# Understanding DOGE and Your Data:
# A Guide for Citizens and Policymakers

*Over the past several weeks, the Department of Government Efficiency (DOGE) within the Trump Administration has been embedding staff in a range of United States federal agencies. These staff have gained access to data maintained by the federal government. This guide explains what is in the data, what DOGE is doing with it, and why it matters to all Americans.*

## I. What are those federal datasets and what do they have to do with me?

<u>What data does the federal government have about me?</u>

The federal government maintains comprehensive records of Americans' interactions with government services. Government records include not only basic information like your name, address, birthday, and Social Security number, but a much broader range of data. Any time you submit a government form, file an application or your taxes with the government, register a complaint, or receive a service, these interactions become data in a government database. For example, the government maintains detailed records of:

- **Financial information:** Your tax returns, federal benefits, and any government payments.
- **Health information:** Your Medicare, Medicaid, or Veterans Administration (VA) records.
- **Social Services and Public Benefits information:** Information regarding any social services you may have applied for, including food assistance (WIC, SNAP), social security and disability income, and housing assistance
- **Education information:** Your educational history in federal student aid records and any government-funded research.
- **Immigration information:** Any visa or immigration benefits for which you applied, or information on applications for individuals you have sponsored.

You may have other data stored by the government as well. For example, if you've ever held a security clearance or government job, there are extensive background check records, including what your former colleagues and neighbors said about you. If you've ever served in the armed forces, your service records, including your mental health records, are held by the federal government. Data like employment records, fingerprints and facial recognition data, immigration status may also be included. Some private records (for example, private health data) may have been accessed by the government if needed for national security or law enforcement purposes.

This is sensitive data. Many private data sets, like social media profiles or consumer records, show only what you choose to share and may not be fully verified. In contrast, government databases contain authenticated data collected by law.

### What does the government normally use this data for?

The data maintained by the federal government is essential to running the government and providing public services. For example, tax records enable fair collection of revenue and distribution of benefits; healthcare data allow the VA, Medicare, and Medicaid to provide care and track outcomes; and education records allow the government to manage student aid and measure program effectiveness. Every function of the federal government, from law enforcement to border protection to managing the economy, depends on robust, accurate data.

Because this data is so valuable and sensitive, the federal government has guardrails in place to ensure it is used appropriately. By law, federal agencies are required to:

- Use the data only for authorized purposes
- Protect it from unauthorized access
- Maintain accurate records of who accesses which data
- Keep data separated between agencies, unless those agencies are specifically authorized to share

### Who normally has access to this data? What qualifications and safeguards are there?

Access to government data is traditionally strictly controlled through multiple layers of protection. Historically, all federal employees have been required to undergo some form of background check to ensure they are  reliable, trustworthy, and suitable for the job, and they must obtain appropriate “clearances” before accessing sensitive data. Higher-level clearances and access to more sensitive data and information require more extensive and rigorous background checks that examine criminal records, financial history, foreign contacts, and other potential security risks, among other things.

In addition to security clearances, access to government data follows “need-to-know” principles. Even employees with security clearances can only access data necessary for their specific roles. Systems maintain detailed logs of who accesses what information and when, and regular audits ensure compliance with these restrictions. Most importantly, access to data is subject to strict privacy protections.

## II. What is DOGE doing with my data?

What is DOGE?

The Department of Government Efficiency (DOGE), formerly the United States Digital Service (USDS), was established by executive order in 2025 under Elon Musk's leadership, with a stated goal of modernizing government operations. Unlike typical government agencies, DOGE is operating without clear limits to its authority, little or no oversight, and little transparency.

Since its formation, DOGE has been granted or has seized unprecedented access to government systems and data across agencies. Its employees often do not have security clearances and have not met the security clearance requirements even as they gain broad access to sensitive systems.

Who from DOGE has access to my data?

Multiple DOGE employees have gained extensive access to government systems containing Americans' sensitive personal data.

At the Treasury Department, DOGE personnel have obtained access to payment systems that process trillions of dollars in government transactions. DOGE employees have "read" access, and at least one employee temporarily had "edit" access as well, meaning that they would be able to both see and alter the data. At the Consumer Financial Protection Bureau, DOGE employees have "read access" to sensitive financial data. Most concerning, DOGE is seeking to give team members access to IRS systems containing hundreds of millions of tax returns and other sensitive tax information.

