Privacy, Trust, and Effective Government

A Bipartisan Blueprint for Modernizing the Privacy Act

PREPARED BY THE OFFICE OF
CONGRESSWOMAN LORI TRAHAN

FEBRUARY 2026

TABLE OF CONTENTS

I. Foreword

Dear Reader:

In March 2025, I set out to reform the Privacy Act of 1974. Like other Americans, I was horrified by the brazen violations to our privacy perpetrated in the name of combatting waste, fraud, and abuse and modernizing information technology systems. Unvetted political appointees were gaining access to, and—as whistleblowers bravely revealed—exfiltrating, reams of Americans' personal data with impunity. These efforts jeopardized individual privacy and elevated cybersecurity risks to critical government systems; exhaustive Congressional investigations are surely in order.

But as the months dragged on, another front opened in the fight to secure Americans' privacy: immigration enforcement. My office releases *Privacy, Trust, and Effective Government: A Bipartisan Blueprint for Modernizing the Privacy Act* against the backdrop of our government deploying citizen-facing technologies like facial recognition and social media scanning that record First Amendment-protected activity while, on the back end, merging that data with information held by civilian agencies like the Internal Revenue Service, Social Security Administration, and Centers for Medicare and Medicaid Services.

Fifty years ago, Congress attempted to forestall such un-American surveillance. In the wake of the Watergate and COINTELPRO scandals and at the dawn of the computer age, Congress enacted the Privacy Act of 1974 to protect Americans' privacy while balancing the informational needs of federal agencies. The Privacy Act was unprecedented, and therefore influential: it served as the inspiration for many international privacy laws and standards in the decades that followed.

But for all of their prescience, the Privacy Act's authors did not, and could not, design a law capable of handling transformational technologies like artificial intelligence. Nor could they have accounted for the aggrandizing nature of the modern imperial presidency.

For these reasons and more, Congress must modernize the Privacy Act. The enclosed recommendations are designed to drive a bipartisan, bicameral conversation about such a reform effort meaningfully forward into the 120th Congress. They are deliberately ambitious yet cognizant of what's technically feasible. I'm grateful to my staff, especially Dylan Irlbeck, who worked diligently over the past year to produce them.

But this report is not just about privacy. Beneath its surface lie two distinct arguments. The first, in the realm of the separation of powers, advances a richer account of the proper relationship between the legislative and executive branches, a problem that transcends privacy and outlasts any single official, agency, or administration. The second offers a template for government reform centered on right-sizing bureaucracy—not dismantling it.

Massive changes to the administration of government are underway, norms are being shattered, and longstanding institutional arrangements are under strain. Renewing America's democratic structures will necessitate a more agentic and capacious Congress, and a more accountable and

transparent Executive. At the same time, Congress cannot afford to simply institute new checks and balances, but must also commit to efficacy: that is, government must deliver on its promises.

It is in this mindset—restoring trust in government by revitalizing Article I and transforming implementation—that my office drafted this report. Privacy Act reform is both a defensive measure against abuse and an offensive strategy to engender good government, regardless of which party controls the White House. Congress should not squander its opportunity or ignore its charge.

Lori Trahan
Member of Congress

II. Executive summary

> The Congress finds that… the right to privacy is a personal and fundamental right protected by the Constitution of the United States.
>
> *—The Privacy Act of 1974, Public Law 93-579*

> The protection of personal privacy is no easy task. It will require foresight and the ability to forecast the possible trends in information technology and the information policies of our Government… We must act now to create safeguards against the present and potential abuse of information about people.
>
> *—Senator Sam Ervin, Introductory Remarks on the Privacy Act*

> Recounting the insights of members of the 93rd and 94th Congresses should embolden us. Their concerns clarify the headwinds that reformers face… Revisiting this history should remind the public that totalizing surveillance is neither acceptable nor desirable. Privacy can and should be ours.
>
> *—Danielle K. Citron, A More Perfect Privacy*

The elusiveness of privacy has not daunted generations of Framers, justices, scholars, legislators, and everyday Americans in their quest to protect it.

The U.S. Constitution secured the people's right against unwarranted search and seizure. Louis Brandeis, enterprising lawyer and future Supreme Court justice, cohered common law, inspired the privacy torts, and animated constitutional privacy doctrine in his influential 1890 article "The Right to Privacy." Nearly a century later, against the backdrop of nascent computing technologies, Professor Alan Westin proffered an encompassing definition of privacy in *Privacy and Freedom* as the claim of individuals (and groups, and institutions) to determine for themselves when, how, and to what extent information about them is communicated to others; for his efforts—which included serving as special consultant to the Senate Government Operations Committee chaired by Senator Sam Ervin—Westin earned a spot in the Congressional Record. Reading Westin's name aloud on the Senate floor, Sen. Ervin credited him among those who worked assiduously to reconcile the Senate's Privacy Act draft with the House's amendments. Those efforts bore fruit: on December 31st, 1974, in the waning hours of the 93rd Congress, President Gerald Ford signed the Privacy Act into law.

By the end of 1974, Congress had located the right to privacy in the Constitution and accorded statutory protections to it; that is, in the context of record-keeping by the federal government. Plenty of privacy problems remained unresolved. The Privacy Act was riddled with exceptions and exemptions for law and immigration enforcement. Over in the commercial sector, the processing of consumer information continued unregulated: while the original Privacy Act would have also covered "private data banks," thus assuming the role of a consumer privacy standard, it was ultimately cabined to "[federal] governmental organizations."

Over fifty years later, privacy pessimism, cynicism, and fatalism predominate. The Congress of today hardly resembles its ancestor, the one that galvanized to protect privacy in an overwhelmingly bipartisan fashion. And while lawmakers and advocates alike dither over comprehensive consumer privacy legislation that patiently awaits its political moment, administration after administration erodes the spirit and tramples the letter of the Privacy Act.

Congress alone can act. Governmental privacy, manifested most foundationally in the Privacy Act of 1974, demands as much—if not more—attention than commercial privacy. Actions by the current administration, particularly in immigration enforcement, underscore the need for Congress to take such a position.

Ascertaining the problems of a law as old as the Privacy Act is challenging. It is ensconced throughout government, and many who are familiar with the law are unable or unwilling to see its shortcomings. But the Privacy Act of 1974 is doubtless failing: the protections it ostensibly affords to individuals do not account for emerging technology or expanding executive power, and its outmoded regulatory framework hamstrings good, effective, and accountable governance.

Recent events have exposed deep vulnerabilities in a law written at the dawn of the computer age, from unauthorized data exfiltration at the Department of Treasury and the Social Security Administration to sprawling surveillance activities at the Department of Homeland Security. These incidents reflect fundamental flaws in how the Privacy Act defines its scope, structures its requirements, and enforces its protections. The Act's system-centric model flattens the distinction between a personnel database and an investigative system. Its consent-based approach to disclosure has devolved into a procedural checkbox that is easily skirted. Its exemptions and exception have been stretched beyond recognition.

Meanwhile, agencies administering critical programs face a paradox: the Act's uniform requirements make low-risk data use needlessly difficult, while those uses of high-risk avoid adequate scrutiny. Civil servants seeking to reduce administrative burden confront an onerous compliance regime replete with kludge. But the fact that the Act applies its requirements indiscriminately is not just operationally ruinous: it is ineffective for privacy. By splintering the focus of watchdogs, the Act pulls attention away from data processing that warrants the most oversight.

This report charts a path forward. Drawing from responses to Congresswoman Trahan's Privacy Act RFI, government reports produced through the decades, ongoing litigation against the government, previous legislation from both houses of Congress, and technical expertise from across civil society and industry, these recommendations reflect a simple aim: to make responsible data processing easier and irresponsible data processing impossible.

Specifically, this report recommends that Congress, with respect to the Privacy Act:

A. **Modernize definitions** to cover more individuals, data, and systems—setting up a shift from system-centric to purpose-centric regulation.

B. **Segment requirements by harm and risk of purpose** rather than enforcing homogenous rules against all forms of data processing.

C. **Right-size requirements** through robust data minimization, elimination of executive order-based purpose authorization, and special protections for high-risk processing.

D. **Regulate agencies' use of commercially available information** through a standardized authorization framework modeled on FedRAMP, bringing transparency and quality control to a sprawling and opaque practice.

E. **Standardize and narrow exceptions** by redesigning the framework around excepted purposes, eliminating the "need-to-know" and "routine use" exceptions that have enabled systematic abuse.

F. **Consolidate transparency measures** into a living, machine-readable public inventory that combines System of Records Notices, matching agreements, and Privacy Impact Assessments.

G. **Adopt privacy-enhancing technologies and techniques** to technically enforce governance reforms while retaining data utility.

H. **Enhance enforcement** by recognizing nonpecuniary privacy harms, authorizing equitable relief and increasing criminal penalties.

I. **Collocate privacy oversight in the legislative** branch, endowing a novel investigative entity with special authority to view telemetry from agency systems and dynamically inspect high-risk data processing.

J. **Resource Chief Privacy Officers** who report directly to agency heads, with the authority and capacity to run privacy programs and interface with Congress and the public.

III. Background

A. The Privacy Act

The Privacy Act of 1974 (hereafter "the Privacy Act" or "the Act") was a landmark piece of legislation that established safeguards governing federal agencies' collection, maintenance, use, and dissemination of Americans' personal information. It is codified at 5 U.S.C. § 552a.

The Act was born in the Department of Health, Education and Welfare's (HEW) Advisory Committee on Automated Personal Data Systems.[1] In its 1973 report *Records, Computers and the Rights of Citizens*, the Advisory Committee proposed a set of Fair Information Practices (FIPs) for automated personal data systems and recommended specific protections for administrative personal data systems, arguing *inter alia* that the concept of privacy needed to be reimagined to recognize the mutual interests that institutions and individuals shared in the fair and appropriate management of personal information.

Though the Privacy Act's intellectual groundwork was laid by the Advisory Committee, two developments created its political impetus. First, throughout the 1960s and early 1970s, a series of scandals revealed illegal surveillance of political opponents and citizens deemed subversive by the state, most notably the Counterintelligence Program (COINTELPRO) and the Watergate affair. Second, computers—particularly mainframes that filled several rooms and required dozens of staff to operate—were rapidly permeating industry and government, raising concerns about the scale and speed at which personal information could be processed.

Equipped with both a policy framework and political momentum, Congressional leaders managed to pass the Privacy Act at the very end of the 93rd Congress. The Act drew heavily from the Advisory Committee's FIPs; Congress hoped that codifying these practices would rebuild trust between Americans and their government. Furthermore, the legislation's authors stressed that computers and sophisticated information technology amplified the potential harms from collecting, maintaining, using, or sharing personal information. Yet despite the prominent role that computers played in driving the Act's passage, the law was still primarily designed around the file cabinet—a key reason it has become so outdated, as this report will show.

In the decades following the Privacy Act, Congress enacted key 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 Security Modernization Act (FISMA), the Judicial Redress Act of 2015, and the Foundations for Evidence-Based Policymaking Act of 2018. Several Presidents worked in parallel, taking executive action to improve the government's privacy posture, including Executive Order 13719, which established a Federal Privacy Council consisting of the Senior Agency Officials for Privacy from twenty-five agencies. Throughout this period, the Privacy Act—the foundational law designed to safeguard Americans' privacy and uphold Congress's belief that "the right to

[1] The Department of Health, Education, and Welfare was created in 1953 and effectively ceased to exist in 1979, when Congress split off its education functions into the Department of Education and retitled the remainder as the Department of Health and Human Services.

privacy is a personal and fundamental right protected by the Constitution of the United States"—has not undergone structural reform.

B. Congresswoman Trahan's focus on privacy reform

Congresswoman Trahan's efforts to reform the Privacy Act of 1974 combine legislative modernization with sustained oversight of the executive branch. In many ways, the motivations for her effort—widespread abuses by the executive and massive advances in information technology—parallel those which animated the Privacy Act's sponsors.

In March 2025, she issued a Request for Information (RFI) to modernize the Privacy Act of 1974 in which she wrote:

> 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.[2]

In response to her RFI, Rep. Trahan received dozens of responses from former government technology officials, watchdogs, good government groups, technology companies, privacy advocates, and individual citizens.

While processing the extensive feedback she received from her RFI, Representative Trahan exercised her oversight prerogative by investigating the Trump Administration's handling of Americans' personal information, and in particular its Department of Government Efficiency (DOGE).

- In April 2025, she requested that two Inspectors General investigate the potential illegal disclosure of sensitive taxpayer information by a DOGE staffer to officials at the General Services Administration, citing a likely violation of the Privacy Act.[3]

- In May 2025, she demanded answers from the National Labor Relations Board regarding whistleblower allegations that DOGE engineers accessed and illegally exfiltrated multiple gigabytes of sensitive data, raising concerns about violations of the Privacy Act and the FISMA.[4]

---

[2] Letter from Lori Trahan, Member, U.S. House of Representatives, Request for Information on Modernizing the Privacy Act of 1974 (Mar. 18, 2025), https://trahan.house.gov/uploadedfiles/final_trahan_privacyactrfi.pdf.

[3] Letter from Lori Trahan, Shontel M. Brown & Suzan K. DelBene, Members, U.S. House of Representatives, to Loren Sciurba, Deputy Inspector Gen., Treasury Office of Inspector Gen., & Robert C. Erickson, Deputy Inspector Gen., GSA Office of Inspector Gen. (Apr. 3, 2025), https://trahan.house.gov/uploadedfiles/trahan_treasury_gsa_oig_letter_doge_spreadsheet_v2.0.pdf.

[4] Letter from Lori Trahan & Gerald E. Connolly, Members, U.S. House of Representatives, to Marvin E. Kaplan, Chairman, Nat'l Labor Relations Bd. (May 1, 2025),

- In June 2025, she sought clarity from the United States Department of Agriculture regarding its consolidation of sensitive personal data from applicants to and recipients of the Supplemental Nutrition Assistance Program, warning that the effort risked violating the Privacy Act and eroding public trust.[5] At a House Oversight and Government Reform committee hearing later that month, she called attention to the executive branch's escalating consolidation of government data and warned that it could create the machinery of a surveillance state, ripe for abuse by either political party.[6]

- In July 2025, she urged the Department of Interior to revoke DOGE officials' unfettered access to critical systems, including the Federal Personnel and Payroll System, citing security, operational, and legal risks, including potential criminal violations of the Privacy Act.[7]

Representative Trahan has also spearheaded important efforts to protect consumer privacy through her seat on the House Energy & Commerce Committee. Those efforts include her DELETE Act to allow consumers to request deletion of their data from data brokers, as well as her TLDR Act to require clear, summary disclosures of complex terms-of-service contracts with online companies.[8] These bills reflect her larger commitment to passing a comprehensive federal consumer privacy standard.

C. Fair Information Practices

One explanatory framework for Privacy Act reform is modernizing the federal government's implementation of the FIPs. As noted earlier, the FIPs were first proposed in the HEW Advisory Committee's final report and soon became the theoretical foundation for the Privacy Act. In 1984, the Organisation for Economic Cooperation and Development substantively revised the FIPs; their formulation is now the most widely cited version.[9]

While the FIPs and their many manifestations have been largely resilient to advances in modern technology and data practices, the Privacy Act has not. This is to be expected: the FIPs are

---

https://trahan.house.gov/uploadedfiles/final_nlrb_privacyact_fisma_violations_trahan_connolly.pdf.

[5] Letter from Lori Trahan, Angie Craig, Jahana Hayes, Shontel M. Brown, James P. McGovern et al., Members, U.S. House of Representatives, to Brooke Rollins, Sec'y of Agric., U.S. Dep't of Agric. (June 18, 2025), https://trahan.house.gov/uploadedfiles/trahan_craig_hayes_brown_mcgovern_usda_letter_data_final.pdf.

[6] Press Release, Lori Trahan, Member, U.S. House of Representatives, *Trahan Rips Trump's Plan to Let Palantir Build Dossiers on American Citizens* (June 6, 2025), https://trahan.house.gov/news/documentsingle.aspx?DocumentID=3596.

[7] Letter from Lori Trahan & Jared Huffman, Members, U.S. House of Representatives, to Doug Burgum, Sec'y of the Interior, U.S. Dep't of the Interior (July 9, 2025), https://trahan.house.gov/uploadedfiles/trahan_huffman_letter_to_doi_privacy_1.pdf.

[8] Data Elimination and Limiting Extensive Tracking and Exchange Act (DELETE Act), H.R. 2612, 119th Cong. (2025); Terms-of-service Labeling, Design, and Readability Act (TLDR Act), H.R. 2019, 119th Cong. (2025).

[9] Gellman, Robert, *FAIR INFORMATION PRACTICES: A Basic History* (July 28, 2025), https://ssrn.com/abstract=5348107.

theoretical principles; the Privacy Act is law, an implementation of those principles for a particular jurisdiction at a specific moment in time.

In 2008, the Privacy Office at the Department of Homeland Security issued its own version of the FIPs titled, perhaps confusingly, the Fair Information Practice *Principles* (FIPPs, emphasis added). Many federal agencies and bodies subsequently adopted this new construction, including the Office of Management and Budget and the Federal Privacy Council.

To illustrate how the reforms described in this report would achieve the objective of modernizing the federal government's implementation of the FIPs, each recommendation enclosed herein are mapped to one or more of the FIPPs as promulgated by OMB in Circular A-130. (This report uses the identifier "FIPs" for historical consistency, but the practices outlined in the chart below and referenced throughout section III correspond to the DHS FIPPs.)

Fair Information Practice	**Description**
Access & Amendment	Agencies should provide individuals with appropriate access to personally identifiable information (PII) and appropriate opportunity to correct or amend PII.
Accountability	Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.
Authority	Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.
Minimization	Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.
Quality & Integrity	Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
Individual participation	Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries

Purpose Specification and Use Limitation	Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
Security	Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
Transparency	Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

D. Scope, state capacity, and sources

Scope

This report nominally concerns the Privacy Act of 1974, which is codified within Title 5 of the U.S. Code: an organizational, administrative, and procedural title. That said, many of its recommendations may in fact relate to or be implemented in other areas of the U.S. Code. For instance, Title 44 houses federal information policy as well as the management and promotion of electronic government services. For ease of discussion, this report references the Privacy Act as a catch-all term for each recommendation it offers related to federal privacy.

