epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

CONGRESSWOMAN LORI TRAHAN

On Efforts to Reform Privacy Act of 1974 and Protect Americans' Data from Government Abuse

---

The Electronic Privacy Information Center (EPIC) submits these comments in response to Congresswoman Lori Trahan's March 18, 2025, request for information on modernizing the Privacy Act of 1974.[1] EPIC applauds Congresswoman Trahan for taking steps to protect Americans' privacy and constitutional rights against current and future abuses. As Congresswoman Trahan accurately notes, Americans' privacy and data security are being challenged in unprecedented ways by illegal government overreach. The Privacy Act of 1974 is a crucial piece of the framework limiting the government's power over individuals' personal information. However, aspects of the Privacy Act have become outdated due to technological advances and increasingly ineffective in the face of deliberate agency defiance. EPIC strongly supports amending the Act to limit its disclosure exceptions, to establish standards for personnel that handle systems of records, and to address the risks posed by emerging technologies. EPIC further stresses that Congress must ensure that agencies are adequately funded and staffed to implement privacy protections for decades to come.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has a particular interest in ensuring privacy, accountability, and the protection of civil liberties and civil rights with respect to the government's use of personally identifiable information. The Privacy Act is fundamental to protecting Americans' personal information from dangerous overreach and abuse by the federal government. EPIC has a long history of advocating for the Act's improvement and leveraging the Act to protect privacy against abuses.[3]

---

[1] Congresswoman Lori Trahan, *Privacy Act RFI* (Mar. 18, 2025), https://trahan.house.gov/uploadedfiles/final_trahan_privacyactrfi.pdf.
[2] EPIC, *About Us*, EPIC.org, https://epic.org/about/.
[3] *See, e.g.*, PRESS RELEASE: EPIC, Democracy Forward, and Federal Worker Sue DOGE for Illegal Seizure of Personal Data from Treasury, Personnel Systems (Feb. 10, 2025), https://epic.org/press-release-epic-democracy-forward-and-federal-worker-sue-doge-for-illegal-seizure-of-personal-data-from-treasury-personnel-systems/.

I. Strong Privacy Protections Are Needed to Ensure That Government Data Practices Serve Rather than Harm Americans.

EPIC calls attention to two primary concerns regarding the federal government's collection, maintenance, use, and dissemination of personal information. First, and most pressing, the federal government's collection and use of personal information creates conditions for significant government overreach and abuse of personal information. Second, the government's procurement and implementation of AI systems are rife with opportunities for privacy abuses. Congress can mitigate these harms by directing the development and adoption of privacy-enhancing technologies (PETs), including differential privacy.

a. Government systems of records are susceptible to privacy abuses and agency overreach.

The federal government collects and stores vast quantities of personal information, generally defined as "records" under the Privacy Act, in the course of carrying out its executive agency functions. Sensitive data from nearly every American citizen, and millions of noncitizens, is stored in one or more of the federal government's information systems. This includes Social Security numbers, financial information, health information, employment records, tax records, address records, and more.

The authors of the Privacy Act worried that a single institution could one day assemble a detailed dossier on any person.[4] They noted that the government's capacity for information-based tyranny was growing rapidly and that the government could commit (and was committing) "flagrant violations of the constitutional rights" of its people based on the personal information it collected.[5] There was bipartisan agreement that safeguards were urgently needed to avoid misuse and preserve the confidence the American people had placed in its government.

The 93rd Congress was right to be concerned. By combining the information held in government systems, a single official or agency can create a detailed snapshot of any person's life. These databases may contain a combination of outdated, inaccurate, and true pieces of information. If such details are shared or otherwise misused, a person's access to employment, housing, education, and other critical services can be undermined.[6] When safeguards against misappropriation and abuse are removed or ignored, agencies are more prone to dangerous mission creep.[7] Further, bad actors inside or outside of the government may combine the information held by different federal agencies in ways that threaten significant harm. For example, officials could combine federal databases to improperly identify and track individuals

---

[4] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 759-761 (1976).
[5] *Id*. at 905-906.
[6] *See* Barry Friedman & Danielle Keats Citron, *Indiscriminate Data Surveillance*, 110 VA Law Rev. 1351, 1351 (2024). *See also*, Danielle Keats Citron, *A More Perfect Privacy*, 104 Boston U. Law Rev. 1073, 1073 (2024).
[7] Mission creep occurs when an agency broadens the use of an information system or its data over time, despite the purpose of the original collection.

or wrongfully limit their ability to obtain benefits, receive tax refunds, or bid on government contracts. This kind of access not only chills free speech and association rights guaranteed under the First Amendment but also invites flagrant violations of due process and Fourth Amendment rights.

