

DOGE and Government Data Privacy

A resource in collaboration between Center for Democracy & Technology and The Leadership Conference's Center for Civil Rights and Technology

Last updated March 17, 2025

Despite the attention that the Department of Government Efficiency (DOGE) receives, little is known about their structure, staff, and actions, including how they are using data and technology to attempt to achieve their stated purpose of identifying and eliminating fraud, waste, and abuse in the federal government. This fact sheet is intended to summarize what is known about the evolution of DOGE's access to government-held data, including mounting lawsuits based on potential violations of federal privacy protections, growing security concerns, and impacts to millions of people, as well as some of the myriad outstanding questions about this new entity.

Evolution of DOGE and Government Data Privacy

While at first it was purported to be an advisory body, DOGE has transformed into an embedded group obtaining expansive access to government databases enabling them to seize the most sensitive information about tens of millions of people across the United States.

THEN

"[T]he Department of Government Efficiency will provide advice and guidance **from outside of Government** and will partner with the White House and Office of Management and Budget to drive large scale government reform...."

Source: [Statement on Truth Social from Donald Trump](#), November 12, 2024

NOW

"Agency Heads shall take all necessary steps, in coordination with the USDS [United States Digital Services] Administrator and to the maximum extent consistent with law, to ensure USDS **has full and prompt access to all unclassified agency records, software systems, and IT systems**. USDS shall adhere to rigorous data protection standards."

Source: [Excerpt from executive order establishing DOGE](#), January 20, 2025

By The Numbers

Fourteen lawsuits allege violations of **six** federal privacy protections across **eight** federal agencies.

Sources: [Just Security Litigation Tracker](#); [New York Times Lawsuit Tracker](#)

“Total information is total control.”

U.S. Senator Barry Goldwater

Source: [DOGE Betrays Foundational Commitments of the Privacy Act of 1974](#), February 7, 2025

Federal Privacy Protections

Personal data held by government agencies is protected under several long-standing federal privacy protections, including the following statutes that have been implicated in lawsuits directed at DOGE’s access to sensitive information:

- **Privacy Act of 1974:** The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of 12 statutory exceptions. This law was passed by Congress out of concern for curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal. **Source:** [Department of Justice Overview on the Privacy Act](#); [The Privacy Act](#).
- **§ 6103 of the Internal Revenue Code (IRC Section 6103):** IRC Section 6103 generally prohibits the release of tax information by an IRS employee except under specific circumstances. Privacy of tax information has been an American principle since 1870 — both administrative and legislative prohibitions on the sharing of taxpayer information were enacted that same year. The Internal Revenue Code was originally enacted in 1939 and then updated again in 1986, which is the current version we see today. **Source:** [26 USC 6103: Confidentiality and Disclosure of Returns and Return Information](#)
- **Fifth Amendment:** Substantive due process protects certain fundamental rights from government interference (grounded in the Fifth Amendment’s protection against deprivation of life, liberty, or property without due process). Infringements on such rights require a sufficient purpose and narrow tailoring to fulfill that purpose. **Source:** [Justia, Substantive Due Process](#)

Federal Privacy Protections (cont.)

- **E-Government Act of 2002:** The E-Government Act recognized that increased reliance on computers, the internet, and other technologies have important ramifications for the protection of personal information contained in government records and systems. Federal Information Security Management Act (FISMA) and Confidential Information Protection and Statistical Efficiency Act (CIPSEA), both portions of the E-Government Act, set security standards and requirements for agencies in their maintenance of data. FISMA generally requires agencies to have a documented security system in place, and CIPSEA prevents the use of data or information that was acquired by an agency confidentially for statistical purposes from being used for any other (nonstatistical) purpose. **Source:** [Federal Information Security Modernization Act of 2014](#); [Confidential Information Protection and Statistical Efficiency Act](#)
- **Computer Fraud and Abuse Act (CFAA):** The CFAA makes it a criminal act to access a government computer without authorization, obtain information on a government computer that one is not authorized to obtain, share information with unauthorized people, or inhibit government operations without authorization. **Source:** [Computer Fraud and Abuse Act](#)
- **§1306 of the Social Security Act:** Section 1306 of the Social Security Act prohibits the disclosure of any tax return information (or portion of return information) by officers or employees of the Social Security Administration and the Department of Health and Human Services, except under specific circumstances. **Source:** [Disclosure of information in possession of Social Security Administration or Department of Health and Human Services](#)

Reported Security Incidents & Sensitive Data Collected

DOGE's access to sensitive information raises serious questions about the extent to which they are adhering to appropriate privacy and security practices and federal law. Reported security incidents include:

- DOGE staffer Marko Elez was '**mistakenly**' given '**read/write**' permissions over part of the Treasury Department payment system responsible for disbursing trillions of dollars every year. **Source:** [Treasury revoked editing access 'mistakenly' given to DOGE staffer](#), February 11, 2025
- The doge.gov website that was spun up to track Elon Musk's cuts to the federal government is **insecure** and pulls from a database that can be edited by anyone. **Source:** [Anyone Can Push Updates to DOGE Website](#), February 14, 2025

Reported Security Incidents & Sensitive Data Collected (cont.)