It is also worth clarifying that this report chiefly concerns civilian agencies that administer federal programs. As such, the reforms proposed address those agencies' use of administrative and statistical data for statutorily authorized purposes. This report does not attempt to resolve, at least directly, specialized privacy issues in the national security, law enforcement, or intelligence community contexts. There are intersections, of course: law enforcement (including immigration enforcement) routinely request data maintained by civilian agencies to conduct investigations, interactions that are generally mediated by the Privacy Act, often through exemptions and exceptions.

On state capacity

Each recommendation in this report requires a critical caveat: adequate capacity is essential for implementation. A government reform effort of this magnitude by definition will require significant resources. An unfunded mandate is an unimplementable mandate. This report elides a formal recommendation for appropriations, but one can imagine it as the substrate atop which each of the recommendations is built.

But capacity is not simply a question about funding. Capacity is also a function of personnel and procedure. The conditions for Privacy Act reform must as a whole be conducive to success.

Government will also need to look at, among other aspects, how it brings in and retains talent (e.g. technologists) and clears away procedural kludge to allow a revised Privacy Act to flourish.[10]

Sources

This report stands on sturdy shoulders. Dozens of responses to Rep. Trahan's RFI from civil liberties groups, former federal officials, private sector organizations, and everyday Americans animate the enclosed recommendations. Additionally, the report draws significantly from many authoritative reports, memoranda, and bills that each advanced the discussion on Privacy Act reform. Staff are indebted to the authors of these products across years and across Congresses for their effort, profundity, and prescience.

Several of these sources are so heavily relied on, so frequently referenced, or otherwise so undergird the report that they warrant special identification:

- **The Department of Health, Education, and Welfare (HEW) Advisory Committee's report:** As previously mentioned, the HEW Secretary's Advisory Committee on Automated Personal Data Systems, chaired by influential computer scientist Willis Ware, proposed in *Records, Computers and the Rights of Citizens*, its final report, the Fair Information Practices to address privacy risks from the increasing use of automated data systems. Through their FIPs, the Advisory Committee supplied the intellectual framework for the Privacy Act and, in fact, many international privacy laws.[11]
- **The Privacy Protection Study Commission's (PPSC) final report, specifically Appendix 4: *The Privacy Act of 1974: An Assessment*:** Established by the Privacy Act to assess its effectiveness, the PPSC in its final report concluded, among its other insights, that the Act needed significant modification and proffered to Congress many recommendations for reform that have since gone unimplemented. The PPSC's final report is largely forgotten today.[12]
- **Legislative History of the Privacy Act of 1974:** Published in 1976 as a joint committee print by the Senate and House Committees on Government Operations, the "source book on the Privacy Act of 1974" compiles the entire legislative history of the Act, including markups, reports, and the various stages of the legislation.[13]
- **The Department of Justice's (DOJ's) Overview of the Privacy Act of 1974, 2020 Edition:** Last updated in 2020 and currently maintained in online form, the DOJ's

[10] Steven M. Teles, *Kludgeocracy in America*, 17 Nat'l Aff. (2013), https://www.nationalaffairs.com/publications/detail/kludgeocracy-in-america.

[11] Department of Health, Education & Welfare (HEW), *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, DHEW Publication No. (OS) 73-94 (July 1973) [hereinafter HEW Report], https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[12] U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977) [hereinafter Privacy Commission Report], https://archive.epic.org/privacy/ppsc1977report/.

[13] S. Comm. on Gov't. Operations & H.R. Comm. on Gov't. Operations, 94th Cong., *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy* (Comm. Print 1976) [hereinafter Privacy Source Book], https://www.justice.gov/opcl/paoverview_sourcebook.

Overview of the Privacy Act pairs discussion of the Act's provisions with relevant case law. It is periodically updated by the DOJ's Office of Privacy and Civil Liberties.[14]

- **Sen. Wyden's *Privacy Act Modernization Act of 2025*, 119th Congress[15] and Sen. Akaka's *Privacy Act Modernization for the Information Age Act of 2011*, 112th Congress[16]:** Sens. Wyden and Akaka made important strides with their bills, manifesting in legislative text ideas including updated definitions, increased enforcement, and enhanced privacy leadership. Any successful Privacy Act rewrite will invariably incorporate parts or all of their proposals.
- **The Congressional Research Service's (CRS) Privacy Act overview:** CRS analyst Meghan Stuessy wrote "The Privacy Act of 1974: Overview and Issues for Congress," a comprehensive yet succinct primer on the Privacy Act that staff frequently referenced over the course of drafting this report.[17]
- **Robert Gellman's Privacy Act report**: Privacy Act expert and longtime Congressional staffer Robert Gellman attempted in his personal capacity a substantial rewrite of the Act. In his 2021 report, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974*, Gellman proposed a draft bill to replace the existing Privacy Act. His ideas were tremendously influential on this report.[18]

E. Acknowledgements

Many individuals and groups provided in-depth responses to Rep. Trahan's Privacy Act RFI and/or offered thoughtful feedback on draft versions of this report. Staff are particularly thankful to Robert Gellman; Matthew Spence; Lacey Strahm; Matthew Cornelius; Jake Pasner; Sydney Saubestre; Alex Prokop; Dave Liesse; the Electronic Privacy and Information Center (EPIC); the Federation of American Scientists (FAS); the World Privacy Forum (WPF); the Association of Public Data Users (ADPU); the Gen-Z Emerging Technology Action (ZETA); Accountable Tech; Asian Americans Advancing Justice | AAJC; the International Federation of Professional and Technical Engineers (IFPTE); the Census Quality Reinforcement Task Force at the National Conference on Citizenship; the Allen Lab for Democracy Renovation, Ash Center, Harvard Kennedy School; the American Statistical Association (ASA); Data Quality Campaign; the Center for American Progress (CAP); the Center for Democracy and Technology (CDT); the Leadership Conference on Civil and Human Rights; the Data Foundation; the Open Technology

[14] U.S. Dep't of Justice, *Overview of the Privacy Act of 1974*, (2020 ed.) [hereinafter DOJ Overview], https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition.

[15] Privacy Act Modernization Act of 2025, S. 1208, 119th Cong. (2025) [hereinafter Wyden Bill].

[16] Privacy Act Modernization for the Information Age Act of 2011, S. 1732, 112th Cong. (2011) [hereinafter Akaka Bill].

[17] Meghan M. Stuessy, *The Privacy Act of 1974: Overview and Issues for Congress* (Dec. 7, 2023), https://www.everycrsreport.com/reports/R47863.html.

[18] Gellman, Robert, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974* (May 12, 2021) [hereinafter Gellman Report], https://ssrn.com/abstract=3844965.

Institute (OTI) at New America; the Surveillance Technology Oversight Project (STOP); the Partnership for Public Service (PPS); Palantir Technologies; and Enveil for their contributions.

IV. Recommendations

A. Modernize definitions

Recommendation
Congress should update the Privacy Act's core definitions–especially "individual," "record," "system of records," and "matching program"–to cover more individuals, data, systems, and disclosures. A successful definitional modernization would lay the groundwork for a fresh privacy model that is purpose-centric rather than system-centric, as discussed in the following subsections.

FIP(s)
Minimization, Individual Participation

Discussion
Congress's highest priority with respect to Privacy Act reform is transforming the law's system-centric privacy model into one that is purpose-centric, in which requirements are logically tethered to and segmented by the harm and risk of the statutory purpose for which an agency must process personally identifiable information (PII).[19] Moreover, this new model ought to be data-agnostic, applying its requirements to any PII that an agency processes pursuant to a statutory purpose. Such a dramatic shift necessitates antecedent changes to at least four of the Act's definition, namely (1) "individual," (2) "record," (3) "system of records," and (4) "matching program."

The Privacy Act defines "individual" as:

> A citizen of the United States or an alien lawfully admitted for permanent residence.[20]

This definition excludes a significant number of non-citizens from the Act's baseline protections and rights, even though federal agencies process data on those individuals. Additionally, the definition excludes organizations—think state governments, non-profits, and corporations—about whom the federal government processes sensitive information like trade secrets or financial data.

Recent Congressional and international efforts to enact comprehensive consumer privacy have generally adopted syntactically simpler, yet more conceptually expansive, definitions for individuals covered by the law: natural persons. For instance, the American Privacy Rights Act (APRA), a bipartisan bill introduced in the 118th Congress, defines individual as "a natural

[19] In this report, "statutory purpose," refers to (1) purposes explicitly authorized by statute (for example, specifying the data elements involved, the operations involving such data, etc.) and (2) purposes reasonably inferred by statute (that is, a purpose flowing from, for example, the authorization of a new program or initiative). For category (2), Congress would likely need to devise a consistency test with which agencies could evaluate an agency's asserted, implied processing purpose against a particular statutory authorization in the spirit of an old recommendation from the Privacy Protection Study Commission.

[20] 5 U.S.C. § 552a(a)(2).

person residing in the United States."[21] In the European Union, the General Data Protection Regulation goes marginally further, granting privacy protections to a "natural person," eschewing APRA's residency requirement.[22]

Congress should redefine "individual" to include all natural persons whose data is processed by the federal government, ensuring foreign nationals are extended privacy rights and protections by the Act. Conveniently, this update would automatically obviate the Judicial Redress Act of 2015 which extended certain rights of judicial redress established under the Privacy Act to citizens of some foreign countries and regional economic organizations.[23]

The Privacy Act defines "record" as:

> Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.[24]

In effect, this definition cabins the range of personal information held by an agency that is subject to the Privacy Act to strictly identifying information ("information about an individual… that contains… [an] identifying particular assigned to the individual"). By constructing its core informational term in this manner, the Act does not directly contemplate linkable data or the resulting "mosaic effect," wherein de-identified information, when combined with other, possibly identifying information, may present emergent privacy risks.[25] But even setting aside the definition's shortcoming vis-à-vis linkability, its inherent ambiguity has led to differing court interpretations about its exact scope.

There are at least three such interpretations worth highlighting. The Second, Third, and Fourth Circuits construe a broad definition, encompassing any information linked to an individual through an identifying particular, such as a name, address, or even a voice or picture on a tape, even if it doesn't reveal a personal trait. In contrast, the Ninth and Eleventh Circuits apply a

---

[21] American Privacy Rights Act of 2024, H.R.8818, 118th Cong. (2024).

[22] Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[23] Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282.

[24] 5 U.S.C. § 552a(a)(4).

[25] OMB Memorandum M-13-13, *Open Data Policy—Managing Information as an Asset* (May 9, 2013), obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf ("The mosaic effect occurs when the information in an individual dataset, in isolation, may not pose a risk of identifying an individual (or threatening some other important interest such as security), but when combined with other available information, could pose such risk. Before disclosing potential PII or other potentially sensitive information, agencies must consider other publicly available data - in any medium and from any source- to determine whether some combination of existing data and the data intended to be publicly released could allow for the identification of an individual or pose another security concern.").

stricter standard, requiring that the information "must reflect some quality or characteristic" of the specific individual involved rather than just being generally associated with them. Staking out a middle ground, and arguably hewing most closely to the spirit of the statute, the D.C. and Fifth Circuits require that information both include an identifying particular and be "about" the individual, though it need not necessarily reflect a specific quality or characteristic. For example, in *Tobey v. NLRB,* the D.C. Circuit ruled that a case-tracking system containing a field examiner's initials was not a record about the examiner since the files themselves were "about" the cases, not the person.[26]

Guidance from the Office of Management and Budget (OMB) has offered a more expansive definition for the concept of personal information that underlies the "record" statutory term. For example, OMB Circular A-130 directly employs "personally identifiable information," or PII, defining it as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[27] This definition contemplates the mosaic effect in a way the Privacy Act, with its focus on "identifying particulars," does not.

Members of Congress have lately been opting for similar definitions when scoping the data covered by their privacy laws. For example, APRA is directionally aligned with OMB, but goes slightly further by contemplating the linkability of data about devices. Specifically, APRA scopes its covered data as "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals."[28]

To modernize "record," Congress should first codify OMB's long-standing definition of PII while considering, as APRA does, whether to expressly include device-linked data. Subsequently, it should tether "record" exclusively to its new "PII" term. Senator Wyden's Privacy Act Modernization Act of 2025, in which he defined "personally identifiable information" roughly the same as APRA and tied "record" to it, illustrates one way Congress could operationalize this approach:

> (4) the term 'record' means any personally identifiable information processed by an agency;
>
> …
>
> (14) the term 'personally identifiable information' means any information that identifies, or is linked or reasonably linkable, alone or in combination with other data, to—
>
> (A) an individual; or

[26] DOJ Overview, *supra* note 14.

[27] OMB Circular A-130, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[28] American Privacy Rights Act of 2024, H.R.8818, 118th Cong. (2024).

> (B) a device that identifies, or is linked or reasonably linkable to, an individual.[29]

The Privacy Act defines "system of records" as:

> A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.[30]

"System of records" is arguably the most consequential definition in the Privacy Act. The Act's disclosure requirements and transparency obligations, including agencies' publication of system metadata in the *Federal Register*, activate only when an information system qualifies as a "system of records." However, this definition is imperfect, reflecting an archaic, manual model of information processing.

Crucially, "system of records" turns on the method by which an agency accesses records, rather than the mere maintenance of such records. That is, an information system is only considered a "system of records"—and therefore subject to an important subset of the Privacy Act's requirements—if agency officials retrieve information by either a name or identifying particular. This retrieval-based definition creates significant gaps in contemporary practice. For instance, it permits agencies to avoid the Act's requirements by searching systems using non-identifiers, despite the fact such a query could very well turn up identified records.

The Privacy Protection Study Commission recognized this gap of "attribute searches" in its final report, citing an example wherein the Veterans Administration "produced lists of names for another agency by using psychiatric diagnosis, age, and several other personal attributes as the search keys."[31] As constructed, "system of records" also fails to account for novel retrieval methods such as natural language queries, the predominant input to large language model-based AI systems.

Courts have also limited the "system of records" scope in other interesting ways, writing, for instance, that "it is not sufficient that an agency has the *capability* to retrieve information indexed under a person's name, but the agency must in fact retrieve records in this way in order for a system of records to exist" (emphasis added).[32]

---

[29] Wyden Bill, *supra note* 15.

[30] 5 U.S.C. § 552a(a)(5).

[31] Privacy Commission Report, *supra note* 12 at Appendix 4.

[32] Henke v. Commerce, 83 F.3d 1453, 1460 n.12 (D.C. Cir. 1996); see also Elec. Privacy Info. Ctr. v. DHS, 653 F.3d 1, 8 (D.C. Cir. 2011) ("Even if . . . the [agency] has the ability to combine various sources of information and then to link names to the images produced using [advanced imaging technology], [the petitioners'] Privacy Act claim still fails because they offer no reason to believe the [agency] has in fact done that." (citing Henke)); Chang v. Navy, 314 F. Supp. 2d 35, 41 (D.D.C. 2004) ("[A]n agency's failure to acknowledge that it maintains a system of records will not protect the agency from statutory consequences if there is evidence that the agency in practice retrieves information about individuals by their names or personal identifiers. . . . [H]owever, mere retrievability – that is, the capability to retrieve – is not enough.").

Congress should ensure that the Privacy Act's requirements apply to all PII processed by an agency pursuant to a statutory purpose. In such a data-agnostic world, the very notion of a system of records would become obsolete, and the definition could likely be removed entirely. The merits of such an update will become even clearer in sections III.B and III.C of this report.

Finally, the Privacy Act defines "matching program" as the following:

> (8) the term "matching program"—
>
> (A) means any computerized comparison of—
>
> (i) two or more automated systems of records or a system of records with non-Federal records for the purpose of—
>
> (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or
>
> (II) recouping payments or delinquent debts under such Federal benefit programs, or
>
> (ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records…[33]

The definition goes on to expressly exclude several types of computer matches including, for instance, "matches performed to produce aggregate statistical data without any personal identifiers."[34]

A product of the Computer Matching and Privacy Protection Act of 1988, which was enacted to provide enhanced privacy and due process protections for select computerized data comparison activities, the term "matching program" captures that subset of data sharing employed to administer federal benefits programs, effectuate improper payments monitoring and debt collection, and facilitate federal personnel and payroll processing.

Congress should look to generalize the definition of "matching program" to ensure all forms of record disclosure (matching, correlation, inference, sharing, etc.) within its current programmatic scope are covered, not just "computerized comparisons."

B. Segment requirements by harm and risk of purpose

[33] 5 U.S.C. § 552a(a)(8).

[34] 5 U.S.C. § 552a(a)(8)(B).

Recommendation
With modernized definitions in place, Congress must embed in the Privacy Act a new privacy model that segments requirements by the relative harm and risk of each purpose. The Act's current approach, of homogenous requirements at the system-of-records-level, has resulted in limited privacy for individual Americans while hindering agencies—especially those who administer critical safety net programs—from processing data responsibly.

FIP(s)
Authority, Minimization, Security

Discussion
In the previous subsection, this report recommended that Congress modernize the Act's core definitions, especially "system of records." Doing so will furnish definitional blocks which Congress must use to rebuild the Privacy Act's privacy model, situating purpose at the foundation.

If the Privacy Act's definitions have unduly confined its scope, its privacy model—which can be characterized as system-centric, consent-driven, and exceptions-ridden—has unduly confined its efficacy.

The central regulatory unit of the Act is the system of records. A regulatory regime operating at the level of a system of records—the Act's current choice—is untenable given the state of modern technology. When the predominant medium of information processing was a file cabinet or a mainframe computer, a system-centric privacy approach made some sense. But when records flow between databases, across agency firewalls, and in and out of AI models, the boundaries of the system in question become indeterminate, leaving system of records an inappropriate basis for regulation. And while Congress enacts evermore complex authorizations, perhaps inspired by advances in the technology sector, modern federal agencies struggle against the Privacy Act's outdated framework to secure the requisite and highly-variegated types and amounts of data.

