

Trump is enabling Musk and DOGE to flout conflicts of interest

What is the potential cost to U.S. families?

Report • By [Celine McNicholas](#) and [Ben Zipperer](#) • May 7, 2025

SECTIONS

Summary:

- By removing certain ethical requirements for civil servants, appointing billionaire Elon Musk as a “special government employee,” and granting DOGE unprecedented access to sensitive government data, Trump has created multiple avenues for Musk and his team to exploit their political positions for their own personal gain.
- There is no evidence of Musk filing ethics forms or addressing any potential conflicts of interest since his appointment as a civil servant. Trump said that Musk will identify his own conflicts, which is in and of itself a conflict.
- Musk and DOGE team members—who are working in government despite having clear private sector interests—now have unprecedented access to nonpublic data that is highly valued in the burgeoning data broker industry. Even if their data access yielded just 10% of the market insights provided by that data broker industry, it would be worth \$43.4 billion.
- If Musk leveraged his access and influence to double the value of federal contracts awarded to his companies, he would capture \$23.6 billion in federal spending.
- Musk and DOGE’s unrestrained and careless access to sensitive data like Social Security numbers will no doubt exacerbate the problem of identity theft in the United States. If current victimization rates doubled, identity theft would affect 50 million people and cost them \$39.4 billion annually.

1. Ethical safeguards • 3
2. Access to federal agencies’ data • 4
3. Federal contracts • 5
4. Identity theft • 8
5. Conclusion • 10

Acknowledgements • 11

Notes • 11

References • 11

Across the federal government, civil servants and political appointees have access to unique datasets, contracting processes, or other insights at their agencies that may be of significant value or interest to private companies. Many administrations of both political parties have long recognized this dynamic and put in place strong ethics standards to limit the ability of individuals to personally profit from their federal service, either during or after their tenure. This includes declaring all financial interests, declaring contacts when traveling abroad, and divesting from or receiving waivers for

identified conflicts. For example, individuals at agencies like the Food and Drug Administration are not allowed to hold individual stocks of companies whose products are significantly regulated by the agency (e.g., pharmaceutical companies).

Ethics standards to prevent conflicts of interest or the misuse of valuable government information—including nonpublic economic performance data, trade secrets, and patents—are essential. And since government officials have the power to make market-moving decisions, the public needs to be assured that they are making those decisions for the public good and not for their own benefit. Since taking office, President Trump has removed some ethics requirements and allowed Elon Musk and the so-called Department of Government Efficiency (DOGE) unprecedented access to personal and proprietary information across multiple federal agencies that could be enormously beneficial to Musk’s business dealings (Weissert 2025).

Elon Musk, as a special government employee, should have filed multiple ethics forms, received briefings, and worked to address all conflicts, whether by recusing himself or divesting from certain assets. However, there is no evidence that he has filed any ethics forms (the White House has confirmed that none are available) and Trump has stated that Musk will identify his own conflicts, which is in and of itself a conflict (COR 2025; Kamisar 2025). Trump removed the typical guardrails protecting the public from compromised government decision-makers to allow the richest man in the history of the world shape U.S. government policy.

Beyond cuts to the federal workforce and programs that have put core government services at risk, Musk and DOGE team members have the potential to personally profit from their positions. Musk and DOGE’s unprecedented access, with virtually no oversight or guardrails, also creates data privacy risks.

In this report, we examine how Trump’s removal of certain ethical requirements for public servants, his appointment of Musk under the unique status as a “special government employee,” and DOGE’s unconventional structure and authority create opportunities for Musk and others to leverage their federal service for their own personal profits. Indeed, there is real potential for Musk and DOGE to blur the line between federal service and private interests. Further, we estimate the potential cost of identity theft if the personal information Musk and DOGE now have access to is not properly safeguarded.

While DOGE’s wide-ranging activities have likely created many conflicts of interests for Musk and its team members, in this report, we focus on their potential to exploit two areas:

1. Musk and DOGE’s access to large swaths of sensitive and personal data, including Internal Revenue Service (IRS) data, Social Security data, and federal payment systems, among others; and
2. DOGE’s potential ability to influence the awarding of federal contracts.