- DOGE released information about the headcount and budget of an intelligence agency. Multiple intelligence community sources [said] that this likely represents a **significant breach**...because anytime any details about U.S. citizens working for one of the intel agencies is released, it puts their safety in jeopardy. **Source:** [DOGE data release criticized by intel community; Trump admin says it's public data](#), February 14, 2025
- Twenty-one staffers of the U.S. DOGE Service announced their resignations Tuesday citing, among other worries, **“mishandling sensitive data.”** Within the White House complex, the **WiFi permissions** — meant to bolster security by prompting users to log in frequently — were recently changed to allow guests to remain logged in for a year, up from seven days, because **so many personal devices** are newly in use. **Source:** [DOGE's grab of personal data stokes privacy and security fears](#), February 25, 2025

These reported security incidents are particularly troubling given the extremely sensitive nature of the data that the federal government collects about individuals, including the examples below.

Examples of Sensitive Data Collected By Federal Agencies						
Identifying Information	Demographics	Contact Information	Life Events	Financial Information	Beneficiary Information	Alleged Legal Violations
Legal name	Race	Work and mobile phone numbers	Pregnancy and birth	Family income	Medical diagnoses and conditions	Domestic violence case files with addresses of survivors
Date of birth	Sex	Home and work addresses	Marriage and divorce	Family information	Past treatments and procedures	Detailed descriptions of civil rights violations, including sexual assaults
Social Security Number	Disability	Email address	Job loss	Bank account information	Mental and behavioral health history	Incarceration
Beneficiary identifier	Citizenship status		Employment records	Credit reports and scores	Prescription drug use	
			Bankruptcy	Loan requests and denials	Hospital bills	
			Family deaths		Housing information	

Impact of Artificial Intelligence Use on Government Data

Emerging stories about how artificial intelligence (AI) may be used to make high-stakes decisions, like firing tens of thousands of federal workers, replacing federal workers, and cutting billions in funding, do not account for limitations of the technology, like inaccuracy, lack of security, and bias. The public may find themselves on the receiving end of AI-driven decisions that upend their access to fundamental government services like Social Security, Medicare, and Medicaid.

- The DOGE team is **using AI software** accessed through Microsoft's cloud computing service Azure to pore over every dollar of money the department disburses, from contracts to grants to work trip expenses, one of the people [with knowledge of the DOGE team's actions] said. **Source:** Elon Musk's DOGE is feeding sensitive federal data into AI to target cuts, February 6, 2025
- Allies of Elon Musk stationed within the Department of Education are reportedly considering replacing some contract workers who interact with millions of students and parents annually with an **artificial intelligence chat bot**. **Source:** Musk Staff Propose Bigger Role for A.I. in Education Department, February 13, 2025
- A senior Elon Musk staffer apparently has **created a custom AI chatbot** that purports to help the Department of Government Efficiency eliminate government waste and is powered by Musk's artificial intelligence company xAI. **Source:** Elon Musk staffer created a DOGE AI assistant for making government 'less dumb,' February 18, 2025

Impact of Improper DOGE Data Access and Use

Collecting, accessing, and sharing sensitive information carries inherent risk to the people who provide the data, making it important to ensure that the potential benefits outweigh the harms. Individuals whose data are being accessed and used by DOGE are at risk of experiencing the following harms:

- **Data misuse and privacy invasion:** DOGE's access to sensitive personal information, including Social Security Numbers and personal health information, threatens people's privacy and may even violate long-standing federal privacy protections. Without additional transparency about why and to what extent DOGE has accessed personal data, potential legal violations and other misuses of data may occur without the public's awareness. **Source:** At least 11 lawsuits are taking on DOGE over data access and privacy laws, February 19, 2025

Impact of Improper DOGE Data Access and Use (cont.)

- **Increased risk of fraud and identity theft:** DOGE's potentially reckless treatment of personal data undermines basic privacy and cybersecurity practices, exposing such information to heightened risks of misuse, leakage, and attacks. If such information is hacked by scammers or foreign adversaries, people are likely to see their data used against them for fraud and identity theft. **Source:** [4 ways to protect your personal data from Musk's DOGE](#), March 1, 2025
- **Federal operations confidentiality:** DOGE's practices also threaten the data privacy of federal employees and the confidential work many of them do. The implementation of a new, government-wide email system to collect millions of data points on federal employees creates significant security vulnerabilities as email is widely understood to be insecure. This practice, along with using AI to assess responses to government-wide queries, threaten both confidential personnel information and information about sensitive government operations. **Source:** [DOGE will use AI to assess the responses of federal workers who were told to justify their jobs via email](#), February 24, 2025
- **Hindering government efficiency and wasting taxpayer dollars:** While the use of data and AI systems can play a legitimate role in increasing government efficiency, DOGE is reportedly using these tools to make high-risk decisions about a host of government programs and hiring. Without appropriate oversight, transparency, and testing, AI tools may not only fail to function properly and reduce government efficiency, thus wasting taxpayer dollars, but can cause significant harm to individuals by producing inaccurate and biased results. **Source:** [The truth about DOGE's AI plans: The tech can't do that](#), March 3, 2025

“This continuing, unauthorized disclosure of the plaintiffs' sensitive personal information to DOGE affiliates is irreparable harm that money damages cannot rectify.”

