DATA&
SOCIETY

Data & Society Statement for the Record
at a Hearing before the House Committee on Oversight and Government Reform on
"The Federal Government in the Age of Artificial Intelligence"

Submitted by:

Alice E. Marwick, PhD
Director of Research

Brian J. Chen
Policy Director

With assistance from:

Jacob Metcalf, PhD
Meg Young, PhD
Serena Oduro

Data & Society Research Institute

June 5, 2025

Committee Chair Comer, Active Ranking Member Lynch, and Members of the Committee:

We are pleased to submit this statement for the record on the federal government's use of artificial intelligence on behalf of Data & Society Research Institute (D&S), a nonprofit, independent research institute that studies the social impact of automation and artificial intelligence (AI). We believe that technology policy must be grounded in research, account for technology's real-world impacts, and serve the public. For the last decade, D&S has conducted empirical social science research on the social implications of emerging technologies, focusing on such areas as privacy, accountability, and fairness. We have deep, grounded empirical expertise on the broader social impacts of AI; with that in mind, we wish to make three points on the federal government's use of artificial intelligence:

First, DOGE's access to sensitive government data violates federal law and threatens the personal privacy of every American.

Second, a hasty rush to roll out untested AI will not result in efficient, high-quality government services. Instead, the unchecked use of AI will accelerate large-scale harms to the public, gutting critical services while offering no avenues for accountability and recourse.

Third, in order to protect Americans' civil rights, the Committee must ensure that the development and rollout of federal AI systems follow procurement laws and best practices.

First, DOGE's access to sensitive government data violates federal law and threatens Americans' privacy.

DOGE's data access violates federal law and diminishes trust in government. President Trump's Executive Order 14158 established the Department of Governmental Efficiency, or DOGE. Under the guise of "efficiency," the world's richest man, Elon Musk, and his DOGE staff gained unprecedented access to personal data about virtually all Americans — with little or no oversight. The government collects an immense amount of information about its citizens, more than 300 types of data.[1] This data includes tax returns, Medicare and VA records, incarceration status, social services and public benefits applications, federal student loan information, biometric data, immigration information, military service records, and much more.[2] Contained within those records are deeply intimate details about American's lives, such as domestic violence history (in HUD data), bank account numbers (in IRS data), and reproductive health details (in Medicare and Medicaid data).

Crucially, this data is kept separate by law and historical norms of cybersecurity. Until the arrival of DOGE, when citizens provided information in one context, such as applying for disability benefits, they could be sure it would not be matched with Census data or voting records. Such firewalls maintain trust in government and allow for different forms of data protection, depending on the data type. For example, the Centers for Medicare and Medicaid Services, the Veteran's Health Administration, and the Indian Health Service are all covered entities under HIPAA (the Health Insurance Portability and Accountability Act of 1996), so they must adhere to the privacy laws governing health information.[3] Combining that specific type of data with IRS

[1] Badger, E. (2025, April 9). Trump wants to merge government data. Here are 314 things it might know about you. *The New York Times*. https://www.nytimes.com/2025/04/09/us/politics/trump-musk-data-access.html

[2] Pascal, A., Stanger, A., Schneier, B., Zalesne, K., Pyati, N., Hubbard, S., & Graubard, V. (2025, March 31). *Understanding DOGE and your data.* Ash Center for Democratic Governance and Innovation, Harvard University. https://ash.harvard.edu/resources/understanding-doge-and-your-data/

[3] U.S. Department of Health and Human Services. (n.d.). *Covered entities and business associates.* HHS.gov. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

data, which is protected by Internal Revenue Code Section 6103, The Privacy Act of 1974, and H.R. 8292, creates an untenable mess that leaves Americans vulnerable to illegal data disclosure and abuse.

Such breaches of historical data security norms also degrade the quality of the data that the federal government relies upon. When people provide information to the government, they do so knowing that this information is for a specific and limited purpose. For example, when a resident fills out the Census, they know it won't be cross-checked against Social Security databases, immigration information, or criminal records. This ensures that our Census data is accurate. The IRS collects money on sensitive matters, such as gambling debts and illegal activities; data protection ensures that tax receipts are accurate and equitable. Similarly, students and families share sensitive details on the FAFSA financial aid form because they trust it won't be used for law enforcement or immigration enforcement purposes. Patients enrolled in Medicare expect their health data to be used to improve care, not to screen for unrelated eligibility requirements or criminal histories. Keeping data systems separate maintains public trust, improves participation, and allows federal agencies to collect accurate information tailored to their specific missions.