The DOGE's activities since President Trump's inauguration perfectly capture the stakes of government overreach and abuse of personal information. Donald Trump was inaugurated on January 20, 2025. That same day, President Trump issued an executive order to create the DOGE in the Executive Office of the President.[8] Despite confusion surrounding the DOGE's leadership, in practice the agency appears to be led by Elon Musk, a temporary federal employee whose ownership stakes in large commercial enterprises regulated by multiple federal agencies present towering conflicts of interest. Since the DOGE's creation, its personnel have sought and obtained unprecedented access to information systems at numerous government agencies, including the Office of Personnel Management,[9] the Department of Education,[10] the Treasury Department,[11] and Centers for Medicare and Medicaid Services.[12] In other cases, through the efforts of dedicated civil servants and civil society, the DOGE has been denied or stripped of access critical systems, including those maintained by the Internal Revenue Service[13] and the Social Security Administration.[14]

By virtue of the access it has gained, the DOGE has been able to amass incredible amounts of sensitive personal information. The full sweep of its activities at federal agencies remains unclear, making it difficult to understand the precise scope of the DOGE's information access. However, it is known that the DOGE has accessed records that paint an intimate portrait of a person's life, such as social security numbers, financial records (including information on taxes and loans), and detailed health and employment records. All in all, the DOGE has accessed records containing the personal information of tens of millions of individuals.

---

[8] Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 20, 2025).
[9] Lea Skine, *Judge Blocks DOGE From Accessing Sensitive Information at US Agencies*, Associated Press (Mar. 24, 2025), https://apnews.com/article/doge-access-education-treasury-office-personnel-management-b925e2b6b6326dab1dffc49d6c6c2b58.
[10] Hannah Natanson, Gerrit De Vynck, Elizabeth Dwoskin, & Danielle Douglas-Gabriel, *Elon Musk's DOGE Is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025), https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/.
[11] Lea Skine, *Judge Blocks DOGE From Accessing Sensitive Information at US Agencies*, Associated Press (Mar. 24, 2025), https://apnews.com/article/doge-access-education-treasury-office-personnel-management-b925e2b6b6326dab1dffc49d6c6c2b58.
[12] Anna Wilde Mathews & Liz Essley Whyte, *DOGE Aides Search Medicare Agency Payment Systems for Fraud*, The Washington Post (Feb. 5, 2025), https://www.wsj.com/politics/elon-musk-doge-medicare-medicaid-fraud-e697b162.
[13] Laurel Wamsley, *The Government Already Knows a lot About You. DOGE Is Trying to Access All of It*, NPR (Mar. 11, 2025), https://www.npr.org/2025/03/11/nx-s1-5305054/doge-elon-musk-security-data-information-privacy.
[14] Tierney Sneed, *DOGE Blocked From Accessing Sensitive Social Security Data, After Judge Raises Concerns of a 'Fishing Expedition*.' CNN (Mar. 20, 2025), https://www.cnn.com/2025/03/20/politics/social-security-doge-fishing-expedition/index.html.

Although the DOGE has secured unprecedented access, its personnel are frequently not trained or cleared to handle the information contained in federal systems. For example, in her order blocking the DOGE's access to Social Security data, U.S. District Court Judge Ellen Hollander found that staffers were granted system access before background checks were completed.[15] This included access to the SSA's master data warehouse, which contains "extensive information about anyone with a social security number."[16] This is far from the only example. Other DOGE personnel, many of whom have no prior government experience, can now view and in some cases alter federal information systems despite questions about their security clearances and cybersecurity practices.[17]

Moreover, the federal government risks losing all control over the personal information accessed by the DOGE if it is allowed to flow from person to person and agency to agency without meaningful limit. For example, a DOGE employee emailed a spreadsheet with personally identifiable information to other federal employees outside the agency that maintained the records.[18] And in considering a lawsuit brought by federal employee unions against the DOGE, Judge Vargas found it likely that sensitive information had already been shared outside of the defendant agency.[19] In another case, government attorneys could not account for the DOGE's actions concerning the records they had accessed.[20]

The actions of DOGE personnel and the agency personnel who have granted them database access reflect a systematic disregard for the Privacy Act. Agencies have provided unlawful access to sensitive and protected data and have allowed that data to be used for purposes that have no connection to the original purposes for which the information was collected. In one egregious example, DOGE employees marked approximately 4 million still-

---

[15] *AFL-CIO v. Social Security Admin.*, No. ELH-25-0596 at 31 (D. MD. Mar. 30, 2025), https://www.documentcloud.org/documents/25868348-afscme-v-ssa-memorandum-order/#document/p33/a2629341.

[16] *Id*. at 30.

[17] *See, e.g.*, Zack Whittaker, *The Biggest Breach of US Government Data is Under Way*, TechCrunch (Feb. 7, 2025), https://techcrunch.com/2025/02/07/doge-biggest-breach-of-united-states-government-data-under-way/. *See also*, Sen. Mark Warren, et al., Letter to White House Chief of Staff Susan Wiles (Feb. 5, 2025), https://www.warner.senate.gov/public/index.cfm/2025/2/release-senate-intelligence-members-sound-the-alarm-about-doge-risk-to-national-security-and-american-privacy (letter from Senate Intelligence members seeking information on DOGE's access to federal intelligence information); Vittoria Elliott, *'It's a Heist: Real Federal Auditors Are Horrified by DOGE*, WIRED (Mar. 18, 2025), https://www.wired.com/story/federal-auditors-doge-elon-musk/

[18] Stephen Fowler, Jenna McLaughlin, *DOGE Says It Needs to Know the Government's Most Sensitive Data, but Can't Say Why*, NPR (Mar. 26, 2025), https://www.npr.org/2025/03/26/nx-s1-5339842/doge-data-access-privacy-act-social-security-treasury-opm-lawsuit. Since this breach, this employee has been granted access to even more sensitive data. Stephen Fowler, Jenna McLaughlin, *DOGE Staffer Who Shared Treasury Data Now Has More Access to Government Systems*, NPR (Mar. 31, 2025), https://www.npr.org/2025/03/31/nx-s1-5345708/doge-data-access-labor-cfpb-hhs.