Leveraging this access to personal data and influence over federal contracts can be extremely lucrative. We estimate that the potential personal profit from access to U.S. individuals’ personal data stands at tens of billions of dollars. Even if DOGE and Musk’s

unprecedented access to nonpublic government data yielded just 10% of the market insights provided by data brokers, it would be worth \$43.4 billion. And if Musk doubled the number of federal contracts awarded to his companies, he would capture \$23.6 billion in federal spending. Lastly, we consider how granting DOGE and its staff access to sensitive personal data, such as IRS data, could lead to an increase in identity theft—and how much this potential surge in identity theft would cost U.S. families. If current identity theft victimization rates doubled, 50 million people would be affected each year by identity theft, with total personal losses reaching \$39.4 billion annually.

Ethical safeguards

The United States has long recognized and guarded against individuals using their positions within government for personal gain and at the expense of the public interest. Today, there are processes, disclosure requirements, and ethical standards in place to ensure federal employees place loyalty to the Constitution and the execution of our laws above their private gain.¹ The current structure and activities of DOGE—and the special employment status of Elon Musk in particular—raise serious questions about the ability of these long-standing ethical safeguards to protect the public interest.

Among the numerous and detailed uniform ethics standards for all executive branch employees, individuals are generally prohibited from “[engaging] in financial transactions using nonpublic Government information or [allowing] the improper use of such information to further any private interest” and “[engaging] in outside employment or activities, including seeking or negotiating for employment, that conflict with official Government duties and responsibilities.”² There are also detailed post-employment standards to limit the unfair use of prior government employment access and knowledge.

Trump and his staff following ethical standards is a general cause for concern but the activities of DOGE are uniquely ripe to be leveraged for personal gain. Unlike most other individuals working in the White House, Elon Musk was hired as a “special government employee,” which has typically been used to streamline the hiring of an individual who is performing work on a temporary basis (Hernandez 2025). As a special government employee, Musk is only allowed to work 130 days in a 365-day period. While special government employees are allowed to hold outside employment, they are still bound by several ethical requirements, including the duty to not engage in outside employment that “that conflict[s] with official Government duties and responsibilities.”³ At a minimum, the nature and volume of Musk’s businesses combined with the activities of DOGE raise the appearance of a conflict of interest—if not direct and serious financial conflicts. As discussed in more detail below, DOGE and Musk have gained direct access to a range of nonpublic data and information which could be used to inform business interests, both now and in the future. In April 2025, Musk announced that he would scale back his DOGE work to one or two days per week, focusing the remaining time on his businesses (Swan et al. 2025). At a time when Musk has publicly admitted to directly advising the President to take certain policy actions that would benefit his companies—such as reducing tariffs—and using the backdrop of the White House to bolster the image of Tesla, it’s clear

that Musk has already blurred the lines between his government work and business dealings (Swan et al. 2025; Pager 2025). Yet these actions may only be a small preview of the multitude of ways Musk can leverage his government position for private gain, both now and well after he exits government.

Access to federal agencies' data

In one of his first executive orders, Trump directed agency heads to provide DOGE with “full and prompt access to all unclassified agency records, software systems, and IT systems.”⁴ Since then, DOGE has embedded team members in agencies across the federal government and sought to gain unprecedented access to extremely detailed and sensitive data (Siddiqui and Bogage 2025). This includes data held by the IRS, the Social Security Administration, and the Center for Medicare and Medicaid Services, among other agencies (Wamsley 2025). While the full breadth of access to these data has been limited to “read only” files in some instances and is still being litigated in court in others, DOGE's access to these data poses a range of potential risks, particularly to the security of data that identify specific individuals (Pascal et al. 2025).

Beyond the immediate concerns about how DOGE is using these data, courts and Congress should recognize that DOGE team members who are in an ethically dubious employment situation—working in government despite having clear business interests in the private sector—have also gained access to data that are highly sought after and valued in the private sector.