By failing to keep up with the changing technology landscape, Congress has allowed the Act to atrophy, rendering it frequently underwhelming for the individuals whose privacy and due process it was chiefly enacted to protect, yet consistently stifling to well-meaning officials and technology teams, especially those who are keen to reduce administrative burden via techniques like data sharing.

One symptom of the Act's decay is its inherent uniformity. That is, despite the fact that a particular information system could have a wildly different level of relative privacy risk than another, the Act treats the systems as equivalent—and, consequently, imposes its privacy requirements homogenously. For example, the Department of Homeland Security maintains the Systematic Alien Verification for Entitlements (SAVE) system, which outside watchdogs argue has become a an "illegal national citizenship database" that the government could use to "determine eligibility to vote and obtain government benefits," at the same time it operates systems for performing routine administrative tasks, like managing personnel.[35]

[35] Adam Smith, *Americans Overwhelmingly Reject Trump-Vance Administration's Illegal National*

The Act's equivalence of systems is a ruinous legal flattening. In particular, it forces agency teams who want to use data for purposes that are of relatively low privacy risk to abide by the same compliance rules and processes as those who want to use data in ways that are of higher risk. But it's also suboptimal for individual privacy: by splintering the focus of privacy officials and watchdogs alike, high-risk data uses don't consistently receive proportionate levels of scrutiny.

The Privacy Act must operate with a different model. Facing an analogous quandary in consumer privacy, other jurisdictions appear to be settling on an answer: data sensitivity. Following from the correct assessment that a one-size-fits-all-approach to privacy is overly simplistic, states and international governments have adopted laws that apply different requirements based on the relative sensitivity of the data themselves.

For example, the California Consumer Privacy Act (CCPA) recognizes several types of data as "sensitive," including seemingly-obvious ones like "Social Security, driver's license, state identification card, or passport number," but also unintuitive, amorphous categories like "philosophical beliefs."[36] At the federal level, the proposed American Data Privacy and Protection Act (ADPPA) similarly treats SSNs and other government-issued IDs as sensitive while making its own arbitrary choices, "calendar information" being a notable one.[37]Armed with these definitions, the CCPA and ADPPA both provide greater protections for and grant consumers enhanced rights with respect to commercial entities' processing of their sensitive data.

Although the data sensitivity model appears to be gaining traction quickly, its popularity may shroud its fundamental problems. As privacy scholar Daniel Solove has written, "the sensitive data approach has significant costs because it creates the illusion of responding to harm and risk while the most harmful and risky situations are inadequately addressed." In contrast, Solove advocates for an approach to privacy focused on, well, "harm and risk,"

> The sensitive data approach falters because it is centered on a conceptual mistake—it views the nature of the data as the primary factor for determining the appropriate level of protection… What matters most is the harm and risk posed by collecting, using, or transferring personal data. *Harm* involves negative consequences from the collection, use, or transfer of personal data that affect individuals or society. *Risk* involves the likelihood and gravity of certain harms that have not yet occurred… Privacy law should provide more stringent protections based on the harm or risk of harm arising out of certain types of situations involving the collection, use, or transfer of personal data.[38]

Citizenship Database, Citizens for Responsibility & Ethics in Wash. (Dec. 8, 2025), https://www.citizensforethics.org/reports-investigations/crew-reports/americans-overwhelmingly-reject-trump-vance-administrations-illegal-national-citizenship-database/; System of Records Notices (SORNs), Dep't of Homeland Sec., https://www.dhs.gov/system-records-notices-sorns.

[36] CCPA, CAL. CIV. CODE § 1798.140(ae).

[37] American Data Privacy and Protection Act, H.R.8152, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[38] Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of*

Regulating based on harm and risk may appear too subjective at first blush, but Solove rightly points out the arbitrariness of how numerous laws define "sensitive data." He suggests that the perceived objectivity and predictability of the sensitivity approach may very well be illusory. In turn, he suggests that the focus of lawmakers "should not be on *data*, but instead about harmful or risky *uses of data*."[39]

Although there are relatively few examples of a true "harm and risk" privacy approach in the wild, one directionally-aligned attempt—that is maximally germane to include a report on the Privacy Act—was made by Robert Gellman, noted federal privacy expert and longtime Congressional staffer.

In his paper *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974*, Gellman proposes the concept of an "agency activity affecting privacy," for which he uses the shorthand "A3P." Gellman defines A3P as:

> any agency function, program, or operation that involves the processing of a record about an individual. [40]

Gellman flows other definitions in his draft Privacy Act update from A3P, concretizing what a foundational—not incremental—shift in the Act's privacy model could look like. He redefines "record," for example, as "any personally identifiable information processed by or for an agency" as part of an A3P. He defines "agency designated disclosure," his successor to the Act's routine use concept, as "a disclosure by an agency of a record from an [A3P]" that is required or authorized by statute, among other qualifications.[41]

A3P inherently implicates the personally identifiable information of potentially-many individuals, across potentially-multiple systems, by focusing on the purpose of data processing. As Gellman explains:

> The A3P definition focuses on the purpose of processing rather than on the manner in which an agency files or retrieves personally identifiable information. The idea is that an A3P would provide the public with a more understandable view of an agency's personal record keeping by allowing multiple filing systems to be included in the same notice if the systems relate to the same function, program, or operation. The internal details of records organization are of less public interest than the kind of records that an agency processes, the purposes of that processing, and the way in which an agency uses or discloses the records.[42]

Sensitive Data, 118 Nw. U. L. Rev. 1081 (2024), https://ssrn.com/abstract=4322198.

[39] *Id.*

[40] Gellman Report, *supra* note 18.

[41] *Id.*

[42] *Id.*

A3P's conceptual flexibility may render it a potent organizing unit for a revamped purpose-centric privacy model, one that is truly cognizant of harm and risk. Unlike system of records, which lacks an inherent risk level, A3P concerns a distinct, statutorily-authorized agency activity that inherently carries harms and risks to privacy that an agency could reasonably ascertain.

Regardless of whether Congress settles on A3P or another legislative invention, it will need to design a framework that achieves a specific outcome: assigning harm and risk levels to each statutory purpose. Within such a framework, Congress could weigh several factors including, but (crucially) not limited to, as this subsection has argued, the relative sensitivity of data involved. Importantly, Congress should undertake this difficult challenge itself rather than delegate it to an agency like OMB.

Once Congress establishes both (1) a construct for mapping statutory purposes to a legislative unit and (2) a framework for segmenting those purposes by harm and risk level, it can move to contemplating new processing requirements and determining which requirements apply to which segments—a task discussed in the next subsection.

C. Right-size requirements

Recommendation
Congress should right-size the Privacy Act's processing requirements—particularly data minimization, exceptions, and special protections for high-risk processing—by leveraging the framework described in section III.B that segments these requirements based on harm and risk. The Act's data minimization provision, which requires agencies to only maintain records "relevant and necessary" to accomplish a purpose set forth in statute or via executive order, should be strengthened. In particular, Congress should apply substantive minimization principles throughout the data pipeline (collection, use, disclosure, and retention). Congress should also eliminate the ability for the President to, via executive order, authorize new processing purposes. Additionally, Congress should reorient exceptions to the Act's processing requirements around the idea of purpose, enumerating narrow and standardized excepted purposes in statute. Finally, Congress should stipulate special requirements for high-risk processing, such as data deletion or additional transparency requirements, while removing the current consent requirement for low-risk processing.

FIP(s)
Minimization

Discussion
Central to the Privacy Act's processing requirements is how it manifests the principle of data minimization, or collecting, using, disclosing, and retaining the minimal amount of information necessary to fulfill a specific purpose. In particular, the Act stipulates that:

> Each agency that maintains a system of records shall…maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.[43]

Importantly, the term "maintain" is redefined in the Privacy Act to include "maintain, collect, use, or disseminate," thereby capturing other aspects of the data lifecycle beyond storage.[44]

It is vital to accurately characterize the Privacy Act's approach to data minimization, which contains aspects of both substantive and procedural minimization.[45] For example, the Privacy Act requires agencies to, for any given purpose, find a legal basis in statute or executive order. By construction, this provision limits the range of permissible purposes for which an agency may collect, use, and disseminate information and carries a clear valence of substantive minimization. At the same time, the Act imposes decidedly procedural requirements on disclosure, permitting agencies to transfer personal information only if they obtain an individual's written consent (subject to several exceptions to be discussed later).[46]

The Act's approach mirrors that chosen by the American Privacy Rights Act (APRA), which authorizes covered commercial entities to process covered data pursuant to an enumerated set of "permitted purposes" or a "specific product or service" requested by an individual.[47] Namely, both the Privacy Act and APRA require as the primary legal basis for processing an external directive (statutory requirement or executive order and permitted purposes or a consumer request, respectively). Such an approach stands in contrast to one whereby an individual agency or business invents lawful purposes *ex nihilo*.

That said, the ability of a President to construct new purposes for agencies via executive order is ripe for abuse and demands reevaluation. On March 20th, 2025, President Trump issued Executive Order 14243, "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos," directing agencies to, among other things, share and "consolidate" records for the ostensible purpose of identifying and eliminating waste, fraud, and abuse:

> Agency Heads shall take all necessary steps, to the maximum extent consistent with law, to ensure Federal officials designated by the President or Agency Heads (or their designees) have full and prompt access to all unclassified agency records, data, software

---

[43] 5 U.S.C. § 552a(e)(1).

[44] 5 U.S.C. § 552a(a)(3).

[45] "Procedural minimization" refers to an approach to data minimization focused on the procedures an entity must follow to secure a legal basis for permissible collection, use, disclosure, and retainment, such as consent mechanisms. "Substantive minimization" refers to an approach to data minimization that focuses on the inherent nature of the data processing activity itself, depending on a more subjective legal determination of permissibility. *See, e.g., Data Minimization's Substantive Turn: Key Questions & Operational Challenges Posed by New State Privacy Legislation*, Jordan Francis (June 2025), https://fpf.org/wp-content/uploads/2025/06/FPF_Data-Minimization.pdf.

[46] 5 U.S.C. § 552a(b) ("No agency shall disclose any record… except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains…").

[47] American Privacy Rights Act of 2024, H.R.8818, 118th Cong. (2024).

> systems, and information technology systems — or their equivalents if providing access to an equivalent dataset does not delay access — *for purposes of pursuing Administration priorities related to the identification and elimination of waste, fraud, and abuse*. This includes authorizing and facilitating both the intra- and inter-agency sharing and consolidation of unclassified agency records.[48] (emphasis added)

Although the EO cannot supersede the Privacy Act's consent-based disclosure requirement, meaning agencies still have to go through pathways like the "need-to-know" and "routine use" exceptions to share data, it does set forth a purpose, "identification and elimination of waste, fraud, and abuse," which agencies have already invoked to authorize novel data collections.

The United States Department of Agriculture (USDA) is just one example. In May 2025, the USDA, listing EO 14243 as one of its legal authorities, requested from state agency directors comprehensive and unprecedented access to any data related to the administration of the Supplemental Nutrition Assistance Program (SNAP), including personal information on applicants and recipients:

> At present, each state, district, territory, and payment processor is a SNAP information silo. These various entities maintain discrete collections of SNAP application, enrollment, recipient, and transaction data, each of which is necessary in ensuring the integrity of the program… Pursuant to, among other authorities, *the President's Executive Order*, 5 USC 553(a)(2), 7 USC 2020(a)(3), and 7 CFR 272.1(e), USDA is taking steps to require all states to work through their processors to submit at least the following data to FNS… records sufficient to identify individuals as applicants for, or recipients of, SNAP benefits, including but not limited to personally identifiable information in the form of names, dates of birth, personal addresses used, and Social Security numbers. [49] (emphasis added)

Although ongoing litigation has frustrated USDA's effort, the ordeal illustrates the risks that attend the data processing hall pass that is the purpose-authorization-via-executive-order clause. Even accounting for legitimate needs for executive agility in responding to unforeseen circumstances, Congress should eliminate this authority and reserve for itself the right to authorize purposes for which the federal government may process Americans' personal data.

Alongside its substantive minimization requirements, the Privacy Act regulates disclosure through procedural mechanisms. In particular, the Act requires an agency to obtain consent from an individual prior to disclosing their records, subject to thirteen enumerated exceptions. Setting aside the fraught nature of these exceptions, which are discussed in a later subsection, the Act's consent-based approach to disclosure itself is inherently flawed and in need of reform.

In fact, a commission created by the Privacy Act suggested as early as 1977 that an overreliance on consent would prove injurious to individual privacy. The Privacy Protection Study

---

[48] Exec. Order No. 14,243, § 3(a), 90 Fed. Reg. 13681 (Mar. 20, 2025).

[49] U.S. Dep't of Agric., Letter re: FNS Data Sharing Guidance (May 6, 2025), https://www.fns.usda.gov/snap/data-sharing-guidance.

Commission (PPSC), established by the Privacy Act, was tasked with studying a host of public and private organizations' data processing activities and making recommendations to Congress about how to protect individual privacy. In its final report, the PPSC criticized privacy models that rely too heavily on consent:

> The Commission finds that as records continue to supplant face-to-face encounters in our society, there has been no compensating tendency to give the individual the kind of control over the collection, use, and disclosure of information about him that his face-to-face encounters normally entail…Where records play [a gatekeeping role], the individual usually has no choice but to allow them to be used in making decisions about him. Since informed consent is valid only if wholly voluntary, it means little in this context. Hence, the Commission finds authorization the appropriate pre-condition of disclosure, rather than informed consent, and couples it with a principle of limited disclosure.[50]

In the consumer privacy context, too, an increasing number of lawmakers and experts are rejecting consent as an end-all privacy control. During an Energy & Commerce Committee hearing on data privacy in the 118th Congress, then-Ranking Member Frank Pallone called for "[rejecting] the coercive notice and consent system that has failed to protect American's data privacy and security." During her testimony in that same hearing, Alex Givens of the Center for Democracy and Technology expounded on the pitfalls of a consent-based approach to privacy:

> Any modern user of technology knows why this notice and consent model is broken. Even if a consumer could feasibly read and understand these labyrinthine privacy policies, they often have no real choice but to consent. Many online services are such an important part of everyday life that quitting is effectively impossible. We have to move on from this broken regime of notice and consent to one that establishes baseline safeguards for consumer information, clear rules of the road for businesses and meaningful enforcement of the law. [51]

That's not to say consent is altogether inappropriate when applied meaningfully, particularly if it functions as a compliment to a baseline of stronger privacy controls. In fact, it may provide a useful level of friction for data processing that is of relatively high-risk to individual privacy. For example, APRA recognizes the value of targeted, informed consent—and selectively applies it to disclosures of sensitive data:

> Subject to subsection (a), a covered entity may not transfer sensitive covered data to a third party or direct a service provider to transfer sensitive covered data to a third party without the affirmative express consent of the individual to whom such data pertains, unless for a [permitted purpose].[52]

---

[50] Privacy Commission Report, *supra* note 12, at 13.

[51] Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy: Hearing Before the Subcomm. on Innovation, Data, and Commerce of the H. Comm. on Energy and Commerce, 118th Cong. (2023).

[52] American Privacy Rights Act of 2024, H.R.8818, 118th Cong. (2024).

Congress could thus improve the Privacy Act's data processing requirements along three critical dimensions: (1) data minimization, (2) exceptions, and (3) special protections for high-risk processing. Specifically, Congress should, assuming that it has instituted a segmentation framework based on the harm and risk of statutory purposes consistent with the previous subsection:

- *Bolster the data minimization standard.* Switch to the language of "necessary, proportionate, and limited" from "relevant and necessary" for an agency's processing of PII. To that end, retain the limitation on agencies' processing of PII to those purposes authorized by statute, while eliminating the authorization-via-executive-order clause. Drop the default consent requirement for low-risk processing, thereby permitting agencies to, for instance, perform a large class of disclosures without written consent.
- *Standardize and narrow exceptions.* Design a new exceptions framework organized around excepted purposes and data processing types. Map all exceptions to the consent-based disclosure requirement to a list of excepted purposes. Conceptually, this list of exceptions would narrowly expand the universe of permitted processing purposes beyond those authorized by statute. With respect to the "routine use" exception, analyze the most common and meritorious routine uses across agencies, such as processing to prevent or mitigate data breaches, and append to the aforementioned list of excepted purposes. Finally, eliminate the "need to know" and "routine use" exceptions entirely. (Note that exceptions are discussed further in section III.E of the report.)
- *Special protections for high-risk processing.* To bolster the baseline requirements described above for data processing pursuant to high-risk purposes ("high-risk processing"), Congress should consider imposing special protections. For example, Congress could retain the current consent-based disclosure requirement only for high-risk processing, but improve the language to require affirmative express consent, in line with many current consumer privacy laws. Additional protections on high-risk processing could include prescribing specific data retention periods after which agencies must dispose of particular data consistent with federal records laws; granting individuals the right to archive their personal information; or building in elevated transparency measures. An especially enterprising Congress could even decide that it wants to exert particular influence and establish a Congressional Review Act-like mechanism for ceasing or otherwise curtailing high-risk data processing on a fast track.

With this new requirement apparatus in place, the Act can be further simplified. Namely, the privacy and due process requirements (for example, the verification and opportunity to contest findings) related to computer matching begot by the Computer Matching and Privacy Protection Act (CMPPA) can instead become additional protections for a qualified subset of high-risk processing (leveraging the revised definition of "matching program" discussed in section III.A).

Congress should transfer the remainder of the CMPPA's provisions, such as the requirement that a written agreement for a matching program exist and include metadata like "the purpose and legal authority for conducting the program" to a consolidated transparency tool. Finally, the ineffectual Data Integrity Boards established by the CMPPA can be done away with, insofar as the new Act imposes robust transparency requirements, facilitates external oversight by the legislative branch, and concentrates internal governance within the agency Chief Privacy Officer. (Note: each of these ideas will be fleshed out in later subsections).

Strengthening the Act's requirements in the manner described in this subsection would effectuate, subtly, another crucial goal: eliminating the distinction between inter- and intra-agency disclosures. Sprawling agencies like the Department of Homeland Security can create serious privacy risks simply by combining data within their own systems. These internal combinations in many cases warrant even stronger protections than the case in which two distinct agencies share data with one another. Strengthened data minimization, purpose-based exceptions, and special protections for high-risk processing collapse this distinction since they turn on data, purpose, and risk, respectively, rather than agency, ensuring privacy protections cover all forms of processing, within and between agencies.