[19] *New York, et al., v. Trump, et al.*, Case No. 1:25-cv-01144-JAV (S.D.N.Y. Feb. 21, 2025) (granting Plaintiff's motion for a preliminary injunction and restraining DOGE from accessing Treasury systems of records).

[20] *American Federal of Labor and Congress of Industrial Organizations v. Dep't. of Labor*, Case No. 1:25-cv-00339-JDB 1, 14 (U.S.D.C. Mar. 19, 2025) ("When it comes to DOL, defendants themselves acknowledge inconsistencies across their evidence.").

living individuals as dead[21] following its baseless claims of rampant Social Security fraud.[22] The DOGE has also used its illegal access to amass information on federal workers, prompting numerous lawsuits.[23] Individuals receiving this unprecedented access are not trained or vetted to handle the sensitive information that has been put in their hands. More alarming still, the DOGE is realizing the fears of the Privacy Act's authors by creating a single immense database full of sensitive personal information that can and will be used to surveil and harm individuals.[24]

b. Federal government uses of AI create significant privacy risks, including the deanonymization of large datasets.

Federal agencies have long sought to implement AI and other automated decision-making systems (ADS) to fulfill government functions, and the adoption of such technologies has rapidly accelerated in recent years.[25] But despite important efforts at oversight,[26] federal use of AI and ADS remains poorly regulated. The design, behaviors, and applications of such systems are often opaque and unvetted, making it difficult to assess whether and how a person's rights may have been violated.

Federal, state, and local governments are already using AI and ADS, including for law enforcement, public benefits and housing eligibility determinations, fraud detection, and more.[27] But each step of the development and procurement process risks harm to individuals and may result in the misuse of personal information. For example, an agency may seek to use the personal information held in its systems of records to train AI or ADS. But such training data is often accessible by users of the resulting system, and once a user retrieves that training data, it can in many cases be deanonymized (if it is not already identifiable). This type of leakage not

---

[21] James Liddell, *How Social Security Claimants Are Being 'Resurrected' After DOGE Falsely Declares Them Dead*, Independent (Apr. 24, 2025), https://www.independent.co.uk/news/world/americas/us-politics/social-security-dead-doge-claims-musk-b2738662.html.
[22] Stephen Fowler & Jude Joffe-Block, *How DOGE May Have Improperly Used Social Security Data to Push Voter Fraud Narratives*, NPR (Apr. 11, 2025), https://www.npr.org/2025/04/11/nx-s1-5352470/doge-musk-social-security-voting.
[23] *See, e.g.*, Advocacy Group, Unions Sue Treasury Department Over Illegal DOGE Data Access, AFGE (Feb. 03, 2025), https://www.afge.org/publication/advocacy-group-unions-sue-treasury-department-over-illegal-doge-data-access/.
[24] Makena Kelly, Vittoria Elliott, *DOGE Is Building a Master Database to Surveil and Track Immigrants*, WIRED (Apr. 18, 2025), https://www.wired.com/story/doge-collecting-immigrant-data-surveil-track/.
[25] GAO-24-105980 *Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements,* GAO (Dec. 2023), https://www.gao.gov/assets/gao-24-105980.pdf (finding roughly 1,200 distinct AI use cases in federal agencies in 2023. This number has certainly risen).
[26] *See, e.g.*, Executive Order 14110 Safe, Secure, and Trustworthy Development and use of Artificial Intelligence, 88 Fed. Reg. 75191, 75191 (Oct. 30, 2023). *See also* Shalanda D. Young, *M-24-10 Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, OMB (Mar. 28, 2024), https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.
[27] Grant Fergusson, *Outsourced and Automated: How AI Companies Have Taken Over Government Decision-Making*, EPIC (Sept. 26, 2023), https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf.

only violates an individual's privacy, but also leave individuals open to further threats such as identity theft.

These systems may also harm individuals once they are deployed. Governments are using AI and ADS in ways that impact individuals' work, benefits, housing, and interactions with law enforcement. AI and ADS are increasingly trusted to make critical decisions in these contexts. Yet it is often impossible to know whether and how such a system is being used, what information it was trained on, whether it yields accurate and non-discriminatory outputs, and how its decisions are derived. For example, the U.S. Department of Agriculture could deploy a system that determines when an individual is entitled to SNAP benefits.[28] If the system wrongly determines that an individual receiving SNAP benefits should receive less (or no) assistance, it may be difficult or impossible to understand how the system was trained, what information the system considered, whether that information was accurate, or how the system weighed the information to arrive at its decision. Not only can this prevent someone from receiving life-sustaining assistance, but it can also violate their right to due process by denying notice and a hearing.

