Congress of the United States
Washington, DC 20515

March 18, 2025

To Whom It May Concern:

Americans' right to privacy, enshrined in our Constitution, is being fundamentally challenged. Unaccountable billionaires, inexperienced programmers, and unvetted political appointees are perpetrating the biggest government privacy scandal since Watergate, when President Nixon weaponized his access to people's personal information to target political opponents ranging from companies to politicians to everyday Americans.

Protecting Americans' privacy has historically been a bipartisan effort that enjoyed broad public support. After President Nixon used his power to access Americans' personal information, Congressional Democrats and Republicans responded by, among other measures, passing the Privacy Act of 1974. Those reformers sought to erect guardrails within which the federal government could deliver its services while upholding Americans' privacy.

I too envision a future in which the government delivers its programs and services in a human-centered, digital-first, and privacy-preserving way. Where Americans know exactly how the information they provide to the government will be used for their benefit. Where the government modernizes by leveraging new technologies like artificial intelligence (AI) to do better by the people it serves. Where entrepreneurial civil servants can innovate while operating transparently for and cooperating productively with Congress and the public. Such a future is possible, but it is not at all what we're witnessing.

In the last six weeks, Americans have watched in horror as unscrupulous state actors breach the computer systems that power dozens of federal agencies and store troves of personal data. These rogue individuals are accessing agency computer systems at an unprecedented pace and scale, with little to no transparency to the American public or Congress. Moreover, their purported motivation for acquiring petabytes of Americans' personal data–to fight waste, fraud, and abuse–could very well shroud a deeper, more sinister undertaking: to build powerful AI systems that, with no human in the loop, perform all sorts of governmental functions from administering health and food benefits, to conducting background checks, to detecting fraud.

In this Orwellian future where AI supplants, rather than supplements, dedicated federal employees, Americans who depend most on government will struggle to find a human to appeal to when they improperly lose Medicaid benefits, are incorrectly denied federal employment or a housing voucher, or are falsely accused of fraud. The Privacy Act, passed at the dawn of the computer age, was supposed to help the government use technology while upholding a key civil liberty. But its gaps are increasingly glaring and demand Congress's attention.

Since the Privacy Act was enacted into law, the federal government's use of information technology has dramatically evolved. Typewriters have been replaced with word processors; file cabinets with databases. To their credit, the authors of the Privacy Act knew that they were writing a law governing norms that

were set to rapidly change. In the bill's enumeration of findings and purposes, lawmakers emphasized that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."

To complement the Privacy Act, Congress enacted key pieces of legislation to govern the federal government's management of electronic information, including the Computer Matching and Privacy Protection Act (CMPPA), the E-Government Act of 2002, the Federal Information Technology and Modernization Act (FISMA), and the Foundations for Evidence-Based Policymaking Act of 2018 to better secure Americans' privacy. Additionally, various Presidents have taken executive actions to improve the government's overall privacy posture, including Executive Order 13719, which established a Federal Privacy Council consisting of the Senior Agency Officials for Privacy (SOAPs) from 25 agencies. All the while, the Privacy Act, the foundational law designed to safeguard Americans' privacy and uphold the principle that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States," has gone untouched.

The combination of challenges stemming from unchecked government officials and significant technological advances warrant a reevaluation of the Privacy Act of 1974 and related laws governing privacy and federal information technology. As I deliberate modernizing these laws, I request feedback from civil society groups, privacy experts, current and recently terminated government technologists, and concerned Americans, including organizations like businesses and nonprofits. I appreciate your responses to the following questions.

1. General questions.

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

    b. How should the federal government balance securing privacy with other priorities, especially promoting security, reducing waste, fraud, and abuse, and improving service delivery (for example, through the use of a public identity verification platform)?

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

    d. How can the federal government most effectively leverage privacy-enhancing technologies (PETs)?

2. Modernizing the Privacy Act of 1974.

    a. Definitions.

        i. How can the Privacy Act's core definitions, including "individual," "record," and "system of records" be modernized to reflect the federal government's current

information management practices? How should these definitions take into account the Office of Management and Budget's incorporation of the term *personally identifiable information* into recent guidance, including OMB Circular A-130?

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

b. Disclosure requirements.

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?

ii. How can the requirements regarding individuals' access to and ability to amend their information be improved? Furthermore, how can agencies' implementation of this requirement be modernized?

iii. 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?

c. Written consent requirement.

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

ii. How can the federal government provide greater transparency to the written consent that individuals have provided to different agencies, about different systems, or for different uses?

iii. Should Congress create greater safeguards to ensure that agencies solicit consent from individuals prior to disclosure? If so, how?

iv. How can Congress balance the need for written consent with efforts to streamline agencies' processes and improve customer experience?

d. Exceptions to the written consent requirement.

i. 5 U.S.C. §552a(b)(1) provides an exception, known as the *need to know* exception, "to those officers and employees of the agency which maintains the record, who have a need for the record in the performance of their duties."

1. Should the *need to know* exception be narrowed, clarified, or otherwise modified? If yes, how?

2. How can Congress improve the transparency around agencies' granting of *need to know* exceptions?

3. Should there be limits on those "officers and employees" who can receive *need to know* exceptions? If so, should this access differ by type of federal employee (for example, political appointees vs. civil servants)? Furthermore, should access differ by the relative risk or scope of a particular system of records?

ii. 5 U.S.C. §552a(b)(3) provides an exception for an established routine use identified in the system of records notice (SORN) that has been published in the *Federal Register*."

1. Should the definition of "routine use" as "a purpose which is compatible with the purpose for which [the information] was collected" be narrowed, clarified, or otherwise modified? If yes, how?

2. Is the information included in the SORN, and the medium of publication via the *Federal Register*, sufficiently effective to notify individuals about the use of their information? Could the SORN and the process by which it is made public be improved?

e. Data sharing between agencies and with third-parties (including researchers).

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?

ii. 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?

iii. Should Congress consider imposing restrictions on *intra*-agency data sharing? If so, how?

f. Civil remedies.

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

g. Privacy leadership, innovation, and oversight.

i. What role should the Office of Management and Budget (OMB), especially its Office of E-Government & Information Technology and Office of Information and Regulatory Affairs (OIRA), play in promoting privacy across the federal government, including through standards-setting?

ii. What role should the National Institute of Standards and Technology (NIST) play in developing technical guidance, frameworks, benchmarks, and tools for agencies to improve their privacy practices?

iii. What role should agency Chief Information Officers (CIOs) play in promoting privacy at agencies? What role should Senior Agency Officials for Privacy (SOAPs) play? How should these two officials work together?

iv. What role should independent officials, councils, and boards–including Inspectors General, the Federal Privacy Council, and the Privacy and Civil Liberties Oversight Board–play in overseeing the federal government's privacy practices?

3. How can related laws, including but not limited to the Computer Matching and Privacy Protection Act (CMPPA), the E-Government Act of 2002, and the Federal Information Technology and Modernization Act (FISMA), and the Foundations for Evidence-Based Policymaking Act of 2018 be similarly modernized to better secure Americans' privacy?

Detailed answers to the questions above will help inform my efforts to secure Americans' privacy from abuse by the federal government. Please send responses to PrivacyActRFI@mail.house.gov by April 30th, 2025. I look forward to reviewing your submissions.

Sincerely,

Lori Trahan
Member of Congress