Response to Representative Trahan's Privacy Act Request for Information

Submitted by the AFL-CIO Technology Institute

April 30, 2025

Dear Representative Trahan:

Thank you for your leadership in seeking to modernize the Privacy Act of 1974. The AFL-CIO Tech Institute works at the intersection of technological innovation in the workplace, centering worker knowledge, expertise, and interests in our modern innovation-based economy to ensure that technological change creates widespread prosperity for all American workers. The Tech Institute was established in 2021 by the AFL-CIO, the national labor federation of 63 national affiliates and 15 million workers across every sector of our economy and public services. The AFL-CIO Tech Institute appreciates the opportunity to provide input on this crucial legislation, particularly at a time when privacy and data challenges are harming workers and everyday Americans.

The current privacy crisis precipitated by the Department of Government Efficiency (DOGE) has laid bare the inadequacies of the Privacy Act of 1974 in its current form. DOGE has bypassed normal means of oversight and gained access to and control over critical technology systems and sensitive data of nearly all federal agencies. This unchecked access threatens not only worker privacy and union activities but also the privacy rights of all Americans.

The scope and scale of DOGE's data access across government underscores the urgent need for Privacy Act reform. The agencies targeted include critical departments like the Office of Personnel Management (OPM) and General Services Administration (GSA), and also those that support civil society functions such as research, regulation, and consumer protection. Alarmingly, DOGE has also accessed data critical to workers from the National Labor Relations Board (NLRB). This level of access to sensitive personal data creates unprecedented risks for federal workers, their unions, and the general public.

1.a. What are your biggest concerns with the federal government's collection, maintenance, use, or dissemination of personal information?

Our most significant concerns include:

1. **Unprecedented access to sensitive personal data**: DOGE has gained control of government databases and technology systems, giving Musk access to valuable troves of data. This includes Social Security numbers, tax records, health information, and home addresses of millions of Americans, creating significant privacy and security risks for workers and the general public.
2. **Cross-agency data aggregation**: DOGE's ability to combine data across agencies creates profound privacy risks. Separate databases is an intentional strategy to protect

the security of data, ensuring that if there is a breach, only some data is compromised. But combining various agency databases allows for complete access and viewing of people and businesses. This capability could enable the creation of comprehensive profiles of individuals, revealing sensitive information that was never intended to be connected.

3. **Insufficient controls on "special government employees"**: The current Privacy Act does not adequately restrict access by non-traditional government personnel, such as DOGE's "special government employees." These individuals, often with significant conflicts of interest, have gained unprecedented access to sensitive data. For example, Musk has direct conflicts of interest with several companies competing for some of these contracts, and he has numerous businesses currently under investigation from agencies with direct oversight.
4. **AI-driven analysis and decision making without proper guardrails**: AI systems can be used to analyze personal data and make consequential decisions without appropriate transparency or accountability. For example, DOGE is reportedly using large language AI models to analyze the responses federal employees provide to Musk's directive that they give a weekly report on their work, all in an effort to streamline and expedite the process to fire people from their jobs. Similar approaches could be used to analyze the data of everyday citizens.
5. **Deliberate circumvention of logging and accountability mechanisms**: DOGE has demonstrated a pattern of tampering with systems that could harm the delivery and timing of Veterans benefits, Social Security payments, and Medicaid and Medicare benefits, resulting in catastrophic consequences. This deliberate avoidance of accountability mechanisms makes it nearly impossible to audit data access and use, which affects federal workers, unions, businesses, and Americans who rely on government services.
6. **Commercial exploitation of government data**: There are serious risks of corruption, theft, and grift where government data access could be used for private gain. Personal information of Americans could be exploited for commercial purposes, particularly when those with access to the data have direct financial interests in AI development and other data-driven businesses.
7. **State-level DOGE expansion**: Many copycat DOGE efforts have emerged at the state level. State agencies hold vast amounts of sensitive information including driver's licenses, property records, and benefit enrollment data, creating additional privacy risks for everyday Americans. A recent executive order pressures states to share their data with the federal government, creating a dangerous pipeline of personal data flowing to DOGE and further endangering the public.

1.c. What are the unique privacy risks created by the government's use of artificial intelligence? How can Congress mitigate those risks?