Many potential applications of AI and ADS by federal agencies run the risk of violating the Privacy Act. Again, the work of the DOGE is illustrative. Personal data, including sensitive financial information obtained from the Department of Education, has been fed into at least one AI system—part of a putative attempt to "radically reduce spending" and support the administration's push to get rid of the Department.[29] Although the full details of this AI deployment are not publicly known, the disclosure of personal information to non-agency (e.g., DOGE or private sector) personnel for the purposes of conducting AI analysis may well have violated the Privacy Act, as the dismantling of government services is almost certainly incompatible with the original purpose of collection.

c. Congress should direct the adoption and development of PETs to safeguard against the risks posed by the maintenance of federal systems of records.

To mitigate the risks associated with the maintenance and use of federal systems of records, Congress should direct and adequately fund the adoption and development of privacy enhancing technologies (PETs). PETs vary widely. They can be highly technical workflows or relatively simple tools that limit data collection or enable data subjects to control their data. PETs can also be used in a wide array of contexts, including financial transactions, healthcare,

[28] A system does exist for the purpose of screening for SNAP fraud. U.S. Dep't of Agriculture, *Fact Sheet: SNAP Fraud Framework*, https://www.fns.usda.gov/snap/fraud-framework.
[29] Hannah Natanson, Gerrit De Vynck, Elizabeth Dwoskin, & Danielle Douglas-Gabriel, *Elon Musk's DOGE Is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025), https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/.

education, data management and transfers, research, and national security.[30] PETs should be more widely incorporated into the data management practices of agencies and their contractors to strengthen data security and lower the risk of data misuse and abuse.

Traditional techniques for deidentifying and anonymizing datasets are ineffective against the threat faced today, where often a single entity can combine multiple datasets to reidentify individuals.[31] PETs such as differential privacy are more effective safeguards in this context. Differential privacy involves the intentional injection of controlled amounts of statistical noise into data products to provide a mathematical guarantee of privacy while preserving the ability to use the resulting data.[32] Differential privacy has proven valuable in a variety of contexts, including the disclosure avoidance system used in the 2020 Census.[33]

EPIC urges Congress to examine how PETs such as differential privacy can be leveraged to protect privacy across the federal government and to require broader adoption of such techniques. EPIC recommends the following resources:

- Cynthia Dwork, *Differential privacy*, International Colloquium on Automata, Languages, and Programming (ICALP) (2006), https://link.springer.com/chapter/10.1007/11787006_1.
- Cynthia Dwork and Vitaly Feldman, *Privacy-preserving prediction*, in Conference on Learning Theory, 1693-1702, 1693-1702.24 (2018), https://arxiv.org/pdf/1803.10266.
- Mark Bun, Cynthia Dwork, Guy N. Rothblum, and Thomas Steinke, *Composable and versatile privacy via truncated CDP*, Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, 74-86.25 (2018), https://projects.iq.harvard.edu/files/privacytools/files/bun_mark_composable_.pdf.
- EPIC, *Comments to the White House Office of Science and Technology Policy on Advancing Privacy-Enhancing Technologies* (Jul. 8, 2022), https://epic.org/wp-content/uploads/2022/07/EPIC-Comments-OSTP-Privacy-Enhancing-Tech-8-July-2022.pdf
- EPIC, *Comments to the National Science Foundation on Developing a Roadmap for the Directorate for Technology, Innovation, and Partnerships at the NSF* (Jul. 27, 2023), https://epic.org/documents/comments-of-epic-to-the-nsf-on-developing-a-

[30] *See* Cem Dilmegani, *Top 10 Privacy Enhancing Technologies & Use Cases in 2023*, AIMultiple (Dec. 21, 2022), https://research.aimultiple.com/privacy-enhancing-technologies/ (outlining use cases for privacy enhancing technologies).
[31] *See, e.g.*, Cynthia Dwork, et al., *Exposed! A Survey of Attacks on Private Data*, 4 Annual Review of Statistics and Its Application 61–84 (2017), https://privacytools.seas.harvard.edu/files/privacytools/files/pdf_02.pdf.
[32] Daniel L. Oberski & Frauke Kreuter, *Differential Privacy and Social Science: An Urgent Puzzle*, Harv. Data Sci. Rev. (Jan. 31, 2020).
[33] Michael Hawes, U.S. Census Bureau, *Differential Privacy and the 2020 Decennial Census* 13 (Mar. 5, 2020), https://www2.census.gov/about/policies/2020-03-05-differential-privacy.pdf. *See also* U.S. Census Bureau, *Why the Census Bureau Chose Differential Privacy*, C2020BR-03 (Mar. 2023), https://www2.census.gov/library/publications/decennial/2020/census-briefs/c2020br-03.pdf.

roadmap-for-the-directorate-for-technology-innovation-and-partnerships-at-the-nsf/#_ftnref20.

