HARVARD Kennedy School
ASH CENTER
for Democratic Governance
and Innovation
Allen Lab for Democracy Renovation

GETTING-Plurality Research Network
Allen Lab for Democracy Renovation
Ash Center for Democratic Governance and Innovation
Harvard Kennedy School
124 Mount Auburn Street, Suite 200-North
Cambridge, MA 02138

Dear Representative Trahan,

The GETTING-Plurality Research Network housed in the Allen Lab for Democracy Renovation at the Harvard Kennedy School's Ash Center for Democratic Innovation and Governance appreciates the opportunity to respond to your Request for Information to modernize the Privacy Act of 1974, and your leadership on this critical issue.

We have compiled comments from our research community including Sarah Hubbard, Ajeet Singh, Allison Stanger, Anna Lewis, and others from the GETTING-Plurality Research Network. Below, we offer targeted responses to some of the questions you have outlined.

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

One of our biggest concerns is the unprecedented consolidation of sensitive government data, particularly through initiatives such as DOGE which are placing vast government databases under the control of both federal authorities and actors with private commercial interests. The drive for efficiency through centralized data leads inexorably toward systems of control that undermine the very possibility of democratic accountability. This is precisely why our system was designed with inefficiencies and separations–not as bugs, but as essential features that protect democratic governance and human agency.

As we recently highlighted in our guide on Understanding DOGE and Your Data, access to government data should be strictly controlled. If access control, security measures, and maintenance aren't being properly upheld, data leaks and improper use could enable identity theft, financial fraud, targeted harassment or discrimination, a loss of public services and benefits (e.g. social security), or other forms of manipulation. These can lead to real concrete harms for individuals– a loss of public benefits can mean eviction, food insecurity, inability to afford medications– with marginalized populations, who are often targeted by these predatory activities, at risk for disproportionate harm.

We are particularly concerned about two patterns that emerge with centralized data:

- Predatory inclusion: Enhanced surveillance and targeting of individuals based on their politics, speech, ethnic/religious affiliations or consumption of certain contested services.
- Predatory exclusion: Improper removal from forms of economic support (e.g. social security, pension) or challenges to legal rights (e.g. citizenship, visa status) based on consolidated data profiles.

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 artificial intelligence, especially from contracted private vendors and companies, raises major privacy and security concerns, as data governance practices (e.g. training, handling, transparency, proximity to FOIA) may differ significantly from government standards. Government databases offer comprehensive, verified records about the most critical areas of Americans' lives– data which would give any private company significant advantages in training AI systems and setting business strategy. Without proper oversight, this access could lead to private companies, with their own commercial interests, profiting from government data which should belong to the public.

In addition, when AI supplants rather than supplements human decision-making, citizens lose the ability to appeal to human judgment when systems make mistakes. This combination of risks– centralized government data accessible to private AI companies– threatens to create prediction engines of unprecedented power. Such systems could model economic patterns, health outcomes, and infrastructure needs with extraordinary precision, giving their controllers both commercial advantage and political power to target opponents with unprecedented precision.

In the recently published International AI Safety Report, an international body of experts categorized privacy risks into: privacy with respect to AI between training risks (e.g., using data for unintended purposes), handling risks (e.g., the duty to care to protect privacy of data during use), and downstream risks (e.g., how can AI be used to violate privacy from malicious actors). Each of these categories will require different mitigation approaches as the federal government increasingly leverages AI systems.

The modernization of the Privacy Act must address these new realities, and Congress could mitigate these privacy risks through:

- Stronger protections against cross-agency data sharing without appropriate safeguards. This includes closing the "data broker loophole" that currently allows government agencies to purchase sensitive population data without Fourth Amendment protections.

- Improved standards by which vendors are accountable to both the government and impacted communities. Established, clear limits on the use of government data for training by any private vendor.
- Enhanced consent requirements that reflect modern data practices, and meaningful civil remedies when violations occur, including a private right of action.
- Mandated transparency about which decisions are informed by AI systems, and human oversight and appeal mechanisms for all consequential AI decisions.

How can the federal government most effectively leverage privacy-enhancing technologies (PETs)? How can the government share personal information–with other agencies, researchers, states and localities, and other entities–in ways that are effective and privacy-preserving?

The federal government can effectively leverage PETs such as:

- Federated analysis: This method can address the fundamental challenge of data sharing by "transferring the code to the data–providing the technical and legal capability to analyze the data within their secure home environment rather than transferring the data to another institution for analysis." This allows data to remain within its original secure environment with comprehensive audit trails that document every query and analysis.
- Differential privacy: These techniques should be standardized for statistical analyses of sensitive government data, especially when results will be made public. These tools help mitigate against the risk of de-anonymization in large datasets (see recent NIST guidelines).
- Zero-knowledge proofs: These techniques can help verify claims without revealing the underlying data and specific details.

For effective implementation, we would recommend tasking NIST with developing standards for deploying and testing PETs, as well as creating clear governance frameworks for when and how different PETs should be applied based on the data and use cases.

Special Considerations for Biometric Data

We would also strongly recommend that biometric data be recognized as a distinct category which requires heightened protection. While you may be able to change a compromised password, biometric data is non-modifiable–when a fingerprint, retina scan, or genetic data are released and identified, that individual is significantly constrained in their ability to exercise any form of privacy. GDPR (Article 4) defines biometric data as "personal data resulting from specific technical processing relating to the physical, psychological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person." Biometric data should have limitations on collection and retention periods, limitations on use and transfer, and other heightened protections and safeguards.

Should Congress consider requiring that agencies provide individuals a "right to be deleted," in which individuals may request that an agency delete their records? If so, how should providing such a right be balanced against other governmental interests, including promoting national security, improving service delivery, and reducing waste, fraud, and abuse?

Yes, we support the "right to be deleted" and a right to meaningfully contest data. The persistence of incorrect or inaccurate information can have compounding consequences in how the state interacts with and governs individuals. When incorrect data leads to harms (e.g. wrongful exclusion from forms of economic support) individuals should be subject to remedies.

This balance could be created through different mechanisms such as creating different tiers of data with different deletion rights based on government needs, data retention policies, or retaining anonymized data while deleting identifiers.

How can agencies use modern technologies and design methodologies to improve the written consent process?

A key element of consent is to ensure that it is truly informed. Current approaches with lengthy, complex text do not enable meaningful forms of consent. Design approaches to encourage meaningful consent might include:

- Clearly summarize what individuals are consenting to with reasonable, accessible language.
- Shift to opt-in rather than opt-out models, or make opt-out options prominent.
- Create standardized consent forms, perhaps learning from the Common Rule model (which governs human subjects research) and was revised to have a "short form" of consent.

Privacy is a cornerstone of democratic governance and individual agency. Modernizing the Privacy Act of 1974 presents an important opportunity to realign our federal privacy framework to adapt to and leverage modern technologies. Our research network is happy to contribute further expertise or resources in support of this critical effort.

About the GETTING-Plurality Research Network

Governance of Emerging Technology and Tech Innovations for Next-Gen Governance (GETTING-Plurality) is a multi-disciplinary research network linking philosophers, social scientists, computer scientists, legal scholars, and technologists. We are building a unique collaborative that unites technology and policy initiatives at Harvard University with external impact partners across higher education and the tech industry. More information: https://ash.harvard.edu/programs/getting-plurality/

For any additional information on the comments above, please reach out to Sarah Hubbard at sarah_hubbard@hks.harvard.edu.