D. Regulate agencies' use of commercially available information

Recommendation
Congress should improve the transparency of and establish an authorization process for agencies' use of commercially available information that may contain personally identifiable information. By modeling this process on or incorporating it into the Federal Risk and Authorization Management Program, which provides a security assessment process for cloud service offerings, Congress could standardize evaluations of commercially available datasets and mitigate privacy risk. Moreover, Congress could stipulate that such authorizations be made publicly available via a centralized portal, facilitating its own oversight while simultaneously improving accountability.

FIP(s)
Authority, Quality & Integrity, Transparency

Discussion
The Privacy Act's authors could not have foreseen the proliferation of commercially available information (CAI) in the decades following the Act's passage—especially CAI containing personally identifiable information (PII) sold by data brokers—nor federal agencies' voracious appetite for such data. Although, the Act's broad framework generally covers CAI containing PII under its system of records umbrella, such information presents emergent privacy risks that demand additional quality and transparency controls which Congress is uniquely positioned to mandate.

In order to regulate CAI effectively, one must first define it. Lacking a statutory definition for CAI, President Biden settled on one for his 2023 executive order on *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*:

> The term "commercially available information" means any information or data about an individual or group of individuals, including an individual's or group of individuals' device or location, that is made available or obtainable and sold, leased, or licensed to the general public or to governmental or non-governmental entities.[53]

[53] Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Nov. 1, 2023).

This definition, however, fails to capture the scope of CAI use across the federal government. While authoritative data remains scarce, public reporting paints a troubling picture:

> For years, news outlets have reported on how federal and state agencies buy Americans' data from private companies called data brokers—in mass. These brokers purchase and aggregate users' location data from virtually all applications. Brokers, in turn, repackage and sell geolocation data to willing buyers, including the federal and state governments. This has led to the government purchasing data on 98 million users from a prayer app, as well as tens of millions of users' data from dating apps, mobile games, the Weather app, Google, rideshare apps, and social media apps. This data can reveal some of the most intimate information about people, from their faith, political associations and beliefs, immigration status, pregnancy status or interest in seeking an abortion, and more. A recently declassified report from the Office of the Director of National Intelligence confirms what has been known for years: Brokers sell people's private data to the government.[54]

Historically, the most common governmental uses of CAI have been by law and immigration enforcement and the intelligence community. However, civilian agencies—the focus of this report—have increasingly relied on CAI to administer federal programs, including by verifying identity and preventing fraud:

> Login.gov, for instance, transmits the data to companies including LexisNexis, an information conglomerate that was awarded a $34 million contract last December to verify users' identities… In 2021, the Department of Labor awarded LexisNexis a $1.2 billion deal to prevent fraud in state unemployment insurance programs. (The contract was later reduced to $528 million.) The Labor Department also has a $2 billion effort for fraud detection, which involves LexisNexis and the credit monitoring agency TransUnion. (TransUnion, which is also registered as a data broker, has its own contract with Login.gov for fraud prevention.) Other companies that are registered data brokers, such as Accenture and Acxiom, also have contracts with the federal government. Accenture has a $73 million contract with the IRS for fraud prevention, while Acxiom did identity verification for the Department of Veteran Affairs.[55]

Unsurprisingly, the federal government's use of CAI raises unique privacy considerations that demand Congress's attention. According to OMB, for example, "factors including the sensitivity and volume of PII contained in some CAI may exacerbate privacy risks and limit the application of key principles that are foundational to agency handling of PII, such as data minimization, transparency, and individual participation."[56]

---

[54] Aaron X. Sobel, *Data Broker Sales and the Fourth Amendment,* Lawfare (March 11, 2024), https://www.lawfaremedia.org/article/data-broker-sales-and-the-fourth-amendment.

[55] Eric Geller, *Lawmakers Demand Answers on Data Brokers Selling Info to Federal Government*, Politico (Dec. 21, 2022), https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600.

[56] Request for Information: Executive Branch Agency Handling of Commercially Available Information Containing Personally Identifiable Information, 89 Fed. Reg. 83,517 (Oct. 16, 2024).

Yet while CAI, generally speaking, presents greater risks to individual privacy than data collected via other channels (such as directly from an individual) agencies routinely lean on it. In fact, this outcome is directly related to the Act's outdated privacy model: by applying requirements uniformly as previously discussed, the Act engenders a dynamic in which civilian agencies under pressure from Congress to meet statutory deadlines routinely look to commercial data brokers rather than other agencies or individuals for requisite data, despite the Act's express requirement to "collect information to the *greatest extent practicable* directly from the subject individual" (emphasis added).[57] Meanwhile, law and immigration enforcement together with the intelligence community enjoy copious exceptions that they, in turn, use to vacuum up as much CAI as possible and liberally share it amongst one another. In the end, individual Americans suffer escalating privacy risks, civilian agencies incur millions of dollars in needless costs, investigatory agencies enjoy unchecked access to CAI, and unregulated data brokers are propped up by lucrative government contracts.

This state of affairs is messy, inefficient, and indefensible. To ameliorate the substantial privacy concerns of CAI, especially CAI containing PII, Congress should, as a preliminary matter, require more transparency, stipulating that every agency explicitly describe whether and how CAI is used for a statutory-authorized purpose. For example, relevant details could include the source of the CAI, its data types, the amount spent on it, and its legal basis. (Suggestions for improvements to the Act's transparency regime are further discussed in section III.F.)

But Congress could and should go further than pure transparency, establishing a standardized authorization framework for CAI that meaningfully mitigates privacy risk for individuals, improves quality control, and eliminates redundant procurements.

In this regard, the Federal Risk and Authorization Management Program (FedRAMP) provides a template. FedRAMP is the federal government-wide compliance program providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Initially established by OMB in 2011, Congress, recognizing its enormous value to the federal information technology enterprise, codified the program in 2022 through the FedRAMP Authorization Act.[58] By all accounts, FedRAMP has been an enormous success:

> FedRAMP has operated by partnering with agencies and third-party assessors to identify appropriate cloud computing products and services, and evaluate those products and services against a common baseline of security controls. Agency authorizing officials use this information to make informed, risk-based, and efficient decisions concerning the use of those cloud computing products and services. Since FedRAMP's inception, agencies have reused existing authorizations hundreds of times across over 300 offerings, and the program has provided a consistent gateway for industry to navigate entry and onboarding into the Federal marketplace.[59]

[57] 5 U.S.C. § 552a(e)(2).

[58] Pub. L. No. 117-263, § 5921 (2022), codified in part at 44 U.S.C. §§ 3607-16.

[59] Office of Mgmt. & Budget, Exec. Office of the President, *Memorandum M-24-15, Modernizing*

With a straightforward substitution of CAI, such a description could be adapted for an imaginary FedRAMP-for-CAI program:

> **FedRAMP-for-CAI** has operated by partnering with agencies and third-party assessors to identify appropriate CAI products and services, and evaluate those products and services against a common baseline of **privacy** controls. Agency authorizing officials use this information to make informed, risk-based, and efficient decisions concerning the use of those **CAI** products and services.

Like FedRAMP, FedRAMP-for-CAI would reap programmatic and financial benefits for agencies, while enhancing regulatory clarity for CAI providers. For example, an agency with an acute data need could first determine whether another, vetted CAI product satisfies its requirements rather than embarking on its own procurement. Moreover, by centralizing CAI authorizations, they could be surfaced on a publicly-available website, available for audit by the public, Inspectors General, and Congress. In designing FedRAMP-for-CAI, Congress should consider existing policy and initiatives impacting CAI, especially the Intelligence Community Policy Framework for Commercially Available Information and OMB's 2024 Request for Information on Executive Branch Agency Handling of Commercially Available Information Containing Personally Identifiable Information.[60]

Although included under the umbrella of Privacy Act reform for the purposes of this report, FedRAMP-for-CAI is a program that would exist upstream of each agency's implementation of the Act's core requirements. That is, by shifting to the purpose-centric privacy model outlined in section III.B, the precise *source* of records—whether from a commercial entity in the form of CAI or an individual, for instance—will not matter: agencies will still be responsible for implementing the Act's processing requirements according to the relative harm and risk of a particular purpose which may implicate a multiplicity of data sources.

E. Standardize and narrow exceptions

Recommendation

Congress should standardize and narrow exceptions to the Privacy Act's requirement that a purpose be statutorily authorized. At present, the Act provides two notable exceptions, known colloquially as the "need-to-know" and "routine use" exceptions. Successive administrations have abused these exceptions, and Congress should eliminate them. In their place, Congress should adopt a standardized framework organized around excepted purpose and the type of data

---

the Federal Risk and Authorization Management Program (FedRAMP) (July 24, 2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/M-24-15-Modernizing-the-Federal-Risk-and-Authorization-Management-Program.pdf.

[60] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, INTELLIGENCE COMMUNITY POLICY FRAMEWORK FOR COMMERCIALLY AVAILABLE INFORMATION (2024), https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf; Request for Information: Executive Branch Agency Handling of Commercially Available Information Containing Personally Identifiable Information, 89 Fed. Reg. 83,517 (Oct. 16, 2024).

processing—collection, maintenance, disclosure, and retention—permitted for the purpose being excepted.

FIP(s)
Individual Participation, Purpose Specification and Use Limitation, Transparency

Discussion
Any privacy law, whether in the governmental or commercial context, will need to contemplate exceptions: those circumstances in which it is impossible, impractical, or otherwise undesirable to enforce its core requirements.

In the context of federal privacy, the primary consideration when designing an exceptions framework is operational flexibility. More specifically, Privacy Act reform must strike the right balance between safeguarding individual privacy and ensuring the effective administration of government, especially when novel circumstances arise. The original Act navigated this dilemma by constructing a list of exceptions to its requirement that agencies obtain consent prior to disclosure.

By default, the Act requires an agency to obtain written consent from the subject individual prior to disclosing their records to any entity, including internal officials:

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains…[61]

However, thirteen statutory exceptions exist to this written consent requirement.[62] Of those exceptions, two have been the most abused by agencies in ways that functionally eliminate the consent requirement—and received commensurate attention from privacy advocates and Congress: (1) the need-to-know and (2) routine use exceptions.

The need-to-know exception excepts from the written consent requirement "those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties."[63] Agencies have likely invoked this exception to facilitate intra-agency disclosures for decades. But the need-to-know exception has received particular scrutiny under the Trump Administration and its Department of Government Efficiency (DOGE).

In early 2025, for example, a group of labor unions representing federal employees sued the Trump Administration, alleging that individuals affiliated with the DOGE were granted unauthorized access to sensitive Treasury Department records in violation of the Privacy Act.[64]

[61] 5 U.S.C. § 552a(b).

[62] 5 U.S.C. § 552a(b)(1)-(13).

[63] 5 U.S.C. § 552a(b)(1).

[64] ALLIANCE FOR RETIRED AMERICANS v. BESSENT, 1:25-cv-00313, (D.D.C. Apr 11, 2025)

In its defense, the federal government invoked the need-to-know exception, alleging that "providing access to agency records to members of the Treasury DOGE team falls within [the exception]."[65] The purported "need" of these DOGE officials, pursuant to the exception, was set forth in one of President Trump's early executive orders, in which the goal of DOGE was defined as, among other aspects, "improv[ing] the quality and efficiency of government wide software, network infrastructure, and information technology (IT) systems," a totalizing mandate with respect to the government's digital footprint.[66] When a "need" can be so widely constructed as to implicate most or all of an agency's information systems, the need-to-know exception effectively swallows any protections against unauthorized *intra*-agency uses that the Privacy Act was designed to provide.

Meanwhile, agencies do not appear to keep detailed records, or any records for that matter, about the need-to-know exceptions they grant, obfuscating the actual scale of the problem—and forcing watchdogs to, as in the DOGE and Treasury case, rely on public reporting to surmise who has access, perhaps unlawfully. The need-to-know exception's utility is questionable at best, while the risks are demonstrable; Congress should consider eliminating it in favor of a more intentional framework for mediating agency employees' access to records necessary to accomplish a statutorily authorized purpose.

The Act's "routine use" exception has been similarly wielded by administrations current and past, albeit for facilitating *inter*-agency (and inter-government) record disclosure. Specifically, this provision excepts from the written consent requirement "a routine use," defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected."[67]

The routine use exception enables routine abuse. While defending the DOGE's sharing of sensitive taxpayer information to agencies and officials outside of Treasury in the same case described above, the Department of the Treasury also cited the routine use exception.[68] Specifically, the "routine use" asserted to defend the DOGE's inter-agency disclosure of taxpayer information was "for the purpose of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, federal funds," listed as a routine use since February 2020 on the System of Records Notice (SORN) for the Treasury payment system in question. This routine use was codified years before the DOGE was created and sustained throughout the Biden Administration.[69]

Indeed, the DOGE seemed to leverage this exception to share sensitive taxpayer information outside of Treasury despite the dubious compatibility of the transfer with the original purpose for which the data was collected. For example, one DOGE staffer combing through Treasury

[65] ALLIANCE FOR RETIRED AMERICANS v. BESSENT, 1:25-cv-00313, (D.D.C. Apr 11, 2025) ECF No. 61.

[66] Exec. Order No. 14,158, § 4(a), 90 Fed. Reg. 8441 (Jan. 23, 2025).

[67] 5 U.S.C. § 552a(b)(3); 5 U.S.C. § 552a(a)(7).

[68] ALLIANCE FOR RETIRED AMERICANS v. BESSENT, 1:25-cv-00313, (D.D.C. Apr 11, 2025) ECF No. 61.

[69] 85 Fed. Reg. 11776 (Feb. 27, 2020).

payment data, which is housed by the Bureau of Fiscal Service (BFS), was granted access to payment systems by BFS officials while his security clearance process was still ongoing. In a legal filing, BFS's Chief Privacy Officer (CPO) stated that the staffer "sent an email with a spreadsheet containing [personally identifiable information] to two United States General Services Administration officials." According to the CPO, the spreadsheet contained rows which "detailed a name (a person or an entity), a transaction type, and an amount of money."[70]

Legally speaking, there isn't much to stand in the way of an agency that seeks to employ a routine use as the legal basis for disclosure. A court's assessment of the validity of a particular routine use generally occurs on a case-by-case basis and turns on an interpretation of the phrase "compatible with the purpose for which [a record] was collected" in the definition of "routine use." The Court of Appeals for the D.C. Circuit, for instance, interpreted a compatible disclosure as one that "would not actually frustrate the purposes for which the information was gathered."[71] The Act's failure to provide a definition of "compatible" or otherwise flesh out the standard for an appropriate routine use has fomented ambiguity ripe for exploitation.

Agencies' SORNs are littered with routine uses that could very well fail a true compatibility test, let alone a sniff test. The Department of Transportation, for example, considers it compatible with the original purpose of collection to disclose records contained in a system that consumers use to report potential violations of motor carrier safety regulations to "foreign governments" for counter-terrorism purposes.[72]

But routine uses don't just service one-off agency needs. Counterintuitively, routine uses have evolved into the legal vehicle of choice for authorizing government-wide, standardized disclosures. EO 14249, for example, directed agencies to "review and modify, as applicable, their relevant System of Records Notices (SORNs) under the Privacy Act of 1974 to include a routine use that allows for the disclosure of records to the Department of the Treasury for the purposes of identifying, preventing, or recouping fraud and improper payments" within 90 days of the order.[73] Moreover, this routine use imposes minimal restrictions beyond the tacit compatibility test: disclosures need only be "relevant to review payment and award eligibility," a criterion that could potentially reach any records related to federal payments for benefits programs, grants, loans, or otherwise. OMB's implementing guidance for EO 14249 even sets forth the exact routine use with which agencies are expected to amend relevant SORNs:

> To the U.S. Department of the Treasury when disclosure of the information is relevant to review payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state (meaning a state of the

[70] State of New York, et al. v. U.S. Department of the Treasury, et al., No. 1:25-cv-1144-JAV (S.D. NY. Mar. 14, 2025).

[71] DOJ Overview, *supra* note 14.

[72] 90 Fed. Reg. 47,496 (Oct. 1, 2025).

[73] Exec. Order No. 14,249, § 3(d), 90 Fed. Reg. 14,011 (Mar. 28, 2025).

> United States, the District of Columbia, a territory or possession of the United States, or a federally recognized Indian tribe) in a state-administered, federally funded program.[74]

Notwithstanding the importance of preventing improper payments in federal programs, attempting to effectuate a government-wide exception to the Privacy Act in the manner of EO 14249 is precisely the sort of job Congress, not OMB, should perform. And yet, many administrations have chosen to go through executive fiat and the Act's exceptions framework rather than Congress for legally authorizing government-wide data sharing necessary to accomplish their policy objectives. In this regard, removing the "routine use" exception would if nothing else force the executive to work more closely with Congress.

The Privacy Protection Study Commission's (PPSC) discussion of the routine use exception just a few years after the enactment of the Privacy Act zeroed in on its flaws. In its final report, the PPSC argued the exception was becoming increasingly unwieldy, especially in the context of law enforcement, and suggested that Congress replace the routine use's compatibility test with a "test for consistency,"

> Currently, agencies of the Federal government seem to be employing the routine-use provision in order to permit the free flow of law enforcement and investigative information… Agency system notices frequently indicate that information will be supplied to appropriate Federal, State, local, and, sometimes, foreign law enforcement agencies of government. In short, the Privacy Act does not place an effective burden on, or barriers to, the free flow of information within the law enforcement and investigative community… the Commission believes that the compatible-purpose test of the routine-use provision should be augmented by a test for consistency, with the conditions or reasonable expectations of use and disclosure under which the information was provided, collected, or obtained. The individual's point of view must be represented in the agency's decision to use or disclose information, and today the compatible-purpose test only takes account of the agency's point of view. [75]

Insofar as an agency posts their routine use in the *Federal Register*, they can define that use arbitrarily and broadly, reducing the Privacy Act's inter-agency disclosure requirement down to a mere procedural hurdle—one that agencies easily clear.