The government's use of AI presents several unique privacy risks for both workers and everyday Americans:

1. **Mass automated decision-making**: AI systems are being used to make significant decisions about benefits, services, and employment without proper oversight or transparency. As an employer, the federal government could potentially use workplace AI systems for key functions, such as hiring, scheduling, task assignment, performance evaluation, and even disciplining or terminating workers. Similar systems could affect everyday Americans seeking government services or benefits.
2. **Training AI models on sensitive government data**: There are significant concerns that government data could be used to train private AI systems, particularly given Musk's ownership of xAI. This could create unfair competition where Musk can leapfrog ahead in AI development due to data access. This could lead to the exploitation of Americans' sensitive personal information for private commercial gain.
3. **De-anonymization capabilities**: Allegedly pseudonymized data can be re-identified, sometimes quite easily. This capability is particularly concerning when combined with cross-agency data access, creating risks for invasion of privacy by linking sensitive information like Social Security numbers, tax records, and health information to specific individuals.
4. **Opaque decision-making and algorithmic bias**: AI hides how data is used to make decisions. This lack of transparency and potential for bias can lead to discriminatory outcomes and denial of benefits to vulnerable populations.
5. **Surveillance capabilities**: The combination of AI systems with government data creates unprecedented surveillance capabilities. Risks of targeted AI-fueled harassment and surveillance of federal workers and opponents. Similar capabilities could be used to monitor the activities of everyday Americans.
6. **Security risks:** Unsafe, untested AI systems can create security risks, especially for critical infrastructure and national security. They can also create cybersecurity vulnerabilities that can harm all Americans.

Congress can mitigate these risks by:

1. **Implementing comprehensive AI governance**: It is essential to have guardrails against harmful uses of AI that would protect both workers and the general public. These should include transparency, human-in-the-loop processes, the right to human review, opt-out/override options, whistleblower protections, and worker consultation.
2. **Prohibiting discriminatory use**: Explicitly prohibit the use of AI systems to target protected classes or engage in discriminatory practices. AI systems must uphold democratic values and not reinforce structural racism, sexism, and other forms of worker exclusion and oppression.
3. **Restricting data use for AI training**: Establish clear limits on the use of government data to train AI systems, particularly those owned by private entities with conflicts of

interest. If a non-governmental entity is found to have unlawfully used government data to train AI systems, all data retained and any AI model trained on the data - including by entities other than the one that originally obtained the data - should be mandatorily deleted as a statutory remedy, in addition to minimum statutory damages.

4. **Implementing robust security measures**: Require enhanced cybersecurity protocols for AI systems accessing sensitive data. Systems must protect personal and worker information through comprehensive security measures.
5. **Mandating consultation**: Require meaningful public input before implementing AI systems that affect individuals' rights or access to government services. The existing mechanism, Privacy Impact Assessments and Systems of Records Notices, have often failed to garner meaningful consultation and transparency, so these processes need to be made more robust.

2.a.ii. Should the Privacy Act address privacy concerns faced by organizations, including businesses and nonprofits? If so, how?

Yes, the Privacy Act should be expanded to address certain privacy concerns of organizations, particularly labor unions. This expansion is critically important given the unprecedented access to data across federal agencies.

1. **Protection of collective and organizational information**: Organizations that advocate for civil rights, labor rights, and other public interests hold sensitive information that deserves protection similar to individual data.
2. **Prevention of targeting and suppression**: There are significant concerns about how data from the NLRB and other sources is being used to identify union members, union leaders, and those in bargaining units. NLRB data could be weaponized by private companies to target, intimidate, and even fire union members, discouraging whistleblowers and undermining fair processing of labor cases. Similarly, data from the Department of Labor and the Internal Revenue Service could be used to trigger audits, challenge non-profit status or otherwise target organizations. When government entities with conflicts of interest have access to organizational data, this creates significant risks not only for workers but for all Americans exercising their rights to organize and advocate.

We recommend the Privacy Act be expanded to:

- **Establish standing for representative organizations**: Allow labor unions and other organizations to bring Privacy Act claims on behalf of their members when data is improperly accessed or disclosed.
- **Require notification to affected organizations**: Mandate that agencies notify organizations when data related to their activities has been accessed or potentially compromised. This would help organizations take protective measures for their members and constituents.

2.b.i. Should the law's provision that requires agencies to only maintain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency," or data minimization provision, be strengthened? If so, how?

Yes, the data minimization provision should be significantly strengthened. The current DOGE situation demonstrates the urgent need for stronger data minimization requirements to protect both workers and the general public.

1. **Implement strict data retention limits**: Require data to be automatically deleted or archived within the agency in compliance with National Archives and Records Administration (NARA) regulations after its purpose has been accomplished, with special protections for sensitive categories. Data that is no longer in active use should no longer be disclosable, including within the agency, under the “agency need to know” or “routine use” exceptions (5 U.S.C. 552a(b)(1) and (b)(3) respectively), but should still be disclosable under the other Privacy Act disclosure exceptions. Such archived data should also be statutorily excluded from any matching programs or agreements. The “need to know” exception should clarify that labor unions are included in the exception in instances where sensitive personal data is: 1) necessary for purposes of representational activities; 2) is inextricably linked to the conditions of employment for the union-represented worker; and 3) the labor union and the agency are accessing the data within the agency firewall.
2. **Mandate audit trails for all data access**: The Privacy Act should explicitly require comprehensive logging of all data access and prohibit the disabling of audit mechanisms.
3. **Prohibit mass data collection for AI training**: The law should explicitly prohibit the collection of data specifically for training AI systems without clear congressional authorization.
4. **Establish strict purpose limitations**: Data collected for one purpose should not be used for unrelated purposes.

2.e.i. It is widely known that anonymized data can sometimes be combined to potentially identify individuals. How can the Privacy Act be updated to mitigate against the risks of de-anonymization in large datasets?

The risk of de-anonymization is particularly concerning for both workers and the general public, especially when data from multiple agencies can be combined.

1. **Expand protected information** to include information that could be used for re-identification when combined with other data sources. This should explicitly include not only traditional identifiers but also behavioral data, device identifiers, geolocation information, and similar data points that can be used for re-identification.
2. **Create special protections for sensitive datasets**, particularly those containing information about workers, union membership, or protected activities.

3. **Establish liability for re-identification attempts** or successful re-identification of anonymized government data. This would create a deterrent against attempts to circumvent privacy protections.

2.f.i. Should Congress consider strengthening the Privacy Act's private right of action to seek injunctive or compensatory relief? If so, how?

Yes, Congress should significantly strengthen the Privacy Act's private right of action. The current enforcement mechanisms are inadequate to address the scale and severity of potential privacy violations, particularly in the context of DOGE's unprecedented access to data systems.

We recommend:

1. **Expand standing to include organizations**: There should be provisions to allow organizations, including unions to bring suit on behalf of their members. This would allow unions to protect workers and the public when agencies improperly access or use worker data.
2. **Broaden scope of violations:** Amend the current law to explicitly include violations related to unauthorized access to or misuse of federal data systems, especially where there is a high risk of identity theft, discrimination or other harms
3. **Allow for immediate injunctive relief**: Create an expedited process for obtaining injunctions when sensitive data is at risk.
4. **Remove the "actual damages" requirement**: Currently, individuals must prove "actual damages" to recover, which creates an unreasonable barrier to accountability for privacy violations. Privacy harms are real and often occur at the moment personal data is misused - whether through unauthorized access, sharing or sale. These violations impact a person's dignity, autonomy and sense of security, even if the financial consequences do not appear right away or are hard to measure. Our law should recognize that these injuries are concrete and serious, just like long-standing legal protections against invasions of privacy. People deserve the right to take action when their privacy is violated, regardless of whether they can show a specific dollar amount of harm.
5. **Include punitive damages for willful violations**: For intentional or reckless violations, punitive damages should be available to dissuade violations.
6. **Strengthen whistleblower protections**: The current administration is firing senior government officials responsible for protecting the right of whistleblowers to speak out against this rogue and illegal activity. The Privacy Act should include robust protections for individuals who report potential violations.
7. **Independent privacy oversight body**: Establish an independent federal agency or privacy watchdog tasked with overseeing compliance with the Act and ensuring transparency in how federal agencies handle personal data. This body would have authority to investigate complaints, conduct audits and enforce penalties.

We urge Congress to act swiftly to modernize the Privacy Act to address the realities of modern data collection, processing, and use. The protection of worker privacy is essential to the functioning of our democracy and the preservation of hard-won labor rights.

Respectfully submitted,

AFL-CIO Technology Institute