DOGE has asserted it is not subject to long-standing public records laws, and as a result we know very little about who works at DOGE, what access they have to private data, or what they are doing with it.[4] In some cases, even letting DOGE employees access certain types of data violates federal law. For example, absent very specific circumstances, IRS employees are forbidden from accessing tax returns, as are government employees who do not work for the IRS.[5] (Tax returns have been considered private, protected information in the United States since 1870.) DOGE has operated without transparency, and often at odds with the mandates of the government offices it is trying to reform.

DOGE's attempts at aggregation enrich Silicon Valley while risking the privacy of Americans. Even more worrisome are DOGE's attempts to connect and aggregate data that must be legally kept separate. President Trump's Executive Order, "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos" calls for "promoting inter-agency data sharing."[6] But combining information collected by different agencies in different contexts is expressly prohibited by the Privacy Act of 1974.[7] The Privacy Act was enacted after the Watergate and

[4] The New York Times. (2025, May 28). The People Carrying Out Musk's Plans at DOGE. *The New York Times*. https://www.nytimes.com/interactive/2025/02/27/us/politics/doge-staff-list.html (updated May 28, 2025)
[5] U.S. Code Title 26 § 6103. (n.d.). Confidentiality and disclosure of returns and return information. United States Code. https://uscode.house.gov/view.xhtml?req=(title:26%20section:6103%20edition:prelim)
[6] Exec. Order No. 14243, 90 Fed. Reg. 13681 (March 20, 2025) https://www.federalregister.gov/documents/2025/03/25/2025-05214/stopping-waste-fraud-and-abuse-by-eliminating-information-silos
[7] U.S. Department of Justice, Office of Privacy and Civil Liberties. (2020). *Overview of the Privacy Act of 1974 (2020 Edition)*. https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition

COINTELPRO scandals revealed that the government was surveilling opposition political parties and a wide range of individuals deemed "subversive," which, at the time, was seen as antithetical to American democracy. As Senator Sam Ervin, the primary sponsor of the bill, said, "[i]f we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens." If concern over the risks of data integration was high in 1974, then we should be far more skeptical of DOGE's intent given today's more sophisticated technologies.

In contrast, DOGE is trying to expand what the government knows about each of its citizens. Specifically, reports claim DOGE is attempting to build a cross-agency database of information scraped from the IRS, the Social Security Administration, the Department of Health and Human Services, and other agencies, in collaboration with the multi-billion dollar Silicon Valley company Palantir.[8] Whistleblowers recently revealed that the Department of Homeland Security is aggregating DHS data, voting records, and Social Security Administration data to surveil immigrants in real time.[9] ICE recently contracted Palantir to track self-deportations under a new system called ImmigrationOS,[10] while DOGE selected Palantir to deploy Foundry, their data analysis platform, across government agencies including the DHS, SSA, Pentagon, HHS, and IRS, further increasing aggregation.[11] Perhaps most worrying is the news this week that President Trump may have tapped Palantir to assemble dossiers on every American citizen, for unclear ends and under no clear authority.[12]

These databases are not just potentially illegal, but provide billions of dollars in government contracts to Silicon Valley companies.[13] Elon Musk co-founded PayPal with Peter Thiel, the billionaire Palantir founder; the *New York Times* reported that at least three DOGE employees

[8]Alms, N. (2025, April 18). DOGE is building a 'master database' of sensitive information, top Oversight Democrat says. *Nextgov/FCW.* https://www.nextgov.com/digital-government/2025/04/doge-building-master-database-sensitive-information-top-oversight-democrat-says/404693/

[9] Kelly, M., & Elliott, V. (2025, April 18). DOGE is building a master database to surveil and track immigrants. *WIRED*. https://www.wired.com/story/doge-collecting-immigrant-data-surveil-track/

[10] Haskins, C. (2025, April 18). ICE is paying Palantir $30 million to build 'ImmigrationOS' surveillance platform. *WIRED*. https://www.wired.com/story/ice-palantir-immigrationos/

[11] Frenkel, S. (2025, May 30). Trump taps Palantir to compile data on Americans. *The New York Times.* https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html

[12] Mordowanec, N. (2025, June 2). 'Trump flipped on us': MAGA reacts to potential national citizen database. *Newsweek.* https://www.newsweek.com/donald-trump-palantir-maga-database-surveillance-2079905; Jones, J. (2025, June 3). Trump's Palantir surveillance plan raises concerns among Americans. *MSNBC.* https://www.msnbc.com/top-stories/latest/trump-palantir-surveillance-americans-rcna210017; Rashid, H. (2025, May 30). Trump taps Palantir to create master database on every American. *The New Republic.* https://newrepublic.com/post/195904/trump-palantir-data-americans

[13] Angwin, J. (2025, April 30). 'This Is What We Were Always Scared of': DOGE Is Building a Surveillance State. *The New York Times.* https://www.nytimes.com/2025/04/30/opinion/musk-doge-data-ai.html

previously worked at Palantir and two others were employed by companies that Thiel funded.[14] Bringing Palantir on board is not just crony capitalism. Palantir makes data analysis and prediction software used by governments around the world to surveill their citizens and target their enemies, and has repeatedly come under fire for facilitating human rights abuses.[15] Alex Karp, the CEO, bragged on an investor call in February about all the money Palantir was making from the Trump administration. "Palantir is here to disrupt," he said. "And, when it's necessary, to scare our enemies and, on occasion, kill them."[16] This is not a partner that inspires trust.

