As Federal Agencies Rewrite Privacy Rules, What It Means for Your Data

February 28, 2026 - Several federal agencies are quietly rewriting the fine print that governs how your personal information moves inside the government.

In recent days, agencies including the Nuclear Regulatory Commission and the Federal Communications Commission have proposed or finalized changes to their "systems of records" under the Privacy Act of 1974. These notices may sound technical, but they function as the official rulebooks for how agencies collect, store, use, and share information about you.
The common thread in the new revisions is expanded or clarified permission to share certain records with the U.S. Department of the Treasury for fraud prevention and improper payment screening. The changes stem from Executive Order 14249, which directs agencies to strengthen payment integrity and reduce waste, and from follow-up guidance issued by the Office of Management and Budget.

In practical terms, this means that before some federal payments go out the door - grants, reimbursements, benefits, vendor payments - the data behind them may be screened through Treasury systems such as Do Not Pay. Agencies are updating their Privacy Act notices to formally allow that sharing as a "routine use," a legal term that permits disclosure without individual consent if it is compatible with the original purpose for collecting the data.

For consumers, this signals a shift toward more centralized, automated verification.

How the system works today

Under the Privacy Act, agencies must publish a System of Records Notice, or SORN, describing what data they keep, why they keep it, and the specific circumstances under which it can be shared. Sharing without consent is generally prohibited unless it falls within an exception. One of the most common exceptions is "routine use."

Historically, agencies have maintained largely separate databases tailored to their programs. They already share information for law enforcement, audits, and program administration. But much of the fraud detection has happened after payments are made, through investigations or recovery efforts.

The recent rule changes move more of that scrutiny to the front end.

Instead of relying primarily on post-payment audits, agencies are formalizing pre-payment screening through Treasury tools. That can include checking whether a payee appears on exclusion lists, whether identity information matches other federal records, or whether there are indicators of duplicate or improper payments.

What changes if the rules take effect

If implemented as written, the revisions will make it easier and more standardized for agencies to transmit certain categories of personal data to Treasury systems before issuing payments.

For the average consumer, the impact will likely be subtle but real.

If your records are accurate and consistent across agencies, you may never notice the difference. Payments may simply move through a more automated fraud filter behind the scenes.

But if your records contain discrepancies - a recent name change, a hyphenated last name, an outdated address, inconsistent employer information, or similar data mismatches - you could encounter delays, additional verification requests, or temporary payment holds while discrepancies are resolved.

Programs like the FCC's Lifeline benefit, which supports phone and internet access for eligible households, are among those updating their notices to allow disclosures to Treasury under the executive order. That does not mean personal data becomes public. It does mean more interagency screening before funds are released.

In effect, the government is tightening internal data highways.

A broader shift toward centralized screening

Taken together, the recent rule changes suggest a continued push toward centralized payment screening and stronger fraud controls across government programs.

Supporters argue that pre-payment verification reduces waste, protects taxpayer dollars, and prevents fraud before it

happens. Critics warn that as more data flows between agencies, the risk of errors, overreach, or misuse increases, especially when automated systems flag individuals based on incomplete or outdated information.

For everyday Americans, the most immediate impact will likely be procedural rather than dramatic: more cross-checks, more backend data comparisons, and possibly more paperwork when records do not line up.

The deeper question is how well agencies balance two competing goals - reducing fraud and protecting privacy.

As these revised notices move through public comment and into effect, they will shape not just how the government pays its bills, but how your personal data travels inside the federal system.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS