The Leadership Conference
on Civil and Human Rights

1620 L Street, NW
Suite 1100
Washington, DC
20036

202.466.3311 voice
202.466.3435 fax
www.civilrights.org

April 30, 2025

The Honorable Lori Trahan
2233 Rayburn House Office Building
Washington, DC 20515

Submitted electronically via email to PrivacyActRFI@mail.house.gov

Re: Request for Information: Reforming the Privacy Act of 1974

Dear Representative Trahan,

On behalf of The Leadership Conference on Civil and Human Rights, a coalition charged by its diverse membership of more than 240 national organizations to promote and protect the civil and human rights of all persons in the United States, and its Center for Civil Rights and Technology, we write in response to your Request for Information (RFI) on Reforming the Privacy Act of 1974.

The need to update the Privacy Act has never been more pressing. Elon Musk and the so-called Department of Government Efficiency (DOGE) have accessed, collected, and combined previously secure federally-held data. Their actions threaten the privacy of individuals' sensitive personal information held by the government and the laws Congress passed to protect that data, including the Privacy Act, which were put in place to protect against abuse, provide for data security, and gain public trust. It has become clear that privacy laws must be modernized, especially considering how federal data are already being weaponized to identify and target individuals based on immigration status, and potentially, people from other historically marginalized and vulnerable communities, as well.

Congress Enacted the Privacy Act of 1974 to Protect Individuals' Data and Gain Public Trust

The passage of the Privacy Act came in the wake of the McCarthy era—one of the darkest periods in American history, marked by unceasing ideological warfare and a government recklessly abusing power, obsessed with constructing vast record systems to house files on hundreds of thousands of individuals and organizations. Secret dossiers on private citizens were the primary tool for suppressing free speech, assembly, and opinion, fueling decades' worth of sedition prosecutions, loyalty oaths, and deportation proceedings. Countless writers, artists, teachers, advocates, and attorneys saw their livelihoods destroyed, while civil

servants were routinely rounded up and purged as part of the roving inquisitions.[1] Actions taken during the Watergate scandal furthered the fear of unchecked government surveillance, especially the potential for the FBI to access and reveal the sensitive information the government has on all of us.

In response, Congress passed the Privacy Act. The law was aimed at reining in the power of the administrative state and preventing abuse. While it contemplated the emergence of high-speed telecommunications and data systems, Congress did not fully consider the rapid pace of the capabilities of these systems, the rise of the Internet, the collection of massive amounts of data on individuals and organizations, and the adoption of data-dependent artificial intelligence (AI) systems.

Modernization of The Privacy Act is Warranted

The recent actions by DOGE highlight critical vulnerabilities in the protection of sensitive personal data held by the government. DOGE's access to vast troves of personal information, including Social Security numbers, tax records, financial data, and educational data, has raised significant concerns about unauthorized disclosures and potential misuse.[2] In addition, the way in which the Trump administration has wielded the data seized by DOGE, targeting individuals based on their immigration status and organizations deemed "disloyal" to the president is alarming.[3] These developments underscore the urgent need to modernize the Privacy Act to ensure robust safeguards against such risks and protecting individuals across the country from targeting and abuse. In the meantime, numerous lawsuits have been filed alleging violations of data privacy laws.[4]

Congress was right to seek to protect individuals and families across the United States in the aftermath of the McCarthy era and Watergate. In this moment, Congress has a moral imperative to protect individuals and families from new and evolving threats to our privacy. We have entrusted the government with our most sensitive data,[5] but the Trump administration and DOGE have broken that trust. There is growing fear that the data accessed can and will be abused in ways that violate civil rights and harm targeted communities, including the most vulnerable and marginalized communities. Contributing to that fear is a lack of transparency about the credentials of the individuals accessing people's personal data; how these invididuals are using the data; how are they keeping the data secure to prevent it from being breached and falling into the hands of criminals and foreign adversaries; and the accountability measures that are in

---

[1] Dell Cameron, "Democratic Senators Call for Privacy Act Reform in Response to DOGE Takeover," Wired (Mar. 31, 2025), https://www.wired.com/story/democratic-senators-privacy-act-reform-doge-takeover/.
[2] "DOGE and Government Data Privacy," The Leadership Conference on Civil and Human Rights and the Center for Democracy and Technology (last updates March 17th, 2025), https://civilrights.org/2025/03/20/doge-government-data-privacy/.
[3] Makena Kelly and Vittoria Elliot, "DOGE Is Building a Master Database to Surveil and Track Immigrants," Wired (Apr. 18, 2025), https://www.wired.com/story/doge-collecting-immigrant-data-surveil-track/.
[4] "Litigation Tracker: Legal Challenges to Trump Administration Actions, Just Security (last updated April 21, 2025), https://www.justsecurity.org/107087/tracker-litigation-legal-challenges-trump-administration/.
[5] Emily Badger and Sheera Frenkel, "Trump Wants to Merge Government Data. Here Are 314 Things It Might Know About You," New York Times (Apr. 9, 2025), https://www.nytimes.com/2025/04/09/us/politics/trump-musk-data-access.html?unlocked_article_code=1.-U4.iSlG.K0rRHUL3t4fl&smid=url-share.

place, if any, to validate that these data, which are very valuable in terms of commercial use, are not used for personal gain of individuals in and connected to the administration.[6]

We acknowledge that there may be instances where the ability to access and use data is necessary for advancing public benefit. For example, the information gained from the decennial census informs the allocation of resources and political representation for communities across the country, and for communities to understand their own circumstances and needs. Preserving the ability to use data for such beneficial purposes, while at the same time not creating loopholes to misuse data, should be kept in mind when considering updates to the Privacy Act.

In the absence of congressional action on broader privacy protections and without reforms to modernize the Privacy Act, the message to individuals is clear: the public should have no expectation of privacy as we are now living in a surveillance state where individuals are being punished for who they are, where they are from, and their closely held beliefs. Any reform to the Privacy Act must strengthen protections for individuals' personal data, ensure accountability for misuse, and enhance transparency.

Reforms in Response to DOGE's Action:

We agree with the measures included in the recent proposal from Senator Ron Wyden, D. Ore., and others on the Privacy Act. These reforms are in direct response to DOGE's activity that highlighted the gaps and shortcomings of existing privacy laws:

- **Ensure Courts' Ability to Hold Agencies Accountable:** The ability to seek judicial redress has proven to be one of the few, if not sole, recourse mechanisms to seek accountability from DOGE for its data grab and abuse. It is crucial to preserve and strengthen courts' authority to stop programs and actions while lawsuits are pending and allow individuals across the U.S. redress for a range of damages, including the mental and emotional distress caused by privacy violations.
- **Address Use of Data to Draw Inferences and Identify Individuals:** The ability to interrogate data and draw inferences, including tying data thought to be anonymous back to specific individuals, is a direct result of advances in technology, and too easily exploited. Modernizing the law to cover any information that identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual will help close this gap.
- **Minimize Data**: A long-held privacy tenet is that entities should only collect data needed to perform the specific function for which the data was provided. Limiting information sharing to the minimum necessary for a legally authorized purpose, and only if consistent with what an agency previously stated they would use records for, would help curb abuse and increase public trust.
- **Prohibit Use of Data for Other Purposes than Why It Was Collected:** Data should only be used for the purposes for which it was collected. We recommend narrowing the so-called

[6] "DOGE and Government Data Privacy," The Leadership Conference on Civil and Human Rights and the Center for Democracy and Technology (last updated March 17, 2025), https://civilrights.org/2025/03/20/doge-government-data-privacy/.

"routine use" exception for sharing information by further requiring that "routine use" disclosures be "appropriate and reasonably necessary."

Additional Suggested Areas for Modernization:

- **Enhanced Data Protection Measures:** The current Privacy Act lacks specific requirements for modern encryption and security protocols, leaving sensitive data vulnerable to breaches. Section 552a(e)(10) requires agencies to establish safeguards to ensure the security and confidentiality of records, but it does not address the use of advanced encryption technologies. Updating this section to include mandatory encryption standards will significantly reduce the risk of unauthorized access and data breaches.
- **Stricter Access Controls:** Section 552a(b) outlines conditions under which personal data can be disclosed without consent, but it does not adequately address internal access controls. Implementing stricter access control mechanisms, such as multi-factor authentication and role-based access, will ensure that only authorized personnel can access sensitive information. This will reduce the risk of internal misuse and unauthorized disclosures.
- **Transparency and Accountability:** Section 552a(e)(4) of the Privacy Act requires agencies to publish notices of their systems of records in the Federal Register, but lacks comprehensive transparency measures regarding data access and usage. Introducing mandatory reporting requirements for data access and usage will enhance transparency and accountability, allowing individuals to know who accessed their data and for what purpose.
- **Updated Consent Requirements:** The existing consent provisions (Section 552a(b)) are outdated and do not reflect the complexities of modern data usage. We support enhancing individual control over personal information. Revising these protocols to ensure individuals are fully informed about how their data will be used and shared will enhance their control over personal information. We recommend including clear, concise consent forms and the ability to easily withdraw consent. Explicit consent can help prevent unauthorized access.
- **Regular Audits and Compliance Checks:** While the Act requires agencies to maintain records of disclosures (Section 552a(c)), it does not mandate regular audits or compliance checks. Establishing regular audits and compliance checks will ensure adherence to privacy standards and identify potential vulnerabilities. This proactive approach will help prevent data breaches and misuse.

Responses to the Questions Posed in the RFI:

1. **General Questions**
    a. **Concerns:** Concerns include the potential for misuse of individuals' personal information, including to target individuals based on immigration status, gender identity, or other protected statuses; lack of transparency in how data are being handled; and insufficient safeguards to protect against unauthorized access. The risk of profiling and discrimination based on collected data is also a significant concern.
    b. **Balancing securing privacy with other priorities:** There must be a privacy-first approach to ensure that any measures to promote security, reduce waste, fraud, and abuse, or improve service delivery do not compromise individual privacy rights.

c. **Privacy risks created by AI:** The use of AI systems can lead to unintended biases and discrimination in decisionmaking. This risk can be mitigated by enacting regulations on AI use, ensuring transparency, mandating risk assessments and regular audits to identify and mitigate biases, and ensuring compliance with privacy standards.

2. **Modernizing the Privacy Act**
   a. **Definitions**: To better reflect the current landscape of data collection, the definitions should be updated to include digital records and data points that can be used to identify individuals. All data capable of identifying individuals should be covered under the Act.
   b. **Disclosure**: The Act would be strengthened by ensuring that only essential information is collected and stored. Individuals should be able to access and amend their data through secure online portals and mobile applications to facilitate this process. Consideration should be given to allowing for a "right to be deleted" with clear guidelines on any exceptions, including for service delivery.
   c. **Written consent**: Agencies should consider the needs of impacted communities, including those of the disability community, older individuals, and individuals with language needs, when providing consent mechanisms, whether analog or digital. Consent mechanisms should provide individuals with the ability to view and manage their consent across agencies. Explanations of how data will be used, stored, or shared should be provided.
   d. **Exceptions**: Any exceptions should be narrowed to ensure that only those with a legitimate and specific need for the data can access it. Agencies should be required to document and publicly disclose the criteria and instances for exceptions. Access should be limited based on roles of the requestors and the sensitivity of the data. Political appointees and civil servants should have different levels of access, along with stricter controls for high-risk data.
   e. **Definition of "routine use"**: The definition should be strengthened and ensure uses are strictly aligned with the original purpose of data collection.
   f. **Anonymized data**: The Act should be updated to provide stricter guidelines on data anonymization and ensure protections include data, including anonymized data, which can be used to identify individuals.
   g. **Data sharing**: Where data are shared, including for delivery of services or for public benefit, then secure data sharing platforms should be used. Psrotocol should be put in place to ensure data are protected through encryption or other means and that access is controlled. Clear agreements and adherence to privacy protections, such as data minimization and use limitations, must be put in place. Updating the Act should include restrictions to ensure that data sharing within agencies is limited to essential purposes and subject to strict oversight and transparency.
   h. **Civil remedies**: Individuals should have the ability to seek effective redress when data are mishandled or abused. Congress can do this by lowering barriers to the ability to pursue legal remedies and by increasing penalties.

i. **Privacy leadership**: The Office of Management and Budget (OMB), National Institute of Standards & Technology (NIST), and Chief Information Officers (CIOs) have essential roles to play. OMB can exert leadership by setting standards and guidelines and ensuring consistent and sound privacy practices across the agencies. NIST can develop and provide technical guidance and tools to help agencies implement best practices in privacy protection. CIOs can oversee the implementation of privacy policies and be accountable for compliance. Independent bodies should also provide oversight and conduct audits to ensure privacy practices are compliant with requirements.

3. **Related Laws**

Congress should consider modernizing other applicable privacy laws to account for current technologies and privacy practices to keep pace with advancements and emerging privacy risks. The Leadership Conference, its coalition, and civil society have called for comprehensive federal privacy laws that explicitly protect the civil rights of every individual in the U.S., and it is critical that the government is held accountable for protecting privacy as well.

Conclusion

The Privacy Act has been essential in protecting individuals' privacy. But while groundbreaking at its inception, the law now has several limitations in today's digital and automation age. The Act's provisions for consent and disclosure are outdated, failing to account for the complexities of contemporary data usage and sharing practices. Additionally, the enforcement mechanisms are insufficient to ensure compliance, particularly in the face of deliberate non-enforcement by certain government entities. These shortcomings necessitate modernizing the Privacy Act to align it with current technological and societal realities. In considering changes to the Privacy Act, Congress should not open the door to revisions that would diminish privacy safeguards or otherwise undermine agency accountability, or other actions that would chip away at our democratic values.

We appreciate the opportunity to respond to this RFI and we look forward to collaborating on this crucial update to safeguard the privacy rights of individuals and families. Should you require further information or have any questions regarding this issue, please feel free to contact Jonathan Walter, senior policy counsel, at walter@civilrights.org.

Sincerely,

Alejandra Montoya-Boyer
Senior Director, Center for Civil Rights and Technology