In conclusion, the need-to-know exception frequently swallows protections against violative intra-agency uses, while the routine use exception similarly undermines safeguards preventing improper inter-agency disclosures. A determined agency armed with these exceptions could very well violate the spirit of the Privacy Act while staying within the limits delineated by the letter of the law. Congress must act to standardize, narrow, and enforce—especially through transparency

---

[74] Memorandum from Russell T. Vought, Dir., Office of Mgmt. & Budget, Exec. Office of the President, to the Heads of Exec. Dep'ts & Agencies on Preventing Improper Payments and Protecting Privacy Through Do Not Pay (Aug. 20, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/08/M-25-32-Preventing-Improper-Payments-and-Protecting-Privacy-Through-Do-Not-Pay.pdf.

[75] Privacy Commission Report, *supra* note 13.

measures, technical controls, and redress as discussed in sections III.F, III.G, and III.H respectively—any exceptions to the Privacy Act's statutory purpose requirement.

With respect to standardization and narrowing, Congress should overhaul the Act's exceptions framework. In particular, section III.C recommended that Congress:

> *Standardize and narrow exceptions.* Design a new exceptions framework organized around excepted purposes and data processing types. Map all exceptions to the consent-based disclosure requirement to a list of excepted purposes. Conceptually, this list of exceptions would narrowly expand the universe of permitted processing purposes beyond those authorized by statute. With respect to the "routine use" exception, analyze the most common and meritorious routine uses across agencies, such as processing to prevent or mitigate data breaches, and append to the aforementioned list of excepted purposes. Finally, eliminate the "need to know" and "routine use" exceptions entirely.

Each of these parts can be fleshed out.

> Design a new exceptions framework organized around excepted purposes and data processing types.

Congress must structure the Act's new exceptions around clearly defined purposes, with additional qualifications (such as limiting exceptions to a particular agency) as necessary. The framework must also distinguish between types of data processing: for example, collection, maintenance, disclosure, and retention.

A focus on excepted purposes maps reasonably well to the method by which leading consumer privacy proposals design their exceptions. Although the American Privacy Rights Act (APRA) uses the term "permitted purposes," it is still excepting from its default state (no collection, use, disclosure, or retention of data unless a consumer has expressly requested a product or service) an enumerated list of purposes. For example, APRA allows covered entities to process data "to conduct market research," an analogous purpose to agencies collecting user feedback to improving their delivery of services.[76]

With respect to data processing types, it is vital to grasp that the Act's current exceptions concern only disclosures.[77] The Privacy Act's exceptions must become inclusive of the entire suite of data processing types, expanding beyond disclosure to cover collection, use, and retention.

A purpose-based framework should organize exceptions into tranches, one for each type of data processing: collection, use, disclosure, and retention. Although this adds conceptual complexity,

[76] American Privacy Rights Act of 2024, H.R.8818, 118th Cong. (2024).

[77] Although the Act does stipulate "general exemptions" (for instance, systems "maintained by the Central Intelligence Agency"), for the purposes of this subsection, this recommendation focuses only on the Act's exceptions to its consent-based disclosure requirement.

it would ease the transition from the Act's current model—which excepts only disclosures. Existing exceptions could be mapped onto the disclosure tranche, while new exceptions could address collection, use, and retention.

Aside from presenting low transition costs, this multifurcation of exceptions would provide ample flexibility for lawmakers. For instance, if Congress wanted to facilitate agencies' collection of user feedback data, an industry-standard technique limited by both the Privacy Act and related laws like the Paperwork Reduction Act, for the purpose of improving service delivery, it could expressly exempt that purpose in the "collection" tranche.[78]

> Map all exceptions to the consent-based disclosure requirement to a list of excepted purposes.

With a purpose-based and processing-type-aware exceptions framework in place, Congress needs to fill it with, unsurprisingly, some excepted purposes. And the first place it should look at is the existing set of exceptions to the consent-based disclosure requirement, frequently referred to as "statutory routine uses," all of which are eligible to be mapped to the new framework, setting aside need-to-know and routine-use which require special treatment.

The Act's exception for the disclosure of records "to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13" is exemplary.[79] This particular exception needn't be revised at all to fit the new exceptions framework since it already contains the requisite components: (1) a specific purpose and (2) a processing type. It is also illustrative of an optional qualification: limiting the disclosure exception to a single agency, in this case the Census Bureau.

The other nine statutory routine uses enumerated in 5 U.S.C. § 552a(b) will likely need to be surgically revised to conform to the new framework. These revisions, however, shouldn't alter their existing scope: that is, any invocation of these exceptions by an agency under the current Act should remain legally valid post-transition to the new exceptions framework.

> Conceptually, this list of exceptions would narrowly expand the universe of permitted processing purposes beyond those authorized by statute.

Under this proposal, agencies would only be legally authorized to process data in two cases: (1) explicitly authorized by statute or (2) their desired data processing activity (collection, maintenance, disclosure, retention, or some combination thereof) is covered by a specific excepted purpose. No longer would an administration or agency be allowed to authorize novel purposes via executive order or vague routine uses, respectively.

This framework also preserves critical safeguards. By focusing on purposes rather than blanket exemptions, the Act's general processing requirements—substantive data minimization,

[78] Alexander Mechanick, *How to Fix the Paperwork Reduction Act*, Niskanen Ctr. (Apr. 16, 2025), https://www.niskanencenter.org/how-to-fix-the-paperwork-reduction-act/.

[79] 5 U.S.C. § 552a(b)(4).

transparency controls, and others—would remain in effect even when agencies invoke exceptions. Within this new framework, exceptions authorize the 'what' of data processing, but not the 'how.'

> With respect to the "routine use" exception, analyze the most common and meritorious routine uses across agencies, such as processing to prevent or mitigate data breaches, and append to the aforementioned list of exceptions. Finally, eliminate the "need-to-know" and "routine use" exceptions entirely.

Given the historical abuse of the need-to-know exception, it should ideally be eliminated and replaced with a framework for internal records access that is more rigorous, standardized, and transparent—the purpose-based access controls proposal discussed further in section III.G is directionally aligned with this idea.

With respect to the routine use exception: the executive branch has at times attempted to use the exception for well-founded, government-wide, inter-agency disclosures rather than effectuating a statutory change through Congress. Those particular routine uses that have merit should be expressly permitted in a rewritten Privacy Act, transposed into the new exceptions model proposed in this subsection.

One such example is combatting data breaches, the scourge of the federal information technology environment. Sophisticated entities, whether organized nation-state actors or cybercriminals, are increasingly exploiting vulnerabilities in federal technology systems. Successful penetration of systems containing personally identifiable information (PII) directly implicates Americans' privacy and demands agencies respond swiftly and forcefully—including sharing information held in impacted systems with internal and external government officials and, potentially, private-sector incident response teams.

In 2017, the Obama Administration recognized the strategic need for agencies to disclose data for the purposes of responding to and mitigating breaches of PII. In turn, OMB directed agencies to add to each of the agencies' SORNs two novel routine uses, including "To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that there has been a breach of the system of records, (2) [the agency] has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, [the agency] (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with [the agency's] efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm."[80] While this routine use is itself too broadly written, its goal of preventing data breaches is reasonable and shows the type of government-wide data processing need that Congress could authorize under a revised exceptions framework.

[80] Office of Mgmt. & Budget, Exec. Office of the President, *Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf.

Notwithstanding the fact that routine uses are at times used to achieve important policy objectives, it is dubious to suggest that, after decades of history and its attendant evidence of misuse, agencies still require the immense flexibility that the exception provides.

To gracefully eliminate the routine use exception, Congress should first inventory routine uses that appear across most agencies and SORNs. It should then codify only the meritorious ones as statutorily-excepted purposes in the disclosure tranche discussed earlier—those providing demonstrable value or whose elimination would undermine Congressional objectives, such as for the goal of responding to data breaches. Robert Gellman refers to this list of exceptions as "allowable disclosures," consisting of the summation of a routine use inventory plus the statutory routine uses discussed earlier in this subsection, such as the exception allowing agencies to disclose records to the Census Bureau.[81]

Taken as a whole, this exceptions model would present a clearer, more principled approach that agencies could not easily abuse. Such a model would force agencies to go through Congress for bespoke purpose authorizations or demonstrate a sufficient need to codify a new government-wide excepted purpose—a high barrier, to be sure, but not an insurmountable one.

F. Consolidate transparency measures

Recommendation
Congress should consolidate the Privacy Act's transparency measures into a living inventory of purposes available on a centralized public website. The current measures (System of Records Notices, matching agreements, Privacy Impact Assessments, and individual access) and their mediums (the *Federal Register*, agency websites, and physical and electronic mail) are insufficient for apprising Congress, civil society, and the public of agencies' privacy practices. Meanwhile, agencies incur substantial compliance costs that disincentivize data processing for low-risk purposes, especially for improving service delivery. Reforming the Privacy Act's transparency regime represents a win-win for Americans' privacy and federal agencies' ability to deliver on their missions.

FIP(s)
Transparency

Discussion
The Privacy Act and succeeding laws (particularly the Computer Matching and Privacy Protection Act (CMPPA) and E-Government Act of 2002) attempted admirably to ensure Americans understood what data government held about them, and how that data was used. In fact, Congress explicitly manifested this goal in the Act's findings section:

> There must be no personal data recordkeeping systems whose very existence is secret.

[81] Gellman Report, *supra* note 18, at 93.

> There must be a way for an individual to find out what information about him is in a record and how it is used.[82]

Unfortunately, the Act's transparency apparatus is wanting. Assembled haphazardly over decades, the amalgam of Systems of Record Notices (SORNs), matching agreements, and Privacy Impact Assessments (PIAs) has become inscrutable, duplicative, and, put plainly, ineffective. A revamped Privacy Act must fundamentally rethink how it implements transparency, leaning into modern technology and open data principles.

The Privacy Act stipulates that every agency must publish in the *Federal Register* a notice regarding "the existence and character" of each system of records, including such metadata as:

> (A) the name and location of the system;
>
> (B) the categories of individuals on whom records are maintained in the system;
>
> (C) the categories of records maintained in the system;
>
> (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
>
> (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
>
> (F) the title and business address of the agency official who is responsible for the system of records;
>
> (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
>
> (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
>
> (I) the categories of sources of records in the system.[83]

As the primary mechanism for apprising individuals of information related to their privacy, SORNs have failed. Even if an individual is successful in discerning their need to consult the *Federal Register*, they'll subsequently need to conjure up the right search query for the SORN of interest—before landing on a page replete with technical jargon.

Where SORNs have succeeded, albeit in a limited way, is providing enterprising researchers, journalists, and privacy experts with an approximation of the federal government's data holdings.

---

[82] The Privacy Act of 1974, Pub L. No. 93-579, §2, 88 Stat 1896 (Dec. 31, 1974).

[83] 5 U.S.C. § 552a(e)(4).

Indeed, SORNs enable some degree of accountability for federal agencies that cannot be disputed.

But the public, through Congress, should demand better. It is difficult to square SORNs' dubious transparency benefits with the chilling effect they seem to have on well-meaning teams within agencies. SORNs often take months if not years to update—if agencies even update them at all. This cumbersome process reduces compliance with the spirit of the Act, requiring agency officials to navigate an onerous regulatory regime to accomplish their mission requirements, usually by seeking out exemptions and exceptions. And even if agencies do the work to update SORNs, they tend to employ overly broad language that shirks accountability: yet another casualty of kludge.

To be clear, it is likely that some agencies, especially those in law enforcement, have deliberately violated the Privacy Act's SORN requirement to conceal controversial data processing.[84] But it is also true that needless friction inherent in the production of SORNs has hamstrung agencies looking to use data responsibly. Combine that with SORNs' relatively low benefit to individuals about whom the government holds data, and the cause for Congressional action on SORNs looks irrefutable.

Enacted in 1988, the CMPPA amended the Privacy Act to impose new procedural, due process, and transparency requirements on agencies looking to perform cross-agency "matching" of individuals' records for the purposes of administering federal benefits programs or handling federal personnel matters. Matching agreements, as defined by the CMPPA, serve as the legal basis for the matching program, and require agencies to furnish important information to OMB, Congress, and the public, including the program's purpose and authority, its justification, the records it will match, and the program's start and end dates.[85]

Oriented around its matching program and agreement constructs, the CMPPA included a bevy of transparency mechanisms intended to facilitate Congressional and public tracking of that subset of inter-agency disclosures concerning, mostly, federal benefits programs. Specifically, the CMPPA stipulated that:

- A copy of each matching agreement must be made available to the public upon request and transmitted to Congress automatically. Although implementing guidance from the Office of Management and Budget (OMB) directed matching agreements to be made publicly available on a website, this requirement is not set forth in statute.
- Agencies must notify Congress and publish notice in the *Federal Register* of any matching program prior to commencing the program.

[84] Gennie Gebhart, *The FBI's Next Generation Identification System: Big Brother's Identity Database*, Electronic Frontier Found.: Deeplinks Blog (May 16, 2016), https://www.eff.org/deeplinks/2016/05/fbi-ngi-privacyact ("But for years FBI skirted the Privacy Act – instead of producing a new SORN for NGI, it relied on outdated SORNs and Privacy Impact Assessments describing very different systems.").

[85] 5 U.S.C. § 552a(o).

Setting aside the procedural and due process requirements of matching agreements, which this report addressed in sections III.B and III.C, the CMPPA's transparency requirements are due for a fresh coat of paint. CMPPA's authors clearly intended for both Congress and the public to receive actionable information about agencies' matching agreements before and during their execution, "upon request" notwithstanding. A rethinking of privacy transparency should build on the signals that the CMPPA's authors sent, but that technology available at the time was unable to implement: namely, Congress should require agencies to maintain living documentation associated with their matching agreements, such as the nature of disclosures made pursuant to the agreement, ideally collocated with information currently wrapped up in SORNs.

The E-Government Act of 2002 took another step forward in the privacy transparency journey, requiring agencies to conduct and publish Privacy Impact Assessments (PIAs) "before developing or procuring information technology" that processes personally identifiable information (PII) or "initiating a new collection of information." That law also required agencies to post their PIAs in a public forum (such as the agency's website or the *Federal Register*). PIAs were designed to require agencies to contemplate privacy risks for any "information system," supplementing the Privacy Act's SORN requirement. Specifically, PIAs document:

> (I) what information is to be collected;
>
> (II) why the information is being collected;
>
> (III) the intended use of the agency of the information;
>
> (IV) with whom the information will be shared;
>
> (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
>
> (VI) how the information will be secured; and
>
> (VII) whether a system of records is being created under [the Privacy Act]. [86]

Like SORNs and matching agreements, PIAs have been similarly reduced to compliance checkbox items, rather than functioning as the anteceding, risk-based, collaborative tool that Congress imagined them to be. For instance, a 2022 GAO report found that only a quarter of surveyed agencies "always" initiated PIAs early enough to influence system design decisions, and only half of those agencies' privacy programs were "sometimes" able to hold system owners accountable for completing PIAs.[87] Furnishing PIAs after systems have been deployed not only contravenes the E-Government Act, it neutralizes the intended effect on agency program officials.

[86] 44 U.S.C. § 3501 note.

[87] Gov't Accountability Off., *GAO-22-105065, Federal Agency Privacy Programs*, at 42 (Sept. 2022), https://www.gao.gov/assets/gao-22-105065.pdf.

Worth discussing is another shortcoming of the Privacy Act in the transparency realm: individual access. One of the Act's core innovations is providing individuals a right to access the data held on them by agencies and permitting civil enforcement of that right if agencies fail to uphold it:

> (d) Access to Records.—Each agency that maintains a system of records shall—
>
> > (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.[88]
>
> (1) Civil Remedies.—Whenever any agency
>
> > …
> > (B) refuses to comply with an individual request under subsection (d)(1) of this section;
> > …
> > the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.[89]

Even if individual Americans succeed in locating the metadata for a system of interest via the *Federal Register*, they'll need to take an additional, manual step to exercise their access right. Specifically, individuals must fill out, sign, and submit a physical or digital form containing specific information about records of interest. Moreover, that form frequently solicits from the individual information which is not easily obtainable.

For example, the Department of Interior's Privacy Act request form requires individuals to "provide the DOI bureau, office, or program that maintains the requested records, the applicable system of records notice (e.g., DOI-16, Learning Management System), and a clear description of the record(s) including date range, subject matter, place records were created, and other pertinent details."[90] Even to the most shrewd of individuals, furnishing such information would be an arduous task: for example, does the phrase "place records were created" refer to a physical space, or cyberspace? And multiply the amount of time tracking down the requisite information by the number of systems at an agency, and then by the number of agencies, and it becomes evident rather quickly that no individual can practicably ascertain the true scope of what data is held about them by the entire federal government.

---

[88] 5 U.S.C. § 552a(d)(1).

[89] 5 U.S.C. § 552a(g)(1).

[90] U.S. Dep't of the Interior, *Form DI-4016, Request for Individual Access to Records Protected Under the Privacy Act*, https://www.doi.gov/sites/default/files/di-4016-request-for-individual-access-to-records-protected-under-the-privacy-act.pdf.

Oft-overlooked is the fact that, under the Act, agencies are required to maintain an accurate accounting of most disclosures—and furnish to a requesting individual an accounting of those inter-agency disclosures involving their records:

> (c) Accounting of Certain Disclosures.—Each agency, with respect to each system of records under its control, shall—
>
> (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—
>
> (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and
>
> (B) the name and address of the person or agency to whom the disclosure is made;
>
> (2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;
>
> (3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and
>
> (4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.[91]

5 U.S.C. § 552a(c) appears to reflect Congress's intent to make individual access a dynamic right—one that enables individuals to trace how their personal information moves across the federal government, not merely to view static snapshots of agency-held data. Yet, as with access request forms for specific systems of records, there does not exist meaningful tooling for individuals to exercise their right to view disclosure accounting. At the same time, the requirement to track disclosures imposes a substantial administrative burden on agencies that would be easier to justify if individuals actually had the means to use the information those efforts produce.