- EPIC, *Comments to the National Telecommunications and Information Administration on AI Accountability Policy* (Jun. 12, 2023), https://epic.org/wp-content/uploads/2023/06/EPIC-NTIA-Comments-June-2023.pdf.

II. The Privacy Act Should Be Strengthened by Imposing Additional Limitations on the Exceptions, Establishing Stricter Standards, and Providing Broader Injunctive Remedies.

The government collects and stores vast sums of personal information, defined as "records" under the Privacy Act, in the course of carrying out agency functions. Sensitive data from every American citizen, and many noncitizens, is stored in one or more of the federal government's information systems. This includes Social Security numbers, financial information, health information, employment records, and address records, among many other data types. Recognizing the potential for government overreach and abuse of personal information, Congress passed the Privacy Act of 1974 to regulate the information practices of the federal government.[34]

The Privacy Act is based on three core principles: individuals have a right to control their personal data; government agencies are limited in how they can disclose that data; and those who manage that data must be subject to strict accountability and transparency safeguards. To implement these principles, the Act establishes several rights with respect to personal data. First, agencies are generally required to show an individual any records kept on them.[35] Second, agencies must follow certain principles, called fair information practice principles (FIPPs), when gathering and handling personal data.[36] Third, government agencies generally are barred from disclosing an individual's information to any person or another agency without the written request or consent of that individual.[37] Finally, the Act provides for both civil[38] and criminal penalties.[39]

The Privacy Act contains important protections that ensure that the government acts responsibly when handling Americans' personal data. However, it has become outdated in key respects as data systems and uses have continued to evolve. The Act's protections must be updated and expanded to protect individuals form external and internal threats. While the Privacy Act can create friction for federal agencies, this friction is necessary to protect the personal information held in government information systems. Further, the Act enables agencies to make

[34] 5 U.S.C. § 552a(e).
[35] 5 U.S.C. § 552a(d).
[36] 5 U.S.C. § 552a(e).
[37] 5 U.S.C. § 552a(b).
[38] 5 U.S.C. § 552a(g).
[39] 5 U.S.C. § 552a(i).

necessary and legitimate disclosures of personal information through several enumerated exceptions. The following proposals would clarify and carry forward the original intent of the Privacy Act without unduly burdening agency operations.

a. **Agencies should be required to obtain affirmative consent from individuals before using personal information to train AI systems.**

The Privacy Act should be amended to require affirmative express consent before an individual's personal data may be used to train an AI model or ADS. As discussed above, government use of AI and ADS remains poorly regulated. Such systems, though often faulty and opaque, are being used to make decisions that have potentially irreversible impacts on people's lives. Many uses of AI and ADS contradict the Act's purpose because they lack accountability and transparency and pose unique harms to the privacy of individuals. For these reasons, the Act should require an agency to obtain the written consent of affected individuals before the agency may use those individuals' personal information to train an AI system. Affected individuals include those who have personal information contained in the agency's system of records that it intends to use in the training of an AI model. In order to reduce the burden of this requirement, such consent should generally be requested when the agency collects the personal information in the first place.

b. **The "need to know" exception should be further clarified to restore its intended scope.**

There are legitimate reasons that an agency may want or need to disclose an individual's personal information. To facilitate legitimate uses of data, the Act contains specific exceptions to its prohibition on the disclosure of personal information. One such exception is the "need to know" disclosure exception. Under that exception, records may be disclosed to other employees of the agency for necessary, official purposes.[40] Generally, an employee has a "need to know" if the records are actually necessary to perform their duties, which may include vetting personnel or performing other administrative functions.[41] However, the "need to know" disclosure exception has been stretched far beyond its intended scope over time. The Privacy Act should be amended to more clearly define this exception.

The "need to know" exception was included in the Privacy Act to ensure that agencies could perform work necessary to administer federal programs. The drafters of the Act intended that agency subcomponents would be considered "intra-agency" for the purposes of the Act.[42] For example, the U.S. Marshals Service may still provide records to the FBI because they are both subcomponents of DOJ. However, the recipient still needs to have a legitimate "need to know." The Privacy Act Guidelines also read the Act to "imply that the use should be generally

[40] 5 U.S.C. § 552a(b)(1).
[41] *Id*.
[42] OMB, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28948, 28954 (Jul. 1, 1975).

related to the purpose for which the record is maintained."[43] Yet over time, the "need to know" exception has been misused and improperly expanded. Too often, agencies leverage the exception to provide access to records in situations where the records are not actually necessary to the recipient's job duties. And agencies are rarely required to justify their need to know or show that it would be prohibitive to complete the task by less privacy-invasive means.[44]

The DOGE is now attempting to invoke this exception to justify its access to federal information systems.[45] It seeks to use records for purposes that are wholly incompatible with the original purposes of data collection. In many cases it has not articulated any valid reason for needing to access the vast reaches of sensitive personal information it seeks.[46] Fortunately, several federal courts have already rejected the DOGE's "need to know" claims.[47] But as a practical matter, the DOGE may still be able to proceed in agencies where it has planted personnel as long as it can articulate a nominal need for the records it seeks—even if that purpose is flimsy and tenuously related to the original purpose of collection.