Palantir and DOGE's imagined database, if actualized, would create a perfect surveillance regime, aggregating all information provided to the government by its citizens and destroying trust and personal privacy in the process. The government could micro-target any suspected enemy or critic, weaponizing data to dig up real or imagined transgressions. Any federal employee with access, regardless of competency or partisanship, could access your bank account numbers, military service records, federal student loan debt, race, number of children, gambling debt or drug prescriptions. **We cannot imagine a greater security risk than having *this much sensitive data* in the hands of *so many people* with *so little oversight.*** More than a decade ago, Georgetown Law Professor Paul Ohm called such a massive aggregation of personal records the "database of ruin."[17] He argued that it would function as a tempting honeypot for malevolent actors wishing to "blackmail, harass, defame, frame, or discriminate against us."[18] This is especially true given the government's history of data breaches. In 2015 alone, 191 million voter records showed up on the open web, while criminals accessed 610,000 tax returns from the IRS; now imagine if all that information had been connected.[19] Given DOGE's slipshod approach to cybersecurity, aggregation opens federal agencies — and thus all Americans — to hostile foreign actors and criminal groups.[20]

---

[14]Frenkel, S. and Krolik, A. (2025, May 30). Trump taps Palantir to compile data on Americans. *The New York Times.* https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html

[15] Iliadis, A., & and Acker, A. (2022). The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society, 38*(5), 334–363. https://doi.org/10.1080/01972243.2022.2100851; Ulbricht, L., & Egbert, S. (2024). In Palantir we trust? Regulation of data analysis platforms in public security. *Big Data & Society, 11*(3). https://doi.org/10.1177/20539517241255108

[16]Hurwitz, S. (2025, February 60. The Gleeful Profiteers of Trump's Police State. *Mother Jones.* https://www.motherjones.com/politics/2025/02/palantir-alex-karp-trump-private-prisons-profiteers/

[17] Ohm, P. (2012, August 23). Don't build a database of ruin. *Harvard Business Review.* https://hbr.org/2012/08/dont-build-a-database-of-ruin

[18] Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*, 1701–1777. University of Colorado Law Legal Studies Research Paper No. 9-12. https://ssrn.com/abstract=1450006

[19] Finkle, J., & Volz, D. (2015, December 29). Database of 191 million U.S. voters exposed on Internet: Researcher. *Reuters*. https://www.reuters.com/article/world/us/database-of-191-million-us-voters-exposed-on-internet-researcher-idUSMTZSAPEBCT4IJVCW/; Mari, C. (2021). Internal Revenue Service Data Breach. *EBSCO.* https://www.ebsco.com/research-starters/computer-science/internal-revenue-service-data-breach-2015

[20] Forland, S. (2025, April 7). DOGE's data grabs and downsizing jeopardize our national security. *New America.* https://www.newamerica.org/oti/blog/doges-data-grabs-and-downsizing-jeopardize-our-national-security/

DOGE employees disregard federal data protection regulations. Although much government data is highly personal and protected, DOGE employees have not adhered to best practices. Instead, they have been reckless and negligent. DOGE employees used personal laptops without the threat assessment and monitoring programs required for all federal devices. They repeatedly accessed private information at the HHS and Social Security administration, including the social security numbers and medical diagnoses of private citizens.[21] DOGE employees viewed highly-protected information at the Department of Labor that had nothing to do with government spending or efficiency and may have included confidential corporate information and information pertaining to labor unions and ongoing lawsuits, potentially relevant to litigation about Musk's companies.[22] One DOGE employee, who was temporarily laid off over racist tweets and then rehired by Trump's order, sent personally identifiable information outside the Treasury Department.[23] Employees have uploaded personal, protected data to large language models like Grok and Llama, where they may have automatically become part of the models' training dataset.[24] DOGE even published classified personnel data from a U.S. intelligence agency, the National Reconnaissance Office, on its public website, raising serious concerns about unauthorized access and misuse of sensitive national security information.[25] They have been sued by employees of the Office of Personnel Management for operating an illegal, unencrypted email server, potentially exposing OPM employees' data to malign foreign actors.[26] In total, fourteen lawsuits have been filed against DOGE, alleging violations of six different federal privacy protections, across eight federal agencies.[27] DOGE's conduct suggests not only a disregard for federal cybersecurity protocols but a fundamental indifference to the privacy rights of the people they are charged with protecting.