This access extends across multiple agencies. While the Treasury Department recently prohibited access to personal taxpayer data, DOGE was not blocked from accessing data at seven other major agencies including the Office of Personnel Management and Departments of Commerce, Education, Energy, Labor, Health and Human Services, and Transportation.

Critically, the information made public about data access is almost certainly incomplete. Because DOGE is not providing transparency about their actions, what is known is based on reports from journalists and those inside agencies. In some cases, the employees in charge of managing access to data, who could have seen what DOGE is doing, have been removed from their posts, limiting Americans' ability to know what is happening.

### Are DOGE employees qualified and authorized to handle my data?

In many cases, they are not. Unlike the government employees that traditionally handling sensitive data, many DOGE team members lack standard security clearances, would likely not have been able to obtain those clearances, or do not have relevant experience. For example, the director of Technology Transformation Services requested access to 19 different IT systems without completing basic background checks.

This represents a dramatic departure from normal security protocols. Without proper clearances, there is no no evaluation of personal integrity or reliability, no assessment of potential foreign influence, and no verification of loyalty to the United States. There is also no confirmation that employees have had the training required to responsibly handle the sensitive data of millions of Americans. Recent reports suggest that DOGE engineers have failed basic technical competency tests administered by the DOGE hiring team.

### Why does DOGE want access to my data?

DOGE's stated mission focuses on government efficiency, but the wide-ranging appropriation of valuable and sensitive data suggests broader ambitions.

For example, Musk may be interested in using personal data for his businesses, since he has publicly claimed "the cumulative sum of human knowledge has been exhausted in AI training." Unlike the messy, unverified data available on the Internet, government databases contain comprehensive, verified information about real-world behaviors and outcomes. This data could enable AI systems to understand and predict societal patterns in ways currently impossible with public data sources. Using sensitive personal data about Americans could give Musk's companies significant advantages over competitors.

DOGE may also be interested in using personal data to take more control over the government. As described above, data is essential to every government program. With access to the government's data on Americans, including the ability to alter and even delete that data, DOGE can shape the operation of the government as it sees fit, regardless of the law.

Unfortunately, Americans can only speculate as to what DOGE wants to do with the data, because DOGE is not providing basic transparency about its intentions and methods.

## III. What are the risks of DOGE accessing my data?

### Why does “read-access” to Americans’ data matter?

DOGE team members have “read-access” to Americans’ data across numerous federal agencies, ranging across the Social Security Administration, Health and Human Services, the Department of Education, the Veterans Administration, and more. Read-access allows those individuals to do the following without any checks or accountability:

- Copy your data to use for unauthorized and unlawful purposes
- Deny you access to public services, benefits, and opportunities such as: medical care, housing, food or student financial assistance, veteran or military benefits, public contracts, and more.
- “Doxx” (share personal information online) or threaten you
- Provide or sell your data to foreign governments, data brokers, and/or private companies (including those that Musk or other DOGE members run or work for)

### Could my data be altered, manipulated, or deleted?

Yes, and this represents one of the most serious risks. Unlike traditional government employees who have read-only access to most systems, some DOGE personnel have been granted edit-access to critical databases at USAID and are requesting this access at other federal agencies. This means they could alter records, modify transaction data, or even erase evidence of their actions.

The implications are particularly concerning for government payment systems. With both read and edit access to Treasury systems, DOGE personnel could modify payment records, redirect funds, or interfere with benefits distribution while covering their tracks. With read-only access, your data could still be copied for other uses.

### Will my data be leaked?

The risk of data leaks is substantial. Without proper training, security clearances, or oversight, DOGE personnel could copy or transfer sensitive data outside government systems. These leaks could be the result of accidents, deliberate targeting of individuals, or transactions with outside parties who want to buy your sensitive personal data. Your personal data could then be used by private companies, scammers, foreign governments, and others for whatever purposes they like. DOGE recently shared sensitive information on their public-facing website, including data on budget and staffing at the National Reconnaissance Office spy agency, which was not intended for public release. This data leak raises national security risks.