To protect against this and future attempts to exploit ambiguities in the Privacy Act, Congress should limit the "need to know" exception to make it clear that any such disclosure must be reasonably necessary and proportionate to the duty the employee must perform. Congress should also clarify the definition of "intra-agency" and ensure that "need to know" uses are related to the original purpose of the system of records. This amendment would bring the exception back in line with the fair information practice principles that are embedded in the Act, including data minimization.[48]

c. The Privacy Act should be amended to prevent overbroad applications of the "routine use" exception.

The Privacy Act should be amended to more clearly limit the scope of the "routine use" exception.[49] The "routine use" exception allows inter-agency disclosure of personal information "for a routine use," provided that such use is first noticed in the Federal Register. The phrase "routine use" is defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected."[50] While this provision is meant to provide agencies some flexibility in their administration of records systems, it is intended to be a narrow exception consistent with the Act's goal of protecting privacy. Legislative history shows that a "routine

---

[43] *Id*.
[44] *Id*. at 28948.
[45] Stephen Fowler, Jenna McLaughlin, *DOGE Says It Needs to Know the Government's Most Sensitive Data, but Can't Say Why*, NPR (Mar. 26, 2025), https://www.npr.org/2025/03/26/nx-s1-5339842/doge-data-access-privacy-act-social-security-treasury-opm-lawsuit.
[46] *Id*.
[47] *Id*.
[48] Fair Information Practice Principles (FIPPs), FPC.gov, https://www.fpc.gov/resources/fipps/.
[49] 5 U.S.C. § 552a(b)(3).
[50] 5 U.S.C. § 552a(a)(7).

use" must be specifically tailored to a defined purpose for which the records are collected.[51] The Privacy Act Guidelines of 1975 provide further clarity about the exemption, explaining that a "routine use" must be related to "the purpose for which the record is maintained."[52]

Despite this clear instruction, however, agencies have often misused the "routine use" exception to circumvent the Act's general prohibition on disclosure.[53] In particular, the term "compatible" has been stretched to encompass uses that are only tenuously connected to the original purpose of collection. Similarly, agencies often maximize their asserted ability to make cross-agency disclosures under the "routine use" exception by publishing short and vague statements of those uses in the Federal Register. While some courts have rejected overbroad applications of the exception, in practice many questionably "compatible" uses are still premised on nebulous system of records notices.[54] Further limitations on this exception are needed to ensure meaningful privacy protection.

d. The Privacy Act's private right of action should be strengthened by providing for expanded injunctive relief.

The Privacy Act should authorize a broader range of injunctive remedies to allow individuals to fully vindicate their rights under the Act and to address harmful agency data practices—ideally *before* they are implemented. The current injunctive remedies available to an individual under the Privacy Act are limited to the correction of inaccurate records and access to records about the individual maintained by an agency. These provisions, while important, do not provide a mechanism for rectifying harmful data practices such as wrongful disclosure or agency reliance on impermissible "routine uses."

Privacy harms are irreparable: once personal information has been illegally accessed or disclosed, the harm cannot be fully undone and the individual cannot be made completely whole, even by damages. Broadening the injunctive relief available under the Act would enable individuals to prevent illegal, invasive, and harmful disclosure of their personal information before it occurs—or at a minimum, to correct unlawful agency privacy practices moving forward. Although some litigants have been able to achieve this form of relief through the Administrative Procedure Act (APA), the APA presents additional complexities that make it an imperfect cause of action for Privacy Act violations. Congress should take this opportunity to

---

[51] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[52] *Id.*
[53] Robert Gellman, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974*, World Privacy Forum at 23-39 (Apr. 2021), https://www.worldprivacyforum.org/wp-content/uploads/2021/04/updating-the-privacy-act-of-1974.pdf.
[54] See, e.g., *Britt v. Naval Investigative Service*, 886 F.2d 544 (3d Cir. 1989) (finding that the routine use published in the federal register was overbroad and did not provide adequate notice to individuals as to what information concerning them will be released and the purposes of such a release).

incorporate broader injunctive remedies into the Privacy Act itself, giving individuals the surest possible remedy when agencies place their personal information at impermissible risk.

e. **Congress can protect Americans' privacy by instating minimum personnel and budget standards for agency Privacy Offices.**

Congress should amend the Privacy Act to include robust vetting and training standards for agency personnel that are granted access to government information systems. Since the inauguration, DOGE personnel have gained staggering access to sensitive information across the federal government without proper qualifications, security clearances, training, or oversight. However, stricter standards alone will not prevent privacy violations without the necessary oversight. Congress can further strengthen the Privacy Act by ensuring that relevant offices are adequately funded and staffed to prevent violations of the Act.

First, the Privacy Act should be amended to establish minimum standards for the training, clearance, and qualification of agency personnel accessing sensitive personal data. DOGE personnel (largely recent college and high school graduates lacking relevant training) have been granted access to massive systems of records that containing sensitive personal information. They have been given access prior to completing background checks, obtaining the necessary agency security clearances, or receiving training to handle personally identifiable information. On at least one occasion, a DOGE employee sent an email with a spreadsheet containing personally identifiable information to two other federal officials. The Privacy Act does not contain clear standards for training, clearing, or qualifying federal employees in order to prevent dangerous disclosures of this kind. Adding such standards would be a much-needed safeguard for the privacy and security of Americans' information contained in federal systems of records.