---

[21] Natanson, H., Menn, J., Rein, L., & Siegel, R. (2025, May 7). DOGE aims to pool federal data, putting personal information at risk. *The Washington Post.* https://www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security

[22] McLaughlin, J. (2025, April 15). Whistleblower details how DOGE may have taken sensitive NLRB data. *All Things Considered. NPR.* https://www.npr.org/2025/04/15/nx-s1-5355896/doge-nlrb-elon-musk-spacex-security

[23] Fowler, S. & McLaughlin, J. (2025, March 31). DOGE staffer who shared Treasury data now has more access to government systems. *NPR.* https://www.npr.org/2025/03/31/nx-s1-5345708/doge-data-access-labor-cfpb-hhs

[24] Kelly, M. (2025, May 22). DOGE used a Meta AI model to review emails from federal workers. *WIRED.* https://www.wired.com/story/doge-used-meta-ai-model-review-fork-emails-from-federal-workers/; Ulmer, A., Taylor, M., Dastin, J., Alper, A., Ulmer, A., Taylor, M., & Dastin, J. (2025, April 8). Exclusive: Musk's DOGE using AI to snoop on U.S. federal workers, sources say. *Reuters.* https://www.reuters.com/technology/artificial-intelligence/musks-doge-using-ai-snoop-us-federal-workers-sources-say-2025-04-08/

[25] Bendery, J. (2025, February 14). (2025, February 14). Elon Musk's DOGE posts classified data on its new website. *The Huffington Post.* https://www.huffpost.com/entry/elon-musk-doge-posts-classified-data_n_67ae646de4b0513a8d767112

[26] Cameron, D. (2025, February 4) Federal Workers Sue to Disconnect DOGE Server. *WIRED.* https://www.wired.com/story/federal-workers-sue-over-doge-server/

[27] Just Security (2025, June 4). Litigation tracker: Legal challenges to Trump administration actions. *Just Security.* https://www.justsecurity.org/107087/tracker-litigation-legal-challenges-trump-administration/; Center for Democracy & Technology and The Leadership Conference's Center for Civil Rights and Technology. (2025, March 17). *DOGE and Government Data Privacy.* Fact sheet. https://cdt.org/wp-content/uploads/2025/03/CDT-Leadership-Conference-DOGE-and-Government-Data-Privacy-Explainer.pdf

This is because the federal government has very detailed requirements for how personal data is to be accessed and used. As the *Washington Post* reports, "Typically, data sharing within the federal government requires multiple steps. That includes legislative permission, public notices of what the government is doing, and 'computer matching' agreements between agencies specifying what is to be shared and why. Independent inspectors general also help make sure information is being used appropriately."[28] DOGE has disregarded these protections, firing staff who attempted to follow the rules and prompting others to quit rather than comply.[29] In February, 21 DOGE staffers (previously employees of DOGE's predecessor agency, not handpicked by Musk) quit, stating that their expertise was being used to "compromise core government systems, jeopardize American's sensitive data, [and] dismantle critical public services."[30] In March, the chief counsel of the IRS quit, refusing to share tax information with other agencies, claiming that what he was ordered to do was against the law.[31] In April, the Interior Department fired four top officials when they objected to DOGE accessing the Federal Personnel and Payroll System.[32] As these federal employees were aware, data privacy regulations are not pesky barriers to seamless government implementation. They are absolutely necessary to maintain the American people's trust in government and to ensure that their privacy is protected. Without them, we are one step closer to an authoritarian government that has one eye on its citizens at all times.

The right to privacy is paramount to human dignity and self-determination, especially in a democracy that aspires to be the "land of the free." Everyone has information they wish to keep private; everyone has the right to keep information private. The price of accessing healthcare, utilizing public services and benefits to which we are entitled, or even simply paying our taxes, cannot be the loss of privacy. DOGE's actions are already potential violations of federal law; any effort to aggregate multiple sources of government data into a mega-database would fundamentally threaten our rights as Americans.

---

[28] Natanson, H., Menn, J., Rein, L., & Siegel, R. (2025, May 7). DOGE aims to pool federal data, putting personal information at risk. *The Washington Post.* https://www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security

[29]Williams, A., Hillyard, V., Alcindor, Y., & De Luce, D. (2025, February 4). USAID security leaders removed after refusing Elon Musk's DOGE employees access to secure systems. *NBC News.* https://www.nbcnews.com/politics/national-security/usaid-security-leaders-removed-refusing-elon-musks-doge-employees-acce-rcna190357

[30] Kolodny, K., CNBC, Smith, A. and Arkin, D. (2025, February 5). 21 U.S. DOGE Service staffers resign over a refusal to 'jeopardize Americans' sensitive data,' letter says. *NBC News.* https://www.nbcnews.com/politics/doge/21-doge-staffers-resign-saying-refuse-compromise-core-government-syste-rcna193622