US District Judge Deborah Boardman in the District of Maryland

Source: [Judge: US gov't violated privacy law by disclosing personal data to DOGE](#), February 25, 2025

Unanswered Questions

In December 2020, President Trump signed Executive Order 13960 that put forth nine principles, including transparency, that federal agencies were directed to meet regarding their use of AI. This executive order is still in place; however, not only is there little clarity around how DOGE is using AI, but there is little known about fundamental data, privacy, and security questions. Without additional transparency about how DOGE is accessing and using the data of millions of people, several key questions remain unanswered:

- **Data Access:** What data systems and related data elements have been accessed by DOGE staff? When were they accessed? Who has accessed the systems or been shown the data? Are they employees of the agency that collects and maintains this information?
- **Data Use:** How has the information been used to identify fraud, waste, and abuse? Has the information been used for reasons beyond fraud, waste, and abuse? What steps are being taken to ensure that such data is not being used to target vulnerable communities, including immigrants, trans people, and people seeking reproductive care?
- **Data Security:** What measures have been taken to secure the data accessed by DOGE? Has it been downloaded, moved, relocated, or sold, and if so where, by whom, and to whom? What type of training has DOGE staff received on how to safely handle and understand this information? How were DOGE staff recruited? Do they have proper clearance to handle sensitive data?
- **AI:** How have AI and other predictive technologies been used to identify purported fraud, waste, and abuse, like making decisions to fire people or to eliminate funding, grants, and programs? Are the AI tools fit for purpose? What are the systems' capabilities and limitations? Has the data accessed by DOGE been used to train or further develop AI tools? Are the AI tools evaluated? What mechanisms are in place to identify and correct errors and minimize harm?

“Part of what is unnerving and is scary both to companies whose data is involved and also Americans whose most sensitive financial information is at risk, is that we don't know what they're doing.”

Erie Meyer, former chief technologist at the Consumer Financial Protection Bureau

Source: [The government already knows a lot about you. DOGE is trying to access all of it](#), March 11, 2025

Additional Information on Personal Data Collected and Maintained by Federal Agencies

U.S. Department of Education:

- [What information will I need to fill out a FAFSA® form?](#)
- [Musk team's access to student loan systems raises alarm over borrowers' personal information](#), February 7, 2025

U.S. Department of Health and Human Services:

- [House Committee on Education and Workforce Letter on DOGE HHS Data Access](#), February, 21, 2025
- [Congressional Letter to HHS Inspector General on DOGE Data Access](#), February 7, 2025
- [Congressional Letter to HHS and CMS on DOGE Data Access](#), February 7, 2025
- [DOGE Aides Search Medicare Agency Payment Systems for Fraud](#), February 5, 2025
- [DOGE broadens sweep of federal agencies, gains access to health payment systems](#), February 5, 2025

U.S. Department of Housing and Urban Development:

- [HUD Enforcement Management System \(HEMS\)](#)
- [HUD Privacy Impact Assessment \(PIA\)](#)
- [DOGE Gains Access to Confidential Records on Housing Discrimination, Medical Details — Even Domestic Violence](#), February 26, 2025

U.S. Department of Labor:

- [House Committee on Education and Workforce Letter on DOGE DOL Data Access](#), February 21, 2025
- [DOGE software approval alarms Labor Department employees](#), February 13, 2025

U.S. Department of the Treasury:

- [IRS Gather Your Documents](#)
- [DOGE presses to check federal benefits payments against IRS tax records](#), March 1, 2025
- [Musk Team Seeks Access to I.R.S. System With Taxpayers' Records](#), February 1, 2025
- [Elon Musk's Team Now Has Access to Treasury's Payments System](#), February 1, 2025
- [How an arcane Treasury Department office became ground zero in the war over federal spending](#), February 1, 2025

U.S. Department of Veterans Affairs:

- [Veterans Benefits Administration](#)
- [Privacy Impact Assessment for the VA IT System](#), October 10, 2023
- [Elon Musk Aide Is Now Working at VA and Accessing Its Computer Systems](#), February 1, 2025

Social Security Administration:

- [Form SSA-1 | Information You Need To Apply For Retirement Benefits Or Medicare](#)
- [Understanding Supplemental Security Income Documents You May Need When You Apply -- 2024 Edition](#)
- [Baldwin Demands Answers from Social Security Administration on Musk and DOGE's Access to Personal Information](#), February 25, 2025

Questions? Contact techcenter@civilrights.org or civictech@cdt.org