The objectives of SORNs, matching agreements, PIAs, and individual access are undeniably important, but the evidence suggests that the mediums, contents, accuracy, and legibility of these tools challenge their utility—to all stakeholders. A modernized Privacy Act must look to consolidate, streamline, and better enforce its transparency provisions. In this regard, it is prudent to look across the Atlantic to another, albeit much smaller, country from which Congress may learn a thing or two.

[91] 5 U.S.C. § 552a(c).

Estonia is arguably the most advanced digital government in the world.[92] Among its many innovations is its unique approach to governmental data governance. Luukas Ilves, former Undersecretary for Digital Transformation and Government Chief Information Officer of Estonia, chronicled his country's approach in a blog post while offering several recommendations to a Congress grappling with an unprecedented data consolidation campaign:

> In Estonia every public database has a living, machine-readable schema published on RIHA, an asset catalogue of data and information systems. Anyone can see what data fields exist, why they are collected and which law authorises them. Every machine-to-machine request on Estonia's X-Road data-exchange layer must have a legal basis (that is transparently visible in RIHA and in the legal gazette). That's not bureaucracy for its own sake; it is a machine-enforced separation of powers. Legislation decides purpose, the executive runs and updates the systems and code, auditors watch the logs, with a tight coherence between what the law says and what the code does. [93]

Luukas stresses the importance of transparency mechanisms that are (1) universal (they apply to every government database, data disclosure, and data element—subject to limited exceptions); (2) publicly-available (posted on a centrally-located website and written in plain language); and (3) machine-readable (to facilitate large-scale data analysis by researchers, journalists, and others).

Mapping these principles to the Privacy Act, a revamped transparency regime should include the following features:

- Every statutory purpose maps 1:1 with a text-searchable, machine-readable, API-accessible entry in a publicly-available inventory. This entry should be created before an agency begins processing data pursuant to that purpose and subsequently updated as needed.
- Each purpose entry contains at least three core elements: (1) metadata on the purpose (including legal authorization; data elements processed and their sources, including commercially-available information (CAI); agencies with whom data is shared and relevant details of the sharing such as the specific data elements), replacing SORNs and matching agreements; (2) a living, risk-based analysis of relative privacy risk conducted by the agency Chief Privacy Officer, with opportunity for public engagement—replacing PIAs; (3) a private view with which an individual can access the data held on them and relevant disclosures for the particular purpose, better manifesting the Privacy Act tenet of individual access.
- Metadata available in the inventory is useful to the public, and practical for an agency to furnish. For instance, the average American doesn't need to know the storage location of the information systems related to the purpose, at least in any precise way, but they

[92] Mark Minevich, *What the U.S. Can Learn from Estonia's AI-Powered Digital Government*, Forbes (May 3, 2025), https://www.forbes.com/sites/markminevich/2025/05/03/what-the-us-can-learn-from-estonias-ai-powered-digital-government/.

[93] Luukas Ilves, *Why an "American Panopticon" might be a good idea* (Apr. 29, 2025), https://open.substack.com/pub/luukasilves/p/why-an-american-panopticon-might.

should have knowledge regarding to which entities an agency disseminates their information.

- Changes to the information systems involved in effectuating the purpose itself could be shipped alongside corresponding changes to its inventory entry. Such a process would result in a tighter feedback loop between the updates to the systems used by an agency and the legible information surfaced to the public.
- The Act should continue to provide individuals with legal remedies to compel agencies to publish and maintain accurate purpose inventories. (Note that enforcement is discussed further in section III.H.)

G. Adopt privacy enhancing technologies and techniques

Recommendation
Congress should require federal agencies to leverage privacy-enhancing technologies and techniques (PETs) of all shades to technically enforce its governance reforms. Several federal agencies have already piloted PETs with significant success. Congress can learn from and scale up these efforts, especially by ensuring agencies have sufficient capacity to maintain systems that leverage PETs.[94]

FIPs
Accountability, Authority, Minimization, Purpose Specification and Use Limitation, Security

Discussion
Digital technology is often rightly described as exacerbating privacy risk. For example, artificial intelligence systems built on large language models increase risk on the front-end—by scraping troves of personal information for training—as well as on the back-end—by increasing the likelihood of reidentification with a well-chosen natural language prompt.[95]

At the same time, certain technologies and techniques can also be used to enhance privacy. Such innovations are frequently referred to as PETs for short. Although advanced PETs like differential privacy, secure multiparty computation, or federated learning draw significant attention and research, and are appropriate in select contexts, they are not the only options. There is no substitute for a system architecture that embodies "privacy-by-design" principles, including by implementing basic PETs like strong access controls, flexible action permissions, de-identification techniques like encryption, robust auditing capabilities, and statistical disclosure limitation. Moreover, any organization, the federal government included, needs to flow technical architectures from robust accountability, oversight, and governance structures. And of course, organizations must ensure their privacy offices have sufficient capacity to actually deliver on the objectives set forth by leadership.

[94] For the purposes of this report, PET is acronymized to include privacy-enhancing technologies *and* techniques. Canonical acronyms tend to refer solely to technologies.

[95] Daniel J. Solove, *Artificial Intelligence and Privacy* (GWU Legal Stud. Rsch. Paper No. 2024-36; GWU L. Sch. Pub. L. Rsch. Paper No. 2024-36, 2024), https://ssrn.com/abstract=4713111.

The federal government has in recent years made strides to standardize PET usage, yet significant gaps remain. In 2022, for instance, the Biden Administration's Office of Science and Technology Policy requested public comment on a national strategy for advancing PETs, especially those that facilitate privacy-preserving data sharing and analytics.[96] The RFI was inclusive of both the public and private sectors, and it expressly invited comment on "secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic data generation tools."[97] The following year, President Biden formally defined PETs and directed federal agencies to deploy them where appropriate through Executive Order 14110 on *The Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*:

> The term "privacy-enhancing technology" means any software or hardware solution, technical process, technique, or other technological means of mitigating privacy risks arising from data processing, including by enhancing predictability, manageability, disassociability, storage, security, and confidentiality… Agencies shall use available policy and technical tools, including privacy-enhancing technologies (PETs) where appropriate, to protect privacy and to combat the broader legal and societal risks — including the chilling of First Amendment rights — that result from the improper collection and use of people's data.[98]

President Trump similarly recognizes how PETs can play an important role in accelerating the United States's leadership on artificial intelligence. The Trump Administration's AI Action Plan directs government to "build world-class scientific datasets" by implementing several recommendations, including enabling secure access to federal data while protecting confidentiality and creating "an online portal for NSF's National Secure Data Service (NSDS) demonstration project."[99]

Notwithstanding past work by the National Institutes of Standards and Technology (NIST) on research, development, and deployment of PETs, the federal government remains largely devoid of leadership on PET governance. Despite this gap, several departments and agencies have recently been experimenting with PETs to further their missions. These deployments demonstrate how, with sustained investment, the federal government could leverage PETs across agencies and contexts to improve privacy. Additionally, these case studies provide a roadmap for evaluating PETs against several criteria, including complexity of implementation and maintenance, scalability, and adaptability, to ensure the technology is fit-for-purpose.

The United States Department of Agriculture (USDA) is the federal department principally responsible for administering the Supplemental Nutrition Assistance Program (SNAP). Pursuant to this requirement, USDA conducts rigorous monitoring of improper payments. One system that USDA has built to address duplicate enrollment—where a recipient, often mistakenly, is enrolled

---

[96] Request for Information on Advancing Privacy-Enhancing Technologies, 87 Fed. Reg. 35,250 (June 9, 2022).

[97] *Id.*

[98] Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Nov. 1, 2023).

[99] Exec. Office of the President, *Winning the Race: America's AI Action Plan* (July 23, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

to receive SNAP in multiple states—is the National Accuracy Clearinghouse (NAC): an interstate data matching system that prevents duplicate issuance of SNAP benefits to an individual with a narrowly-tailored technology solution that protects personally identifiable information (privacy-preserving record linkage). From the NAC's System of Record Notice:

> The [NAC] contains the following categories of records: information on SNAP participants and applicants, SNAP case information, and match resolution information. SNAP participant and applicant names, social security numbers, and dates of birth are used by the State agencies to find a positive match. However, these identifiers are not uploaded directly to the NAC. In order to protect participant information, State agencies will use a privacy-preserving record linkage (PPRL) process to convert these data elements to a secure cryptographic hash before sharing the information to the NAC. The PPRL process allows the NAC to accurately match individuals, while preventing the collection and storage of the names, social security numbers, and dates of birth in the NAC system.[100]

According to USDA, the NAC went live in February 2024, already operates in 11 states, and all SNAP state agencies are expected to integrate with the system ahead of an October 2027 regulatory deadline.[101] The NAC and the PET it employs—PPRL—especially illustrates how, through conscientious application of technology, agencies can promote program integrity, deliver effective government services, and uphold Americans' privacy.

In the military, PETs have also yielded significant benefits. The Navy, for instance, has successfully piloted the deployment of a bespoke end-to-end encrypted (E2EE) platform that secures real-time sailor communications across 23 ships in its fleet.[102] While E2EE technology is an invaluable tool for securing communications, encryption generally is a proven approach to de-identification, especially in data storage, that agencies should consider implementing by default.

Although Congress should be rightfully hesitant about prescribing specific technologies in statute, it can and should directly contemplate how the executive branch will implement its policies using technology while it maintains a rigorous focus on outcomes. For instance, if the shift towards the purpose-centric and harm-and-risk-segmented privacy model articulated in sections III.A, III.B, and III.C of this report was not technologically practical, agencies would surely flounder.

But the case is not so. There are enough proven PETs that Congress should feel comfortable—confident even—in legislating transformative Privacy Act reform knowing a successful

---

[100] 88 Fed. Reg. 11,403 (Feb. 23, 2023).

[101] SNAP National Accuracy Clearinghouse (NAC), U.S. Dep't of Agric., Food & Nutrition Serv., https://www.fns.usda.gov/snap/nac (last visited Nov. 3, 2025).

[102] Letter from Ron Wyden, U.S. Senator, Or., & Eric Schmitt, U.S. Senator, Mo. to Robert P. Storch, Inspector Gen., Dep't of Def. (Dec. 4, 2024), https://www.wyden.senate.gov/imo/media/doc/wyden-schmitt_dod_letter.pdf ("Some DOD components have begun to pilot, on a limited basis, a potentially more secure superior communications platform, known as Matrix, which is end-to-end encrypted by default, interoperable, not controlled by any one company, and widely used by multiple NATO allies. For example, the attached presentation, provided to Congress in July, describes the Navy's successful use of Matrix, including on 23 ships.").

implementation is possible. One such PET is purpose-based access controls (PBACs): a method for determining access to data based on purpose (variants include attribute-, role-, or system-based access controls). Federal information systems governed by a rewritten Privacy Act and powered by PBACs could, in theory, have the following virtues:

- Systems' representations of purposes ("system purposes") would be mapped directly to statutory purposes and/or implementing regulations.
- System purposes share a one-to-many relationship with data assets: the subset of agency data necessary, proportionate, and limited to effectuating the purpose.
- The lifecycle of a system purpose would be equivalent to the lifecycle of the statutory purpose. Expiration of the underlying statutory purpose, for instance, would coincide with expiration of the system purpose, immediately locking down access to data.
- Instead of applying to access a data set, or an entire system, government officials (political appointees and civil servants alike) would apply for access to a system purpose.
- PBACs would be linked to robust audit logs recording what system purposes exist, which officials are assigned to those purposes, the rationale provided when applying for or granting officials access to purposes, and what processing occurs pursuant to the purpose.

Congress need not be fatalistic about technology's impact on privacy. On the contrary, PETs provide a tangible way in which the federal government can actually bolster privacy with technology and better effectuate its policy objectives. A report on adoption of PETs by New America cogently summarizes the value of PETs to federal data governance:

> As data becomes increasingly essential for effective governance, protecting privacy remains critical. Privacy-enhancing technologies (PETs) provide a means for governments to unlock the value of data while safeguarding sensitive information. By promoting innovation, fostering collaboration, and offering clear guidelines, governments can create an environment where data serves the public good without compromising privacy.[103]

To fully capitalize on the promise of PETs in government, Congress should:

1. Pass the Privacy Enhancing Technology Research Act which, among other provisions, would direct the NIST to develop a standardized decision-making framework to guide federal agencies in evaluating the use of PETs.[104]
2. Require the Office of Management and Budget (OMB) to direct agencies to pilot various PETs, especially in the context of data sharing and analysis, in parallel with NIST's development of its framework described above. Such guidance should solicit from

[103] New America, Open Technology Institute, *How to Protect Government Data with Privacy-Enhancing Technology* (2025), https://www.newamerica.org/oti/reports/how-to-protect-government-data-with-privacy-enhancing-technology/.

[104] Privacy Enhancing Technology Research Act, H.R.4755, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/4755.

agencies case studies and/or use case examples that OMB can surface on a "PET Use Case Inventory" or other centralized platform, from which other agencies can learn.[105]

3. Scale the National Secure Data Service Demonstration Project (NSDS-D), a pilot program under the bipartisan CHIPS and Science Act that President Trump has signaled his support for. The NSDS-D, assuming it leverages a privacy-protective architecture with appropriate levels of federation, could reap significant benefits for statistical research and could benefit from additional Congressional support.
4. Establish within the General Services Administration's (GSA) Technology Transformation Services a Center of Excellence (CoE) focused on PETs to support agencies through the lifecycle of technology adoption, similar to its existing CoEs for Artificial Intelligence, Cloud Adoption, and Infrastructure Optimization.
5. Support the bipartisan, bicameral Modernizing Government Technology Reform Act to reauthorize and expand the scope of GSA's Technology Modernization Fund such that it can fund projects which "enhance cybersecurity and privacy" at agencies, including, presumably, PET deployment.[106]
6. Update federal procurement policy to incentivize vendors to develop solutions that preserve privacy while retaining data utility, catalyzing innovation in the public interest.

H. Enhance enforcement

Recommendation

Congress must meaningfully enhance enforcement of the Privacy Act's requirements by:

- *Expanding civil remedies:* Congress should recognize non-pecuniary privacy harms (i.e. emotional or reputational harm) and grant courts the ability to provide equitable relief for violations of the Act, including novel forms of redress like data deletion or algorithmic disgorgement.
- *Increasing criminal penalties:* Congress should elevate the fines levied on agency officials who violate privacy laws and design new types of offenses, such as an intent to commercialize data.

FIP(s)

Accountability

[105] For inspiration, Congress could look to NIST's proposed community-driven differential privacy deployment registry as well as federal agencies' AI use case inventories required under Executive Order 13960. Gary Howarth et al., *A Community-Driven Differential Privacy Deployment Registry*, NIST Interagency Rep. 8588 (Initial Public Draft) (Nat'l Inst. of Standards & Tech., Sept. 17, 2025), https://doi.org/10.6028/NIST.IR.8588.ipd.

[106] Modernizing Government Technology Reform Act, S.3306, 119th Cong. (2025), https://www.congress.gov/bill/119th-congress/senate-bill/3306; Modernizing Government Technology Reform Act, H.R.2985, 119th Cong. (2025), https://www.congress.gov/bill/119th-congress/house-bill/2985.

Discussion

The Privacy Act establishes four distinct civil causes of action for an individual, with a two-year statute of limitations:

> (1) Civil Remedies.—Whenever any agency
>
> > (A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;
> >
> > (B) refuses to comply with an individual request under subsection (d)(1) of this section;
> >
> > (C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or
> >
> > (D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual.
> >
> > > the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection. [107]

Warranting particular focus is 5 U.S.C. § 552a(g)(1)(D), often referred to as the Privacy Act's "catch-all" cause of action and the basis for several ongoing Privacy Act suits.[108] This cause turns on the phrase "adverse effect." Under Privacy Act jurisprudence, courts have generally held that "adverse effect" encompasses a broad range of pecuniary and non-pecuniary harm (such as psychological injury, embarrassment, and emotional trauma).[109] The Supreme Court in deciding *Doe v. Chao* in 2004, for example, affirmed that "adverse effect acts as a term of art identifying a potential plaintiff who satisfies the injury-in-fact and causation requirements of Article III standing, and who may consequently bring a civil action without suffering dismissal for want of standing to sue."[110] Historically, this term of art has proved a flexible standard for plaintiffs looking to establish standing under the Privacy Act's catch-all cause of action;

---

[107] 5 U.S.C. § 552a(g)(1).

[108] *See, e.g.*, Electronic Privacy Information Center v. U.S. Office of Personnel Management, 1:25-cv-00255, (E.D. Va.) ECF 1 at 26; American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland) ECF 1 at 26.

[109] *See, e.g.*, Speaker v. HHS Ctrs. for Disease Control & Prevention, 623 F.3d 1371, 1382-83 (11th Cir. 2010); Doe v. Chao, 306 F.3d 170, 187 (4th Cir. 2002) (Michael, J., dissenting) ("The majority and I . . . also agree that emotional distress can qualify as an adverse effect."), aff'd, 540 U.S. 614 (2004).

[110] Doe v. Chao, 540 U.S. 614, 624 (2004).

nevertheless, in revisiting the Act, Congress should validate that "adverse effect" most closely reflects its intent to capture a broad range of injurious outcomes.

At the same time, a more recent decision throws *Chao* into question and poses an existential threat to much Privacy Act enforcement. Indeed, plaintiffs have had mixed success in proving standing in Privacy Act suits against the Trump Administration as that decision gets inconsistently applied by district and appellate judges.

Under the Supreme Court's decision in *TransUnion LLC v. Ramirez*, a 2021 case addressing Article III standing under the Fair Credit Reporting Act, plaintiffs bringing federal suit must now go beyond mere statutory violations in their claims.[111] Specifically, they must cite a concrete injury, defined as an injury with a "close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts."[112] To establish a concrete injury in fact in recent Privacy Act cases involving, for instance, the DOGE's access to sensitive health and financial information at the Social Security Administration, plaintiffs bringing suit have relied heavily on the tort of intrusion on seclusion as the common law analog of choice—arguments which several district courts have accepted.[113]

Some higher courts, however, have not. For example, in vacating and remanding a district court's decision to enjoin the DOGE from accessing sensitive federal personnel records, the Fourth Circuit found that the "Plaintiffs seemingly lack standing under *TransUnion*."[114]

Article III standing in Privacy Act cases under the cloud of *TransUnion* remains fraught, and barring specific clarification from the Supreme Court, or general developments in standing

---

[111] TransUnion LLC v. Ramirez, 594 U.S. 413 (2021).