[31] Hussein, F. (2025, March 13). IRS removes its chief counsel after clashing with DOGE over sharing tax info, AP reports. *PBS NewsHour.* https://www.pbs.org/newshour/politics/irs-removes-its-chief-counsel-after-clashing-with-doge-over-sharing-tax-info-ap-reports

[32] Alms, N. (2025, April 9). Interior fires senior leaders after fight over DOGE access to key payroll system. *Nextgov.* https://www.nextgov.com/people/2025/04/interior-fires-senior-leadership-after-fight-over-doge-access-key-payroll-system/404421/

Second, hastily deployed AI systems will not make the government more efficient and risk withholding government benefits from people who need them.

The Trump administration is claiming to use an "AI-first strategy," led by DOGE, to eliminate "waste, fraud, and abuse."[33] The results have not been promising. What we have seen is the unchecked use of AI to fire federal workers, cut Americans off public benefits, and slash critical spending for federal programs.[34] Government efficiency, if anything, has suffered.[35]

Given the overall deficit of transparency around the government's use of AI — especially to make critical decisions, e.g. approving or denying benefits, placing people under detention, selecting someone for surveillance — the American public deserves to know much more about how federal agencies are deploying AI and how such use is improving government operations. In the absence of this evidence, substantial empirical research suggests that the administration's strategy to drive mass AI adoption is unlikely to ever achieve improved efficiency.[36]

First, AI is error-laden, biased, inaccurate, and dysfunctional, especially if it is not carefully built to fulfill a narrow purpose.[37] Its failures at the essential functions of civil servants are well-documented: AI has advised people to break the law,[38] generated false positives for unemployment insurance fraud,[39] and performed worse than judges at predicting criminal reoffenders.[40] **Even from a purely technical perspective, there is little evidence on the effectiveness and impact of AI tools.[41]**

Second, unproven AI systems are not a replacement for government employees. Even if AI improves and makes fewer technical errors, it's a mistake to assume it can simply replace

---

[33] Exec. Order No. 14243, 90 Fed. Reg. 13681 (March 20, 2025)
[34] Riedl, J. (2025, May 8). The Actual Math Behind DOGE's Cuts. *The Atlantic.* https://www.theatlantic.com/politics/archive/2025/05/musk-doge-spending-cuts/682736/; Sainato, M. (2025, April 6). Doge's attack on social security causing 'complete, utter chaos', staff says. *The Guardian*. https://www.theguardian.com/us-news/2025/apr/06/musk-doge-social-security; Sasha Rogelberg. (2025, April 27). DOGE's mass federal workforce cuts may cost taxpayers $135 billion this fiscal year alone. *Fortune.* https://www.yahoo.com/news/doge-mass-federal-workforce-cuts-110200918.html
[35] Natanson, H. (2025, June 2). DOGE vowed to make government more 'efficient'-- but it's doing the opposite. *The Washington Post.* https://wapo.st/4kr9npC
[36] Chen, B. (2025, March 25). *Dispelling Myths of AI & Efficiency*. Data & Society Research Institute. https://datasociety.net/library/dispelling-myths-of-ai-and-efficiency/
[37] *See*, *e.g.*, Inioluwa Deborah Raji, et al., *The Fallacy of AI Functionality*, FAccT '22 (June 20, 2022), https://dl.acm.org/doi/10.1145/3531146.3533158.
[38] Colin Lecher, *NYC's AI Chatbot Tells Businesses to Break the Law*, The Markup (Mar. 29, 2024), https://themarkup.org/news/2024/03/29/nycs-ai-chatbot-tells-businesses-to-break-the-law.
[39] Robert N. Charette, *Michigan's MiDAS Unemployment System: Algorithm Alchemy Created Lead, Not Gold*, IEEE Spectrum (Jan. 24, 2018), https://spectrum.ieee.org/michigans-midas-unemployment-system-algorithm-alchemy-that-created-lead-not-gold.
[40] Nikki Rojas, *Does AI help human make better decisions?*, The Harvard Gazette (June 14, 2024), https://news.harvard.edu/gazette/story/2024/06/does-ai-help-humans-make-better-decisions-artificial-intelligence-law/
[41] Imogen Parker, Anna Studman, Elliot Jones, *Learn fast and build things*, Ada Lovelace Institute (Mar. 14, 2025), https://www.adalovelaceinstitute.org/policy-briefing/public-sector-ai/.