The Electronic Privacy Information Center has already filed suit against OPM, Treasury, and DOGE over data breach concerns.

## Could my data be used against me?

Yes, and the risks are both immediate and long-term. In the short term, unauthorized access has already enabled targeting of individuals for harassment. For example, some employees of the United States Agency for International Development (USAID) have been "doxxed," i.e., had their personal information released publicly, after DOGE accessed personnel files. Federal workers are reporting fear of political retaliation, with FBI officials particularly concerned about the targeting of those perceived as disloyal to the administration. While these examples involve federal employees, the data DOGE is accessing would enable similar attacks against many Americans who do not work for the federal government.

For example, DOGE could use this data to target Americans with ties to immigrants. Many Americans sponsor visa applicants or sign affidavits of support guaranteeing that the applicant will not need to rely on public benefits such as SNAP. Any immigrant applying for permanent residence or coming to work in the United States must have an American financial sponsor, meaning millions of Americans have sponsored immigrants. An administration hostile toward immigration could use this information to target Americans with ties to immigrants, even if they are in the United States legally. IRS data accessed by DOGE was recently used to target and cancel contracts to religious organizations that support refugee resettlement.

The longer-term risks are even more concerning. Beyond identity theft or fraud, comprehensive access to government data could enable unprecedented capabilities for prediction and influence of citizen behavior. An AI system trained on this data could understand not just individual patterns but societal-scale relationships between policies and outcomes. Today, consumer technology companies often use customer data to predict and manipulate the actions of their users. A government that uses data without appropriate safeguards could do the same to the American public.

What would any of that mean for my life?

The impacts could range from personal inconvenience to systemic harm. On an individual level, leaked data could enable identity theft, financial fraud, or targeted harassment. Your private information and identity "credentials" could be revealed, alterned, or even deleted.

More broadly, the ability to analyze and manipulate government data at scale could enable unprecedented capabilities for social control and economic influence, not only by the American government but by anyone with access to the data, including foreign nations.

## IV. How real are these concerns?

Why would the richest man in the world want my personal data?

The quality of AI systems depends on the data used to train them. Much of that data is information scraped from the internet that can be messy, biased, or unreliable, and leading AI companies now spend enormous sums of money to buy higher-quality data. Government databases offer something fundamentally different: comprehensive, verified records about the most critical areas of Americans' lives. At least one prominent technology executive has suggested that the United States and other countries consolidate all of their national data into a single dataset that could be used to train AI models, though the American public has not consented to personal data being used for these purposes.

Access to Americans' data could give Musk's companies significant advantages in training AI systems and in setting business strategy. For example, X, formerly known as Twitter and owned by Musk, aims to become the "Everything App," which customers could use for a wide range of tasks, including payments. A rich source of Americans' financial data could help X succeed.

Musk may also be interested in taking over critical government functions for profit. Weakening the government, while simultaneously taking Americans' personal data, could allow Musk to profit by filling the gap.

If used responsibly and in the public interest, AI might enable capabilities far beyond current government systems. By allowing AI to analyze the results of everything from healthcare outcomes to the impact of economic policies, public data might enable a more efficient and effective government. However, if used recklessly and without oversight, the data could allow certain private companies to profit from our sensitive information and foreign governments to better understand how to harm America.

### Aren’t these concerns just paranoia?

The safeguards for government data were put in place over years to protect Americans. The destruction of those safeguards is not just a possibility - it is already happening. The worst possible outcomes of that destruction might happen tomorrow or in five years, but given the scale of DOGE’s activities, they are very likely. Americans can lose critical services, be targeted for harassment and attacks, or be subject to discrimination. Just as importantly, we can be manipulated by the government, private actors, or foreign powers.

The combination of comprehensive government data access and advanced AI capabilities could enable unprecedented, unauthorized control over the American people. This represents a fundamental challenge to democracy and the freedom of every American as an individual.

Last updated: Feb. 28, 2025

Contributors include: Vivian Graubard, Alex Pascal, Nick Pyati, Bruce Schneier, Allison Stanger, and Kinney Zalesne.