[112] *Id* ("[W]ith respect to the concrete-harm requirement in particular, this Court's opinion in *Spokeo v. Robins* indicated that courts should assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts. . . . *Spokeo* does not require an exact duplicate in American history and tradition. But *Spokeo* is not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts.").

[113] *See, e.g.,* American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland) ECF 110-1 at 84 ("If receiving a single unwanted text message or phone call is sufficiently offensive to constitute concrete harm for standing purposes, in the context of intrusion upon seclusion, as several Circuits have determined, then providing the DOGE Team with access to the medical records and sensitive financial information of millions of people, if unauthorized, or without adequate need, is surely sufficiently offensive so as to constitute concrete harm. Such unrestricted access to [personally identifiable information] that SSA provided to the DOGE Team would be highly offensive to an objectively reasonable person."); ALLIANCE FOR RETIRED AMERICANS v. BESSENT, 1:25-cv-00313, (D.D.C.) ECF 42 at 29 ("Plaintiffs' alleged injury—the disclosure of their private information to third parties without a lawful right to access it—bears a close relationship to the harm essential to an intrusion upon seclusion at common law.")

[114] American Federation of Teachers v. Scott Bessent, 25-1282, (4th Cir.) ("In factual terms, Plaintiffs complain that the agencies granted unauthorized parties access to their information. And this, they argued below, bore a close relationship to the harm inflicted by the common-law tort of intrusion upon seclusion. But intrusion upon seclusion has long been understood to guard not against the disclosure of sensitive information as such, but against the feeling of unease when and where one should ideally be at peace… And without a common-law analog, Plaintiffs seemingly lack standing under *TransUnion*.").

doctrine that account for the unique nature of privacy harms, it will continue to be so.[115] The remaining discussion on remedies thus comes with a caveat: one's likelihood of success in establishing Article III standing in *any* Privacy Act suit is far from certain.

Insofar as plaintiffs could establish standing in spite of *TransUnion,* the Privacy Act prescribes varying levels of injunctive and/or compensatory relief (in the form of monetary damages) corresponding to each cause of action. With respect to injunctive relief, plaintiffs are only eligible after having exhausted administrative remedies first. Each cause of action, furthermore, is eligible for reasonable attorney fees and other litigation costs.

Cause of action (under 5 U.S.C. § 552a(g)(1))	**Relief**
(A) – an agency refuses to amend a record in accordance with an individual's request.	Injunctive – agency to amend an individual's record in accordance with their request.[116]
(B) – an agency refuses to comply with an individual's request to access their records.	Injunctive – agency must produce to the individual their records.[117]
(C) – an agency fails to accurately maintain an individual's record in such a way that leads to an adverse determination (of benefits, opportunities, etc.).	Compensatory – actual damages (minimum: $1000).[118]
(D) – an agency fails to comply with any other provision of the Act in a way that adversely affects an individual (catch-all).	Compensatory – actual damages (minimum: $1000).[119]

[115] Electronic Privacy Information Center v. U.S. Office of Personnel Management, 1:25-cv-00255, (E.D. Va.) ECF 35 at 11 ("The Court pauses to note that there is a dearth of case law on this subject—neither the parties nor the Court have found cases in this Circuit applying the common law tort of intrusion upon seclusion in similar circumstances to establish Article III standing following *TransUnion*."); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222 ("Courts struggle with privacy harms because they often involve future uses of personal data that vary widely. When privacy violations result in negative consequences, the effects are often small—frustration, aggravation, anxiety, inconvenience—and dispersed among a large number of people. When these minor harms are suffered at a vast scale, they produce significant harm to individuals, groups, and society. But these harms do not fit well with existing cramped judicial understandings of harm… Our typology of privacy harms elucidates why certain types of privacy harms should be recognized as cognizable.").

[116] 5 U.S.C. § 552a(g)(2).

[117] 5 U.S.C. § 552a(g)(3).

[118] 5 U.S.C. § 552a(g)(4).

[119] *Id.*

To receive damages under (g)(1)(C) or (g)(1)(D), an individual must demonstrate that an agency acted in an "intentional or willful" manner—a particularly formidable test. For example, negligence violations, where an agency inadvertently violates the Privacy Act, are insufficient. Several district courts have even required plaintiffs to identify the agency official who disclosed the information to meet the intentional or willful standard.[120]

Even after passing this test, barriers remain. Under *FAA v. Cooper*, the Supreme Court has interpreted actual damages to be "limited to proven pecuniary or economic harm."[121] In that case, the Court determined that Congress did not intend Privacy Act victims to recover damages for non-pecuniary harm, including mental distress, embarrassment, or emotional trauma.[122] Indeed, as evidence for its argument, the Supreme Court cited Congress's failure to act on a recommendation from the Privacy Protection Study Committee (PPSC) made decades earlier which, if implemented would have authorized general damages.[123] In its report, the PPSC wrote:

> If the rights and interests established by the Privacy Act are worthy of protection, then recovery for intangible injuries such as pain and suffering, loss of reputation, or the chilling effect on constitutional rights, is a part of that protection.[124]

It would be straightforward for Congress to clarify the Privacy Act's treatment of non-pecuniary harm. Congress could, for example, adopt the approach taken by Sen. Wyden in his Privacy Act Modernization Act of 2025, amending 5 U.S.C. § 552a(g)(4) to read "actual damages, *including nonpecuniary damages*, sustained by the individual…" (emphasis added).[125]

Although necessary, simply fine-tuning the Privacy Act's existing remedial framework is insufficient. The speed and opacity with which the DOGE in particular accessed federal information technology systems highlights the need for Congress to authorize novel forms of relief. Congress could, for instance, empower courts to grant preliminary and other equitable relief for Privacy Act violations, including injunctions against violative processing activities and orders requiring data deletion or algorithmic disgorgement modeled on Federal Trade

---

[120] *See, e.g.*, Convertino v. DOJ, 769 F. Supp. 2d 139, 146 (D.D.C. 2011) ("To meet the Privacy Act's high standard for a showing of willfulness or intentionality, [plaintiff] must know the leaker's identity. . . . [L]acking any evidence of the leaker's identity, no reasonable fact-finder could find that DOJ acted willfully or intentionally with regard to any leak in this case.").

[121] FAA v. Cooper, 566 U.S. 284 (2012).

[122] *Id* ("This parallel suggests the possibility that Congress intended the term 'actual damages' in the Act to mean special damages. The basic idea is that Privacy Act victims, like victims of libel per quod or slander, are barred from any recovery unless they can first show actual – that is, pecuniary or material – harm.").

[123] *Id* ("Although [the Privacy Protection Study Commission] later recommended that general damages be allowed, Congress never amended the Act to include them. For that reason, we held that it was 'beyond serious doubt' that general damages are not available for violations of the Privacy Act… Although we are not bound in any way by the Commission's report, we think it confirms the reasonableness of interpreting "actual damages" in the unique context of the Privacy Act as the equivalent of special damages.").

[124] Privacy Commission Report, *supra* note 12 at Appendix 4.

[125] Wyden Bill, *supra* note 15.

Commission enforcement actions.[126] Beyond equitable relief, Congress could adopt Senator Wyden's proposal to expand the Act's monetary relief from actual damages to include punitive damages, thereby deterring future violations.[127]

Authorizing equitable relief—if appropriately balanced with agencies' need to deliver programs and services—would also help ameliorate concerns about the Privacy Act's intersection with the Administrative Procedures Act (APA) evinced in recent litigation. Many Privacy Act lawsuits have relied on the APA's provision allowing suit over final agency actions "for which there is no other adequate remedy in a court" to receive the injunctive relief that the Act itself does not presently allow for.[128] This is a tenuous, brittle enforcement framework, notwithstanding its modest success.[129] The APA, put plainly, is an imperfect cause of action for redressing Privacy Act violations, particularly given the existence of the bespoke remedial framework in (g)(1).

For example, in *American Federation of Teachers v. Bessent*, several federal labor unions sued under the Privacy Act and the APA to challenge agencies' disclosures of vast amounts of personal information (including Social Security numbers, bank records, and home addresses) to officials affiliated with the DOGE. The Fourth Circuit eventually vacated the district court's order enjoining several agencies from granting the DOGE access to their information technology systems, writing:

> With its enumerated violations and details on jurisdiction, venue, and timing, the Privacy Act at least plausibly reflects Congress's intent to preclude suit under the APA in circumstances like those presented here.[130]

Put simply, courts should be able to provide equitable relief under the Privacy Act itself; Congress ought to revamp the Act's remedial scheme, specifically the relief available to the catch-all cause of action, accordingly.

Turning now to criminal penalties: the Privacy Act specifies three crimes, all categorized as misdemeanors and punishable by fines of not more than $5,000. These crimes consist of (1) unauthorized disclosure of records, (2) failure to notice a new system of records, and (3) obtaining records from an individual under false pretenses:

---

[126] Algorithmic disgorgement is "the ordered deletion of computer data models or algorithms that were developed with improperly obtained data." Joshua A. Goland, *Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC's Newest Enforcement Tool for Bad Data*, 29 Rich. J.L. & Tech. 2 (2023), https://ssrn.com/abstract=4382254.

[127] Wyden Bill, *supra* note 15 ("if the court determines that the agency acted in a manner that was intentional or willful, the United States shall be liable to the individual or person, as applicable, in an amount equal to the sum of… *(iii) punitive damages in an amount determined appropriate by the court*.") (emphasis added).

[128] 5 U.S.C. § 704.

[129] *See, e.g.,* FAA v. Cooper, 566 U.S. 284 (2012) ("The Act deters violations of its substantive provisions in other ways… possibly by allowing for injunctive relief under the Administrative Procedure Act (APA).").

[130] American Federation of Teachers v. Bessent, 8:25-cv-00430, (D. Maryland) ECF 55.

> (1) Criminal Penalties.—
> Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
>
> (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.
>
> (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.[131]

Recent events suggest that the Act's criminal penalties may be insufficient to deter agency officials from illegally disclosing data.[132] In reforming the Act, Congress should scrutinize the penalty amounts, offense classifications, and range of covered crimes. Congress could consider instituting penalties proportional to the number of records involved, individuals impacted, or severity of the offense. While a President could pardon agency officials who commit Privacy Act crimes, strengthened criminal penalties would nonetheless help deter malicious executive branch officials from abusing Americans' privacy.

Indeed, in 2011 U.S. Senator Daniel K. Akaka introduced the Privacy Act Modernization for the Information Age Act of 2011 to, among other changes, "strengthen [the Privacy Act's] civil and criminal penalties" and "add penalties for using private agency records for commercial gain and upgrade the penalty for obtaining records from an agency under false pretenses to a felony."[133] Specifically, Sen. Akaka's bill would penalize any unlawful record disclosure that was done for "commercial advantage, personal gain, or malicious harm."[134]

---

[131] 5 U.S.C. § 552a(i).

[132] Teddy Schleifer & Daniel Lippman, *Trump's DOGE Got Access to Social Security Data. Experts Say That May Be Illegal*, Politico (Jan. 20, 2026), https://www.politico.com/news/2026/01/20/trump-musk-doge-social-security-00737245 ("Two members of Elon Musk's DOGE team working at the Social Security Administration were secretly in touch with an advocacy group seeking to "overturn election results in certain states," and one signed an agreement that may have involved using Social Security data to match state voter rolls, the Justice Department revealed in newly disclosed court papers.").

[133] Press Release, S. Comm. on Homeland Sec. & Governmental Affairs, Subcomm. on Oversight of Gov't Mgmt., *Senator Akaka Introduces Bill to Modernize the Privacy Act* (Oct. 18, 2011), https://www.hsgac.senate.gov/subcommittees/OGM/majority-news/subcommittees-oversight-of-government-management-majority-media-senator-akaka-introduces-bill-to-modernize-the-privacy-act/.

[134] Akaka Bill, *supra* note 16.

Congress ignored Sen. Akaka at its peril. While the DOGE—run for a time by billionaire Elon Musk and staffed by officials with direct ties to him (including dual employment at least one of his companies)—was pillaging agency information technology environments, outside experts were growing increasingly concerned that the sensitive data they were accessing would be used to train commercial AI models.[135]

I. Collocate privacy oversight in the legislative branch

Recommendation
To ensure independent oversight of executive branch privacy activities, Congress should either establish a new legislative branch oversight entity or expand the role of the Government Accountability Office. This entity should have specialized powers related to privacy, including authority to receive automated system telemetry (logs, usage metadata, notice of data outflows) and issue non-binding legal opinions on prospective privacy risks or retrospective harms. Operating independently from the executive branch, it would collaborate directly with Congress and agency officials. Additionally, Congress could subsume the Privacy and Civil Liberties Oversight Board—currently an executive branch agency focused on balancing counterterrorism with privacy and civil liberties—under its new entity to centralize independent privacy expertise.

FIP(s)
Accountability, Transparency

Discussion
To ensure independent accountability of even the most aggrandizing of presidential administrations, Congress must rethink how it designs oversight structures This need is as pronounced in government privacy as it is in other policy areas.

Recent actions by the executive branch are shifting the formerly stable ground upon which the modern administrative state was built. Historically independent agencies, bodies, and officials are being dismantled, dissolved, and fired without cause, shattering longstanding norms and precedents. For example:

- Just days into President Trump's second term, he fired seventeen Inspectors General (IGs), violating the statutory requirement to notify Congress thirty days prior to removal.[136]
- Shortly after, President Trump unlawfully fired the Democratic members of the Privacy and Civil Liberties Oversight Board (PCLOB), the federal watchdog over counter-

[135] Thomas Germain, *DOGE Threat: How Government Data Would Give an AI Company Extraordinary Power*, Gizmodo (Feb. 21, 2025), https://gizmodo.com/doge-threat-how-government-data-would-give-an-ai-company-extraordinary-power-2000573609.

[136] Farnoush Amiri & Mary Clare Jalonick, *Trump Fires More Than a Dozen Inspectors General in Middle of Night. Congress Says It's Unlawful*, Associated Press (Jan. 24, 2025), https://apnews.com/article/trump-inspectors-general-fired-congress-unlawful-4e8bc57e132c3f9a7f1c2a3754359993.

terrorism activities that impact Americans' privacy. These officials were later reinstated following a legal challenge, but their status on the PCLOB remains tenuous.[137]

- In March 2025, President Trump unlawfully fired two Democratic Commissioners of the Federal Trade Commission.[138]
- In June 2025, President Trump removed and replaced the Department of Education's Acting Inspector General after she reported to Congress that her office had "experienced unreasonable denials and repeated delays" from administration officials in response to information requests.[139]

The current Supreme Court's likely response to these actions—reversing *Humphrey's Executor*, the 90-year-old precedent affirming Congress's right to limit the removal of executive branch officials, and, in general, manifesting the dubious constitutional theory of the "unitary executive"—will functionally erase the independence of oversight bodies that reside in the executive branch, including agency IGs and the PCLOB. [140]

To ready itself for a world in which the independence of executive branch entities cannot be guaranteed, Congress must begin collocating oversight capacity in the legislative branch. A modernized Privacy Act provides fertile ground to experiment with this approach in the context of federal privacy. Specifically, Congress must design novel structures, increase its technical capacity, and appropriate significant resources—to itself—in order to support its oversight responsibilities of the Privacy Act and related laws. That said, although establishing an organizational framework is a necessary step, it is by no means sufficient. In parallel, Congress must legislate particular technical architectures that facilitate oversight of the executive branch's privacy activities.

The process by which Congress currently obtains information from the executive branch is asynchronous and anachronistic. To draw a caricature: Congress initiates an information request to an executive branch agency; days, if not weeks, pass; further correspondence to clarify the scope of the request commences; and information is ultimately furnished that is outdated, incomplete, or otherwise unactionable. Combine these ad-hoc information requests that are easily stymied by a recalcitrant agency with Congress's other, similarly-ineffectual transparency tool of choice—statutorily-required reports that routinely go unread—and you are left with a model of oversight that is no longer fit for purpose.

---

[137] Camille Caldera, *Judge Overturns Firing of Democrats on Intelligence and Privacy Oversight Body*, Nextgov (May 9, 2025), https://www.nextgov.com/people/2025/05/judge-overturns-firing-democrats-intelligence-and-privacy-oversight-body/405505/.

[138] Jacob Knutson, *Trump Fires Democratic FTC Commissioners*, Axios (Mar. 18, 2025), https://www.axios.com/2025/03/18/trump-fires-democratic-ftc-commissioners.

[139] Erich Wagner, *Two Independent Watchdogs Quietly Replaced by Trump*, Gov't Executive (July 11, 2025), https://www.govexec.com/oversight/2025/07/two-independent-watchdogs-quietly-replaced-trump/407073/.

[140] Holland & Knight LLP, *Supreme Court's Potential Restructuring of FTC* (Sept. 2025), https://www.hklaw.com/en/insights/publications/2025/09/supreme-courts-potential-restructuring-of-ftc; Nina Totenberg, *Supreme Court Appears Poised to Vastly Expand Presidential Powers*, NPR (Dec. 8, 2025), https://www.npr.org/2025/12/08/nx-s1-5626876/supreme-court-trump-ftc-unitary-executive.

Modern technology enables a fundamentally different approach: namely, a future in which the feedback loop between executive branch operations and legislative branch oversight is automated, real-time, and exhaustive. Most information systems built today keep robust audit logs, creating comprehensive digital paper trails that are then, generally speaking, dumped in a centralized location for future analysis. Known to those in the software industry as "telemetry," these in-situ logs serve many purposes. For instance, they prove vital when a system suffers an incident, allowing engineers to retrace the flow of data through a system to debug what went wrong and implement a fix.

It is not difficult to imagine Congress mandating that for high-risk data processing, relevant telemetry be transmitted to a legislative branch repository in a secure, encrypted, and privacy-preserving fashion. Technologically speaking, this requirement would be straightforward to implement. Furthermore, telemetry subject to executive privilege, classification, or other statutory requirements could be trivially filtered out before transmission.