government workers. That belief reflects a common tech fallacy: the idea that new tools alone can fix complex social problems. In reality, lasting improvements come from people and technology working together — not from technology alone.[42] Human expertise cannot be replicated by machines, even ones that are technically advanced.[43] Contrary to the view that AI and robots will inevitably replace workers, evidence shows that successful uses of new technology require human labor (usually undervalued and invisible[44]) to integrate them into existing infrastructures.[45] Ironically, if the administration wants to integrate AI systems into government services, it has made its job exponentially more difficult by firing more than 100,000 civil servants. Successful innovations are produced alongside workers and through careful integration with institutional experience. **Without worker expertise, the government is going to be left with costly AI systems that don't work.**

Finally, there are many reasons to doubt the government's claims that it is eliminating "waste, fraud, and abuse" through AI. For one thing, the numbers cited by the Trump administration to support its claims of savings have often failed to withstand scrutiny.[46] More to the point: crossing government programs off a balance sheet is not improving efficiency. Withholding public benefits is not eliminating fraud. AI may well prove helpful in specific circumstances for government operations. The Trump administration, however, is following a well-trodden path: its use of AI is simply cutting Americans off from vital public services.

A recent report by TechTonic Justice found that "the use of [AI in public benefits] over the past two decades demonstrates the capacity for broad, systemic harms with immense suffering at scales and speeds that were impossible with the human-centered methods that precede them."[47] Indeed, decades of the use of automated decision systems in public benefit distribution suggest that AI will not identify fraud, but instead will erroneously make opportunities more scarce and social insurance programs further inaccessible.[48] A 2009 example is instructive: After entering a $1 billion contract to modernize its public assistance systems through "remote eligibility" technology, the State of Indiana canceled the contract after more than one million residents had

[42] Brian J. Chen and Jacob Metcalf, *Explainer: A Sociotechnical Approach to AI Policy*, Data & Society Research Institute (May 28, 2024), https://datasociety.net/library/a-sociotechnical-approach-to-ai-policy/.
[43] Green, B. (2025, June 3). Using AI to reform government is much harder than it looks. *Tech Policy Press.* https://www.techpolicy.press/using-ai-to-reform-government-is-much-harder-than-it-looks/
[44] Mary L. Gray and Siddharth Suri, *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass* (May 2019).
[45] Alexandra Mateescu and Madeleine Clare Elish, *AI in Context: The Labor of Integrating New Technologies*, Data & Society Research Institute (Jan. 30, 2019), https://datasociety.net/library/ai-in-context/.
[46] Fahrenthold, D. and Singer-Vine, J. (2025, March 13). DOGE makes its latest errors harder to find. *The New York Times.* https://www.nytimes.com/2025/03/13/us/politics/doge-errors-funding-grants-claims.html; McCarthy, B. (2025, March 7). Fact-checking Trump's claims on DOGE spending cuts. *AFP Fact Check.* https://factcheck.afp.com/doc.afp.com.36ZC8HW
[47] Kevin De Liban, *Inescapable AI: The Ways AI Decides How Low-Income People Work, Live, Learn, and Survive* 7, TechTonic Justice (Nov. 2024), https://www.techtonicjustice.org/reports/inescapable-ai.
[48] *Id.*; Michele Gilman, *Poverty Lawgorithms*, Data & Society Research Institute (Sept. 15, 2020) https://datasociety.net/wp-content/uploads/2020/09/Poverty-Lawgorithms-20200915.pdf.

wrongly lost or been denied access to food stamps, Medicaid, and cash benefits — a 54 percent increase over three years.[49]

Empirically, user fraud in government programs is rare.[50] Yet the administration is marshaling new technologies, such as AI, to freeze out low-income people, disabled people, and people of color from government assistance.[51] These short-sighted attempts to target fraud reproduce the stigmatization of poverty, disability, race, and gender. The mistaken assumption that technology can "reduce fraud and increase efficiency only compounds inequality in the way that public benefits are delivered."[52]

The scholar Virginia Eubanks has critiqued how this "digital poorhouse" — the use of automated systems to determine benefits eligibility and fraud — "concentrates administrative power in the hands of a small elite. Its integrated data systems and digital surveillance infrastructure offer a degree of control unrivaled in history. Automated tools for classifying the poor, left on their own, will produce towering inequalities unless we make an explicit commitment to forge another path."[53]

This Committee has the important role of ensuring that the federal government is delivering on its promises to improve government services and programs. Unfortunately, the bulk of evidence suggests that the administration is using AI to consolidate control of public services, wind down public spending that helps Americans, and eliminate levers of accountability.

Third, in order to protect Americans' civil rights, the Committee must ensure that federal agencies follow the government's guidance on AI use and procurement.