Second, Congress must ensure that oversight offices within federal agencies are adequately funded and fully staffed by qualified civil servants. Each federal agency contains offices and staff dedicated to performing or facilitating oversight of the agency's actions. These include the Chief Information Officer, the Privacy Officer, the FOIA Liaison, and their staff. Some agencies, such as the Treasury Department, also have a combined FOIA/Privacy Act Office. These offices are responsible for monitoring agency activities to ensure they are respecting privacy and following the law. However, these offices cannot perform their roles without robust and reliable funding. Further, these offices must be adequately staffed by individuals qualified to identify and respond to agency actions. After EPIC filed FOIA requests to the Office of Personnel Management in January of 2025, we learned that every staff member in OPM's FOIA office had been fired other than the FOIA Public Liaison. While the FOIA only explicitly requires agencies to staff the public liaison, this action violates the FOIA's mandate to ensure that offices are adequately staffed to respond to requests from the public.[55] This appears

[55] 5 U.S.C. § 552(j)(2).

to be an attempt to illegally shield the agency from public oversight and hinders outside accountability.

The Privacy Act, including any substantive amendments Congress may make, cannot be effective if these offices are not adequately staffed, funded, and protected from improper interference. Congress should act to ensure that the federal workers tasked with protecting Americans' privacy have the means and training to do so.

III. Americans' Privacy Can Be Better Secured by Updating Other Government Oversight Laws, Including the E-Government Act of 2002 and the Federal Agency Data Mining Reporting Act of 2007.

In addition to the Privacy Act, other laws provide essential guardrails on the federal government's use of personal information by establishing procedures and oversight mechanisms. These include the E-Government Act of 2002 and the Federal Agency Data Mining Reporting Act of 2007. Like the Privacy Act, these statutes require updates to truly protect privacy against technological changes and executive malfeasance. Congress should amend these laws to close loopholes and provide additional enforcement mechanisms.

a. The E-Government Act of 2002 should be updated to ensure the efficacy of privacy impact assessments.

Technological growth has made collection for and access to information systems easier and faster. To ensure the protection of personal information, Congress enacted the E-Government Act of 2002. The E-Government Act supplements the Privacy Act by requiring all federal agencies that develop, procure, or make changes to information technology to conduct Privacy Impact Assessments (PIAs).[56] The PIA must be publicly available and must analyze how information is collected, stored, protected, shared, and managed to demonstrate that privacy protections have been put in place throughout a system's life cycle. However, the implementation of this requirement leaves much to be desired.

Agencies routinely fail to produce PIAs at all or do so on a timeline of years rather than weeks. Similarly, agencies do not update their PIAs in a timely manner to ensure meaningful oversight. For example, the U.S. Postal Inspection Service runs a secret intelligence program called the Internet Covert Operations Program (iCOP).[57] This program runs many information collection systems but operates with little oversight or transparency.[58] The iCOP secretly tracked and collected information on First Amendment activities. iCOP's activities require a PIA, but none was ever created. Without such a PIA, there was no way to discover the true nature of the program until it was leaked to a journalist. Further, agencies do not face consequences for their

---

[56] § 208 (b)(1)(A) E-Government Act, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).
[57] EPIC, EPIC v. U.S. Postal Service (2022), https://epic.org/documents/epic-v-u-s-postal-service/.
[58] Joseph Cox, Here's How the Post Office's Internet Cops Describe Themselves, Vice (Aug. 31, 2021), https://www.vice.com/en/article/m7enk3/us-postal-inspection-service-icop-presentation (quoting an internal USPIS training presentation).

failure to analyze privacy harms in a PIA or account for those harms. When agencies refuse to create required PIAs or only create PIAs far after the fact, harmful agency systems can take root and cause harm that is difficult or impossible to reverse.

When agencies do complete a required PIA, it is frequently done as a box-checking exercise after the system is implemented. The E-Government Act is clear that agencies must conduct PIAs "before developing or procuring information technology … or initiating a new collection of information…."[59] However, a 2022 GAO report on compliance with privacy protections found that only a quarter of surveyed agencies "always" initiated PIAs early enough in the system development process to impact the design or outcome of the system.[60] PIAs cannot be effective when they are completed after the fact: by then, the system is already in place and likely already in use.

For PIAs to be a meaningful tool for protecting privacy and providing oversight, they must be completed well in advance, include detailed accounts of the intended systems and actions, and include information on third party data and systems. Further, agencies must face consequences for failing to follow the law. For further reading on EPIC's recommendations regarding the E-Government Act of 2002, please refer to:

- EPIC, *Comments to the Office of Management and Budget Responding to Request for Information: Privacy Impact Assessments* (Apr. 1, 2024), https://epic.org/wp-content/uploads/2024/04/EPIC-Comment-to-OMB-re-PIAs-April-2024-with-Appendix.pdf.
- EPIC, *Comments to the Administrative Conference of the United States Regarding Disclosure of Agency Legal Materials* (Jul. 18, 2022), https://epic.org/wp-content/uploads/2022/07/EPIC-Comments-ACUS-Agency-Legal-Records-18-Jul-2022-combined.pdf.

b. The Federal Agency Data Mining Reporting Act of 2007 should be modernized and expanded to help Congress and the public understand agency data uses.