In fact, there is precedent for government-wide logging policy. In 2021, the Office of Management and Budget (OMB) issued M-21-31, which describes logs that agencies must capture as well as required retention times to facilitate prevention and response to cybersecurity incidents. OMB further directs agencies to, upon request, furnish their centralized logs to the Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation.[141]

To complement centralized telemetry tooling, Congress should stipulate other measures that enable oversight fit for the digital age. Among these include the ability for Congress to obtain read-only "audit" accounts that provide more direct access to requested systems; make agency officials available for interviews within a specified timeframe; and collocate legislative branch oversight officials within agencies for the duration of investigations.

With an effective architecture for digital fact-finding in place, Congress could empower a novel investigative unit—as a standalone entity or an outgrowth of its Government Accountability Office (GAO)—focused on overseeing the privacy practices of executive agencies. To consolidate resources, Congress could subsume under this office the PCLOB, including its statutory responsibilities and accompanying resources. After all, a unitary executive would hardly allow a PCLOB to produce recommendations that cut against his objectives: better for Congress to incorporate the PCLOB into its own oversight apparatus, appropriations and all.

Such an idea may sound radical, but is hardly a departure from precedent. In fact, Congress has already contemplated the role of the Comptroller General, and by extension the GAO, in privacy oversight (albeit in a world where big data systems were non-existent). Specifically, Congress through the Privacy Act and later the Computer Matching and Privacy Protection Act delegated to the GAO significant oversight authorities, including, respectively, (1) an exception from the consent-based disclosure requirement and (2) a stipulation "that the Comptroller General may

[141] Office of Mgmt. & Budget, Exec. Office of the President, *M-21-31, Memorandum for the Heads of Executive Departments and Agencies: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (Aug. 27, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

have access to *all* records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the [matching] agreement" (emphasis added).[142]

Importantly, Congress could endow its novel privacy office with specialized oversight and quasi-adjudicatory powers, building on GAO's existing bid protest authority. For example, the office could issue non-binding legal opinions on whether an agency has correctly assigned a risk and harm level to a particular purpose. Such opinions could be triggered when a sufficient number of impacted individuals petition for review, with specific thresholds defined by statute. From an investigatory standpoint, the office could leverage Congress's existing subpoena authority—though in a world of abundant telemetry, such compulsory legal tools would ideally be seldom used. So long as the office is not vested with authorities that legally elevate it to an executive agency, its placement in the legislative branch would be consistent with Congress's Article I powers.

J. Resource Chief Privacy Officers

Recommendation

Congress should establish and resource a Chief Privacy Officer (CPO) at every agency.[143] Each CPO should own their agency's privacy program, report directly to the head of their agency, and possess a requisite background in law and technology. CPOs should collaborate closely with Chief Information Officers (CIOs) to advance agencies' missions while balancing privacy considerations. Moreover, the CPO should report regularly to Congress (including the new legislative branch oversight entity described in section III.I) and the public on the agency's privacy activities and conduct investigations—as needed—in concert with the Inspector General. The CPO should supplant the Senior Agency Official for Privacy, a position born of executive fiat and inconsistently staffed across agencies. Moreover, CPOs should obviate the need for Data Integrity Boards: bureaucratic creatures that lack demonstrable value. Finally, to facilitate interagency privacy policy and enhance government-wide privacy leadership, Congress should establish a Federal CPO position within the Office of Management and Budget, similar to the Federal CIO, and constitute a CPOs Council to replace the Federal Privacy Council.

FIP(s)

Accountability

Discussion

The Constitution vests Congress with authority to establish, structure, and reorganize federal agencies as it deems necessary. Accordingly, Congress has directed agencies to staff many C-suite positions with ownership over vital agency functions, including the Chief Financial Officer (CFO), the Chief Information Officer (CIO) and the Chief Human Capital Officer.

[142] 5 U.S.C. § 552a(b)(10); 5 U.S.C. § 552a(o)(1)(K).

[143] For the purposes of this recommendation, the term "agency" refers to the 24 Chief Financial Officer (CFO) Act agencies.

To the extent that privacy is as critical an agency function as cybersecurity or financial management, agencies ought to have a designated official for whom it is their principal focus: a Chief Privacy Officer (CPO). However, the Privacy Act does not require agencies to establish a privacy office or appoint a CPO. The Privacy Protection Study Committee (PPSC) identified this leadership gap early on in the Act's implementation, writing in its final report:

> In order to provide for more effective implementation of the [Privacy Act], the Commission believes that the head of each agency should designate one official with authority to oversee implementation of the Act. The official's responsibilities would include issuing instructions, guidelines, and standards, and making such determinations, as are necessary for the implementation of the Act. He would also be responsible for taking reasonable affirmative steps to assure that all agency employees and officials responsible for the collection, maintenance, use and dissemination of individually identifiable records are aware of the requirements of the Act.[144]

In the succeeding decades following the PPSC's unimplemented recommendation, federal privacy leadership evolved with minimal Congressional intervention. That is, until the 2000s, when escalating investments in domestic surveillance following 9/11 spurred Congress to safeguard Americans' civil liberties, especially privacy:

- In the Homeland Security Act of 2002, Congress established within the Department of Homeland Security (DHS) the federal government's first statutorily-required Privacy Office and a CPO to lead it. Among the DHS CPO's responsibilities are "assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices," "conducting a privacy impact assessment of proposed rules," and "preparing a report to Congress on an annual basis on activities of the Department that affect privacy."[145]
- In 2004, through the Intelligence Reform and Terrorism Prevention Act of 2004, Congress established in the executive branch the notionally-independent Privacy and Civil Liberties Oversight Board (PCLOB) to, *inter alia*, "ensure that privacy and civil liberties are appropriately considered in the development and implementation" of policies designed to protect the nation from terrorism. [146]
- In the FY2005 omnibus appropriations package, Congress directed each "agency" to "acquire a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy."[147] However, there are conflicting interpretations regarding the scope of this provision, particularly after its codification at 42 U.S.C. § 2000ee-2: at least some experts believe it should be read to cover only those agencies funded by the particular division in the appropriations bill (i.e. those within the Departments of Transportation

[144] Privacy Commission Report, *supra* note 12 at Appendix 4.

[145] Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135 (Nov. 25, 2002).

[146] Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004).

[147] Pub. L. No. 108-447, 118 Stat. 2809 (Dec. 8, 2004).

and Treasury, and a slew of independent agencies), and didn't necessarily require the establishment of a new privacy office or position at every federal agency.[148]

- Through the Violence Against Women and Department of Justice Reauthorization Act of 2005, as amended, Congress required the Attorney General to designate a senior official in the Department of Justice to assume primary responsibility for privacy policy.[149]
- In 2007, Congress granted DHS's CPO new investigative authorities, including the ability to issue subpoenas to private entities to compel the production of pertinent information.[150]

Consequential changes to federal privacy leadership also resulted from executive action. The Bush Administration, for instance, went further than Congress did in the Consolidated Appropriations Act 2005 passed just months prior, directing *every* department and agency to identify a Senior Agency Official for Privacy (SAOP).[151] Then, in 2016, President Obama issued Executive Order 13719, *Establishment of the Federal Privacy Council*, in which he established the Federal Privacy Council as the "principal interagency forum to improve the Government privacy practices of agencies."[152]

Despite all of these positive developments, federal privacy leadership remains lacking. For example, the Government Accountability Office (GAO) in 2022 found that although each of the 24 CFO Act agencies had designated a SAOP, most of those officials did not have privacy as their primary responsibility. Moreover, at least some of these SAOPs lacked any background in information technology whatsoever: arguably a prerequisite for effective oversight of privacy practices in today's digital age:

> The 24 [CFO Act] agencies have each designated a senior agency official for privacy. However, most of these officials do not have privacy as their primary responsibility and have numerous other duties relating to, for example, managing IT and information security…Other designated SAOPs included officials such as the agency Chief Administrative Officer, Deputy Assistant Secretary for Operations, Deputy Assistant Secretary for Global Information Services, Assistant Secretary for Management, General Counsel, and Acting Deputy Administrator. By contrast, few agencies had assigned the role of SAOP to an official whose primary duties were privacy-related.[153]

---

[148] Harold C. Relyea, *Privacy Protection: Mandating New Arrangements to Implement and Assess Federal Privacy Policy and Practice*, Cong. Rsch. Serv., Order Code RS21851 (July 27, 2005), https://www.justice.gov/file/267796/dl?inline= ("Located in Title V of the division, the requirements of the section appeared to be applicable only to agencies directly funded by the division. Furthermore, it did not appear that the section created new positions, but instead prescribed privacy officer responsibilities to be assigned to an appropriate individual in an existing position.").

[149] Pub. L. No. 109-162, § 1174, 119 Stat. 2960, 3124 (Jan. 5, 2006).

[150] Pub. L. No. 110-53 § 802, 121 Stat. 266 (Aug. 3, 2007).

[151] Office of Mgmt. & Budget, Exec. Office of the President, *Memorandum M-05-08, Designation of Senior Agency Officials for Privacy* (Feb. 11, 2005), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-08.pdf.

[152] Exec. Order No. 13,719, 81 Fed. Reg. 7687 (Feb. 9, 2016).

[153] *GAO-22-105065 Federal Agency Privacy Programs*, Gov't Accountability Off. at 42 (Sept.

Like the PPSC 40 years before, GAO recommended in its report that Congress "consider legislation to designate a senior privacy official, such as a chief privacy officer, at agencies that currently lack a position." Furthermore, GAO highlighted several aspects that would make such a directive impactful for agency privacy practices, including that the CPO "should have privacy as its primary duty, the organizational placement necessary to coordinate with other agency functions and senior leaders, and the authority to ensure that privacy requirements are implemented and privacy concerns are elevated to the head of the agency."[154]

GAO's observations align with concerns raised by privacy practitioners with direct oversight experience. As one PCLOB Member noted, current privacy officials "often lack the tools to oversee the full range of privacy issues," and many serve in part-time capacities with numerous other responsibilities. [155] The CPO position must be a full-time role with privacy as its primary and sole responsibility. Congress should prohibit the assignment of privacy responsibilities to officials serving in multiple capacities or to offices buried deep within organizational hierarchies. For instance, agencies should not follow the problematic model where a senior privacy officer simultaneously handles compliance, ethics, contracting, asset forfeiture, and privacy—a structure that inevitably dilutes privacy governance.

Beyond structural placement, the nature of the CPO's work must reflect modern realities. The CPO's responsibilities must extend beyond compliance activities to encompass proactive engagement in agency policymaking, operations, and procurement. Accordingly, the CPO should possess demonstrated expertise in privacy law, information technology, and policy development. CPOs should be consulted during the development of new programs, operational decisions, and policy initiatives that may impact privacy, not merely after implementation. This is particularly critical when agency CIOs are evaluating or deploying emerging information technologies like artificial intelligence. Properly empowered CPOs can prevent privacy violations before they occur—for example, by conducting initial privacy assessments of information systems before deployment and identifying when agency practices may, for instance, violate the Privacy Act's prohibition on processing records related to individuals' First Amendment-protected activities.[156] This role would position the CPO as both a facilitator of the agency's mission and an advocate for proper treatment of Americans' personal information consistent with the Privacy Act and other statutes.

In the same way that the legislative branch oversight entity described in section III.I must have adequate capacity to be successful, effective privacy oversight by an agency CPO also requires resources. Congress should mandate minimum staffing levels for CPO offices proportional to agency size and data processing activities. Experience demonstrates that privacy offices with

---

2022), https://www.gao.gov/assets/gao-22-105065.pdf.

[154] *Id.*

[155] Travis LeBlanc, *It is time for federal chief privacy officers*, The Hill (Feb. 12, 2021), https://thehill.com/blogs/congress-blog/politics/538571-it-is-time-for-federal-chief-privacy-officers/?rl=1.

[156] 5 U.S.C. § 552a(e) ("Each agency that maintains a system of records shall… (7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.").

only one or two personnel cannot provide comprehensive oversight across an entire agency—a reality that leads to delayed investigations and incomplete assessments. Appropriations committees should establish dedicated budget lines for CPO offices to prevent under-resourcing that impedes effective implementation.

In the 118th Congress, the bipartisan Federal Information Security Modernization Act of 2024 took an important step towards implementing the recommendations outlined in this subsection. Specifically, this bill would have resolved any doubt about the applicability of the Consolidated Appropriations Act, 2005's requirement that every federal agency must designate a CPO.

> "(j) (1) Notwithstanding paragraphs (2) and (3) of subsection (a), the head of each agency shall, in accordance with section 522(a) of division H of the Consolidated Appropriations Act, 2005 (42 U.S.C. 2000ee–2), designate a Chief Privacy Officer with the necessary skills, knowledge, and expertise, who shall have the authority and responsibility to—
>
> > "(A) lead the privacy program of the agency; and
> >
> > "(B) carry out the privacy responsibilities of the agency under this chapter, section 552a of title 5, and guidance issued by the Director.
>
> "(2) The Chief Privacy Officer of each agency shall—
>
> > "(A) serve in a central leadership position within the agency;
> >
> > "(B) have visibility into relevant agency operations; and
> >
> > "(C) be positioned highly enough within the agency to regularly engage with other agency leaders and officials, including the head of the agency.[157]

Borrowing language from the FISMA of 2024, a modernized Privacy Act should clarify Congressional intent with respect to privacy leadership, ensuring every agency has installed under its head a CPO. Moreover, Congress should consider going even further, granting some or all of these agency executives authorities of the sort enjoyed by DHS's CPO.

By codifying a strong CPO at every agency, and funding them, Congress could obviate other bureaucratic structures whose value is dubious. For example, the SAOPs previously discussed could instantly be eliminated. But Congress could be even more forceful in its procedural simplification: dissolving Data Integrity Boards (DIBs). Noted Privacy Act expert Robert Gellman articulates the case against DIBs most effectively:

> One of the controls in the Privacy Act comes from Data Integrity Boards (DIB). The Privacy Act requires each agency involved in matching to establish a DIB to review and approve matching activities. It is not apparent that the DIBs remain useful, if they ever were. At some agencies, the approval process is a "paper" activity, with matching

[157] Federal Information Security Modernization Act of 2024, H.R. 4552, 118th Cong. (2023).

> agreements circulated for signature rather than for discussion at a DIB meeting. That process has little value because each office involved in matching simply approves what another office proposes so that its own matching activity will be approved. There is no tension or incentive for serious review. There is no evidence that the role of DIBs expanded into other privacy areas. As a result, there is no good reason to continue DIBs.[158]

By clearing out the kludge, Congress can make way for purpose-fit structures, including those that facilitate interagency privacy policy and enhance government-wide privacy leadership. It could even consider, for example, reviving Sen. Akaka's idea for a Federal CPO, translating an agency-level tool into a government-wide one; there's precedent for such a position in the Federal Chief Information Officer.[159]

Additionally, Congress could establish a CPOs Council that meets regularly to address common challenges, share best practices, and develop coordinated approaches to emerging privacy risks, including from those exacerbated by artificial intelligence. The CPOs Council could supplant the Federal Privacy Council created via executive order, and Congress could model it on the CIOs Council.[160] But Congress wouldn't even need to model, it could copy: Sen. Akaka in his Privacy Act for the Information Age Act also proposed a CPOs Council chaired by his Federal CPO.[161]

[158] Gellman Report, *supra* note 18, at 129.

[159] Akaka Bill, *supra* note 16.

[160] 44 U.S.C. § 3603.

[161] Akaka Bill, *supra* note 16.

V. Conclusion

When Senator Sam Ervin introduced the Privacy Act in 1974, he emphasized that effective privacy protection would "require foresight and an ability to forecast the possible trends in information technology."[162] This report attempts to channel that very spirit, proffering reforms that address urgent challenges and forestall problems on the horizon, driven especially by artificial intelligence. It operates proudly at the edge of what's technologically possible.

The ten recommendations presented in this report would fundamentally transform governmental privacy. Collectively, they would shift the Privacy Act's regulatory model from being system-centric to purpose-centric; from uniform requirements to risk-based protections; and from a focus on procedural compliance to an emphasis on substantive privacy safeguards. The recommendations would also streamline and consolidate transparency mechanisms, employ modern technologies and techniques to complement novel governance structures, and establish meaningful oversight insulated from executive branch influence.

The transition from recommendations to legislation necessarily begins with deliberation. This report is intended to facilitate bipartisan and bicameral engagement on comprehensive Privacy Act reform. The proposals reflect contributions from members of both political parties, draw on prior legislative efforts in both chambers, and incorporate perspectives from a broad range of stakeholders. They build on earlier initiatives, including Senator Akaka's 2011 proposal, Senator Wyden's 2025 bill, bipartisan efforts to modernize the Federal Information Security Modernization Act, and the proposed bipartisan reauthorization of the Technology Modernization Fund. Privacy protection is not a partisan concern; lawmakers across the political spectrum have expressed shared interests in preventing government overreach while ensuring effective service delivery.

Actions by the current administration underscore, but do not themselves motivate, the need for reform. When officials acting under ambiguous legal authority can access large volumes of tax, health, and financial data with limited oversight, the Privacy Act's protections are insufficient. When agencies consolidate sensitive information across systems pursuant to executive directives of uncertain legal basis, statutory safeguards are inadequate. When individuals lack meaningful avenues for redress following privacy violations, the Act's requirements are reduced to mere words on paper.

These outcomes, however, are not inevitable. The federal government can responsibly leverage data while maintaining robust privacy protections. Agencies can apply strong data minimization principles while retaining information necessary to carry out their missions. Congress can establish effective oversight mechanisms that respect both individual rights and legitimate mission requirements. Privacy protection and effective governance are complementary objectives, not competing ones.

The 93rd Congress enacted the Privacy Act in response to the abuses revealed by Watergate and the rise of computerized information systems. The 119th—and, soon, the 120th—Congress now

[162] Privacy Source Book, *supra* note 13.

faces a comparable responsibility to address emergent challenges by the executive branch and sea changes in the modern information technology environment headlined by artificial intelligence. This report provides a roadmap for that effort. The work of translating these recommendations into legislation, and ultimately into law, must now begin—without delay.