The stakes of government procurement processes for AI are high. It is through purchasing that the government has the opportunity to define the goals of an AI system, articulate them to agency needs, and anticipate harms. Purchasing is also the primary opportunity to conduct risk assessments on AI for civil rights, privacy, cybersecurity, and other essential protections for

[49] Virginia Eubanks, *Want to Cut Welfare? There's an App for That*, The Nation (May 27, 2015), https://www.thenation.com/article/archive/want-cut-welfare-theres-app/.
[50] Michele Gilman, *AI algorithms intended to root out welfare fraud often end up punishing the poor instead*, The Conversation (Feb. 14, 2020), https://theconversation.com/ai-algorithms-intended-to-root-out-welfare-fraud-often-end-up-punishing-the-poor-instead-131625 (detailing that less than 1% of SNAP benefits go to ineligible households and that the majority of Medicaid fraudulent activity is committed by health care providers, not users).
[51] *See Poverty Lawgorithms* at 38; Alexandra Mateescu, *Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care*, Data & Society Research Institute (Nov. 16, 2021), https://datasociety.net/library/electronic-visit-verification-the-weight-of-surveillance-and-the-fracturing-of-care/.
[52] Serena Oduro, Brittany Smith, and Alexandra Mateescu, *Electronic Visit Verification: A Guide to Intersecting Harms and Policy Consequences* 9, Data & Society Research Institute (Nov. 16, 2021), https://datasociety.net/wp-content/uploads/2021/11/EVV_PolicyBrief_11162021.pdf.
[53] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (2018).

Americans. Building on the Biden administration's efforts, the Trump administration's recent Office of Management and Budget (OMB) guidance for AI use and procurement is well-aligned to these needs: it provides for a review of how existing tools meet agency needs, gives due consideration to problem formulation, prioritizes the need for a pilot and evaluation period, and stipulates requirements for data governance and stakeholder engagement.[54] It also includes a set of risk assessment and mitigation techniques that direct agency attention to the most high-risk systems to ensure Americans' rights and privacy are protected.

As federal agencies will soon be required to come into compliance with these OMB protocols, it will be critical for this Committee to ensure agency implementation. In the absence of such requirements — as the first few months of this administration have demonstrated — the government's unchecked acquisition of AI creates significant harm to the American public.[55] For example, earlier this year, the General Services Administration initiated a rapid rollout of "GSAi," a generative AI chatbot intended to reduce administrative burden.[56] Within a month, usage grew from 150 to 1,500 employees, then jumped to 13,000 users in a single day.[57] The rapid rollout of GSAi resulted in a number of problems, including data security concerns, integration issues, and diminished utility. Staff noted that the chatbot was deployed amid the rollback of essential tooling, like enterprise subscriptions to Adobe Acrobat, as well as staff layoffs.[58] The GSAi rollout bodes poorly for efficient and safe use of AI in the Trump executive branch; expediently adopted and flawed systems are being pushed through at scale at a time that staff is undergoing workforce reductions. Responsible AI procurement requires more lengthy evaluation periods to ensure that government work is proceeding cautiously and without errors. Procurement requirements matter because they serve as an internal pre-deployment check on the likelihood that AI systems will in fact deliver enhanced efficiency; the deep disruptions to federal agencies over the last few months are what happens when rapid adoption of AI is prioritized over a cautious and intentional deployment.

---

[54] The White House. (2025, April 7). *White House Releases New Policies on Federal Agency AI Use and Procurement.* The White House.
https://www.whitehouse.gov/articles/2025/04/white-house-releases-new-policies-on-federal-agency-ai-use-and-procurement/

[55] Larkin, C. J. (2025, May 1). 100 Days of DOGE: Assessing Its Use of Data and AI to Reshape Government. *Tech Policy Press.*
https://techpolicy.press/100-days-of-doge-assessing-its-use-of-data-and-ai-to-reshape-government

[56] Schiffer, Z. (2025, March 20). Elon Musk's DOGE Is Working on a Custom Chatbot Called GSAi. *WIRED*.
https://www.wired.com/story/doge-chatbot-ai-first-agenda/

[57] Heilweil, R. (2025, March 20). GSA debuts new generative AI tool for workers. *FedScoop*.
https://fedscoop.com/gsa-generative-ai-tool-doge/; Schiffer, Z. (2025, March 20). 'We Don't Want an AI Demo, We Want Answers': Federal Workers Grill Trump Appointee During All-Hands. *WIRED*.
https://www.wired.com/story/gsa-staff-all-hands-meeting-ai/

[58] Crumley, B. (2025, March 10). DOGE's AI App Replacing Fired Federal Workers Proves "About as Good as an Intern." *Inc.*
https://www.inc.com/bruce-crumley/doges-ai-app-replacing-fired-federal-workers-proves-about-as-good-as-an-intern/91158894; Schiffer, Z. (2025). 'We Don't Want an AI Demo, We Want Answers': Federal Workers Grill Trump Appointee During All-Hands. *WIRED*. https://www.wired.com/story/gsa-staff-all-hands-meeting-ai/; Wong, M. (2025, March 10). DOGE's Plans to Replace Humans With AI Are Already Under Way. *The Atlantic.*
https://www.theatlantic.com/technology/archive/2025/03/gsa-chat-doge-ai/681987/

