to the APDU *Primer on the Privacy Act of 1974* available at https://apdu.org/apdu-in-action/Data-Privacy-Resources/.

A Simple Administrative Solution

To lower these risks, in 2007 the Department of Homeland Security (DHS) adopted a new policy[3] based on the Office of Management and Budget's original Privacy Act guidance[4] and, for the first time, required a common approach across all mixed systems within DHS:

- **Common Standards:** All records within a system of records follow the same privacy and security practices, and the same exemptions apply, ensuring a uniform, efficient baseline of practice.
- **Expanded Administrative Rights:** Non-U.S. persons get notice and are allowed to see their records and request fixes, preventing secret systems and reducing errors.
- **Legal Limits:** The policy is an administrative fix; it cannot and does not give non-U.S. persons the right to sue the government under the Privacy Act.

Most agencies adopted this approach at the time, informally or formally, due to its practicality.

Current Status: A Fragmented Landscape

The landscape has shifted with executive priorities. In 2017, *Executive Order 13768* stripped non-U.S. persons of Privacy Act protections (to the extent allowed by law).[5] Agencies quickly adopted a "U.S. persons only" approach, bringing back the very problems the DHS policy tried to fix. In 2021, *Executive Order 13993* reversed that stance, once again allowing agencies to extend rights to everyone.[6] DHS restored its approach to mixed systems in 2022.[7] Other agencies followed, applying the policy to specific systems of records or the entire agency.

When agencies implement the policy, they may run more efficiently and fulfill their missions more effectively. If the agency does not invoke an exemption (such as for law enforcement), the policy provides more people with the opportunity to exercise Privacy Act rights, such as accessing their own records. Conversely, where this policy is not adopted, ignored, or irrelevant due to exemptions, these mutual benefits disappear.

Inconsistency creates a fragmented landscape where protections depend on which agency holds the records. The fragmentation is even more confusing to the public, which does not have a simple way to find out to which programs the policy applies. Without standardizing legislation, this lack of uniformity is likely to persist.

THE GLOBAL STAKES: RECIPROCITY

International data sharing is a two-way street. Other countries are more likely to share data with the U.S. if they trust we will protect their citizens' privacy. This helps ensure that American citizens receive similar privacy protections when abroad.

3 U.S. Department of Homeland Security. (2009, January 7). *DHS privacy policy regarding collection, use, retention, and dissemination of information on non-U.S. persons* (Privacy Policy Guidance Memorandum 2007-01, as amended). https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2007-01.pdf

4 Office of Management and Budget. (1975). *Privacy Act implementation: Guidelines and responsibilities*. 40 Fed. Reg. 28948. (July 9, 1975) https://www.govinfo.gov/content/pkg/FR-1975-07-09/pdf/FR-1975-07-09.pdf

5 Exec. Order No. 13,768, 3 CFR 268 (2018). https://www.govinfo.gov/content/pkg/CFR-2018-title3-vol1/pdf/CFR-2018-title3-vol1-eo13768.pdf

6 Exec. Order No. 13,993, 3 CFR 439 (2022). https://www.govinfo.gov/content/pkg/CFR-2022-title3-vol1/pdf/CFR-2022-title3-vol1-eo13993.pdf

7 U.S. Dept. of Homeland Security, (2022, May 4). *Privacy Policy regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information* (Instruction 262-16-001). https://www.dhs.gov/sites/default/files/2024-03/22_05_04_priv_plcycollectionuseretentionpiiinstruction_262-16-001.pdf