Data mining combines computer science with statistics to identify and extract patterns in massive data sets. Most often, mining techniques, including machine learning and predictive analytics, attempt to predict outcomes. While data mining can help agencies achieve their goals more efficiently, it poses significant privacy and constitutional risks to privacy that must be accounted for.

First, the data sources used may pose significant issues for obtaining usable results while respecting the privacy and other civil rights individuals hold. Data mining relies on broadscale collection of all kinds of information. This encourages agencies to vacuum up data

[59] § 208 (b)(1)(A) E-Government Act, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).
[60] GAO-22-105065 Federal Agency Privacy Programs, Gov't Accountability Off. at 42 (Sept. 2022), https://www.gao.gov/assets/gao-22-105065.pdf.

indiscriminately, sometimes in violation of the Privacy Act and Paperwork Reduction Act. This approach may lead to the collection of false data or personally identifiable information, including U.S. person information. This becomes even likelier when agencies buy up commercially available information from data brokers. Not only does buying commercially available information pose serious problems under the Fourth and First Amendments, but data brokers often do not verify or correct the information they sell. This means that government programs and systems may be built on the back of information that is of dubious quality at best.

Recognizing that data mining systems are "prone to inaccurate results" and "ripe for abuse, error, and unintended consequences," the Federal Agency Data Mining Reporting Act was created to ensure agencies are transparent, accountable, and protective of Americans' privacy.[61] To those ends, the Act requires an agency to submit a report to Congress and the public if the agency uses data mining to identify criminal or terrorist activity. Among other things, the report must include a description of the data mining technology used, its data sources, and the basis for determining criminal or terrorist activity. The report should also assess what impacts the agency's data mining activities will have on privacy and civil liberties and discuss the steps which the agency will take to mitigate those risks.

EPIC has reviewed existing data mining reports to evaluate how well the Act is meeting its goals. Our review revealed several deficiencies.

First, agencies are not following through on their obligations despite the Act's clear mandate. Only a handful of agencies, such as ODNI and DHS, complete data mining reports. Although materials from other agencies (including DOJ, the DEA, and the FBI) suggest that they conduct data mining activities, these agencies have never produced reports. While it is possible they only conduct data mining activities that would be confidential, there is no way for the public to know whether these agencies transmit a confidential data mining report to Congress. This undermines the public accountability the Act attempts to instill.

Second, when agencies publish reports at all, they typically provide insufficient information to determine compliance with the reporting requirement. The Act requires discussion of the data mining activity's efficacy, its potential impacts on privacy and civil liberties, and how the agency is protecting against those impacts. In effect, agencies fail to provide adequate information. For example, ODNI's reports are extremely short, usually clocking in between five and ten pages, and contain exact copies of previous program statements. This reflects an unwillingness to engage the Act's reporting requirement and makes meaningful oversight impossible.

Finally, agencies face no consequences for failing to report. For example, DHS failed to publish reports beginning in 2020 despite years of compliance. It was not until EPIC filed a FOIA request in 2023 that DHS complied with its obligation and published a joint report

[61] 42 U.S.C. § 2000ee-3 (2007).

covering 2020 and 2021. While DHS stated then that it was actively working on reports covering 2022, 2023, and 2024, none have been published. FOIA is an important method for holding agencies accountable, but it cannot be the only means of enforcing the Act.

EPIC recommends that Congress amend the language of the Act to be more inclusive of modern data mining techniques. EPIC further recommends that the Act require agencies that transmit confidential annexes to Congress to disclose a public statement containing high-level descriptions of the systems discussed in the annex.[62]

EPIC will follow up with Rep. Trahan's office in the coming months with a final report detailing our review of agency compliance and recommendations for updating the Federal Agency Data Mining Reporting Act of 2007.

IV. Conclusion

EPIC again commends Congresswoman Trahan for her commitment to protecting privacy by updating Privacy Act of 1974. While the Privacy Act is a cornerstone of federal privacy law, it must be amended to protect against existing and emerging threats. EPIC strongly urges Congress to update the Privacy Act to (1) require explicit consent for the use of personal information in the training of AI and ADS; (2) limit the "need to know" and "routine use" exceptions to the Act's disclosure prohibition; (3) include injunctive relief; and (4) institute minimum standards for vetting and training agency personnel who access and handle personal information.

While recent events crystallize the need for updated privacy protections, EPIC urges Congress to adopt broad reforms that go beyond the current moment. Further, EPIC strongly encourages Congress to ensure that relevant offices have the funding and expertise needed to effectively implement privacy protections for decades to come. EPIC appreciates the opportunity to respond to Congresswoman Trahan's request for information, and we are eager to engage with her office further on any of the issues raised within our comment.

[62] The CIA publishes such a statement each year.