Indeed, it is often the case that AI systems that appear dysfunctional and poorly designed are most effective at their real purpose: advancing agendas and rhetoric of government dismantlement and austerity.[59] Because AI is seen as rational and objective, it provides a technocratic smokescreen: a justification for firing federal workers, denying needed government benefits, or cutting necessary services.[60] But when these services are pared back, they are likely to fail, leaving the American people underserved and further decreasing trust in the government. In contrast with procurement processes that begin with identifying particular needs and determining whether AI can meet them, hasty adoption of low-quality tools will diminish the quality of and access to federal services.[61]

Government procurement protocols, although time consuming and complex, play an essential role in protecting Americans from harms. Specifically, the Trump administration's OMB Memo M-25-10 maintains that high risk systems must undergo pre-deployment review for efficacy and civil rights compliance:

> *"Agencies must complete an AI impact assessment before deploying any high-impact AI use case [of] the potential impacts of using AI, supported by documentation on potential impacts on the privacy, civil rights, and civil liberties of the public, and of using or not using AI. The assessment should reference privacy impact assessments, CAIO-approved minimum risk management practice waivers or other materials, if relevant, and also describe any planned mitigation measures for anticipated negative impacts, such as unlawful discrimination…conduct ongoing monitoring…ensure adequate human training…provide additional human oversight and accountability…offer remedies or appeals…and consult and incorporate feedback from end-users and the public."*[62]

This guidance is consistent with the gravity of the potential for harm. **Without careful evaluation and risk assessment, public agencies risk adopting expensive AI systems that violate people's rights and fail to work as intended.** Responsible adoption of AI takes time: time to identify impactful opportunities for computational tools, time to frame agency needs and requirements, time for stakeholder engagement, and time for intentional development, slow

[59] Bender, E. M., & Hanna, A. (2025). *The AI Con: How to Fight Big Tech's Hype and Create the Future We Want.* Harper.; De Liban, Kevin (2025, June 4). Austerity intelligence. *Tech Policy Press.* https://www.techpolicy.press/austerity-intelligence/
[60] Brennan, K., Kak, A., & Myers West, S. (2025). *Artificial Power: 2025 Landscape Report.* AI Now Institute. https://ainowinstitute.org/publications/research/ai-now-2025-landscape-report
[61] Salvaggio, E. (2025, February 9). Anatomy of an AI Coup. *Tech Policy Press*. https://techpolicy.press/anatomy-of-an-ai-coup
[62] Office of Management and Budget (2025). Accelerating Federal use of AI through innovation governance and public trust. OMB Memorandum No. M-25-21, page 17. https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf

rollout, testing, and course-correction. The reckless pattern of behavior adopted by DOGE evinces a disinterest in AI that actually serves Americans or government workers. Instead, it embraces the idea of AI as a panacea, throwing it at every problem without the attention and caution that the public deserves.

Congressional oversight will be critical to the implementation of OMB's recent AI use and procurement guidance. As those directives become live, this Committee should exercise its oversight authority to regularly require agencies to demonstrate compliance. External oversight will be key, as this administration has elsewhere shown a willingness to skip internal guardrails and flout institutional checks.[63]

Conclusion

The federal government's adoption of AI technologies should be guided by democratic values. Yet under the guise of efficiency and innovation, DOGE has unlawfully accessed sensitive data, deployed untested AI systems at scale, and circumvented critical safeguards in federal procurement. These actions do not merely risk technical failure. They erode the rule of law, weaken public trust, and potentially inflict material harm on millions of Americans, particularly the most vulnerable.

AI is being used not to modernize government, but to dismantle it. Launched without transparency or accountability, the systems we discuss in this document are already being used to fire civil servants, deny essential benefits, analyze private information, and centralize power. At the same time, lucrative government contracts are flowing to politically connected technology firms whose products undermine privacy and civil rights. This is not digital transformation; it is technocratic austerity cloaked in the rhetoric of progress.

The Committee's intervention is essential to prevent the normalization of unlawful, untested, and unsafe AI and data access practices across the federal government. We urge this Committee to exercise robust oversight, enforce compliance with federal privacy and procurement laws, and ensure that AI systems serve the public interest rather than private power.

[63] *See*, *e.g.*, Blake Brittain and Jeff Mason, *Judge rebukes Trump administration, demands to know status of illegally deported man*, Reuters (Apr. 11, 2025), https://www.reuters.com/legal/judge-orders-trump-administration-advise-its-steps-return-wrongly-deported-2025-04-11/.