Today, firms have a strong demand for individual-level consumer data to inform their business decisions. There are several firms that acquire and then sell a range of personal data to other companies, sometimes at a steep cost. These firms are often referred to as data brokers. Generally, data brokerage companies acquire data on individuals directly from the consumers that are purchasing or using the company's products, by purchasing the data secondhand from other companies, or by scraping government websites that contain public records (Sherman 2021). As the Federal Trade Commission has explained, these data brokers in turn combine data on individuals, such as their income, location, spending patterns, or educational attainment to create categories of consumers (e.g., “working-class mom,” “financially challenged,” or “affluent baby boomer”) that they then sell to advertisers and other companies (FTC 2014). Individuals and companies that purchase these data and insights may use it for different reasons, including for marketing and targeting ads or informing other business strategies.

The data broker market is a rapidly growing industry. According to one estimate, the global market was valued at roughly \$434 billion in 2025 and is expected to exceed \$616 billion by 2030 (Research and Markets 2025). The data broker industry has increasingly received attention from state and federal regulators given the potential risks it poses to consumers. Last year, the Consumer Financial Protection Bureau proposed a rule to limit the ability of data brokers to sell personally identifying data, including Social Security numbers.⁵ The rule would also ensure that individuals' financial data, such as details about their income, are only used for legitimate purposes like mortgage approval.

In the context of a quickly growing market where top firms are racing towards bigger and better data, it's concerning that DOGE and Elon Musk have gained access to the very kind of data that would be sold in the data broker market and used to inform key business decisions. Alarming, as the *New York Times* has reported, DOGE is attempting to stitch together various datasets from across the government to compile far more detailed and complete information on individuals (similar to how data brokers create categories of consumers; Badger and Frenkel 2025).

While it's difficult to pinpoint a specific estimate on the value of these data, in part because the true value is in insights an entity could glean or leverage, access to one-of-a-kind data would evidently give DOGE staff unprecedented market advantages. Specifically, access to government data that contains sensitive information, like individuals' Social Security numbers, as well as comprehensive information on entire markets of consumers not held by nongovernment data sources, could lead to unique insights that could be leveraged by DOGE staff to gain a market advantage in specific markets. For example, how might DOGE's access to complete sets of tax returns inform the future development of AI software that could be sold to the more than \$14 billion tax preparer industry (McErlaine 2025)? Or how might DOGE's access to combined data on financial records (such as mortgages or student loans) be used to inform business dealings in lending markets down the road? Or how might these data inform bids on future contracts as federal agencies significantly downsize and contract out certain services in the future?

These aren't far-fetched hypotheticals. The seemingly revolving door between DOGE activities and private companies is already in motion with Musk returning his attention to his businesses. And others on the DOGE team are also well positioned to do the same, such as the senior DOGE staffer at the Department of Housing and Urban Development who is on leave from a property technology company reported to be "on a long-term mission to aggregate the hardest to find data" (Elliott and Gilbert 2025).

The various ways that DOGE and Musk may utilize their access to these data for personal gain, both in the short term and in years to come, may never fully be known. But as DOGE continues to stitch together nonpublic, sensitive data from across agencies, it's clear that the opportunities to abuse this access are countless. In many ways, it appears that DOGE is doing exactly what data brokers in the private sector are doing—combining sensitive and unique datasets to provide actionable insights across a range of markets. It doesn't require connecting too many dots to intuitively understand the profit windfall DOGE and Musk stand to gain from a mere few months of access to some of the country's most sought-after data. But just how much is this all actually worth? Consider this: If DOGE and Musk leverage their government access to gain just 10% of the market insights afforded by data brokers in the private sector, the data would be valued at \$43.4 billion.

Federal contracts

The Government Accountability Office (GAO) estimates that in fiscal year 2023, the federal government spent over \$759 billion on contracts (GAO 2023). This includes contracts for military aircraft, food pantries, vaccines, dialysis care for veterans, and other services that

working people rely on. While most federal contracts relate to our national defense, government contracting impacts almost all sectors.

As the federal government is an extremely large purchaser, federal contracts are highly coveted by companies. Long-term federal contracts can account for a sizable portion of a company's business or help give it an edge over its competitors. The process for bidding on and securing a federal contract has long been executed by career civil servants to ensure that the most qualified providers are chosen based on merit.

Generally, before a contract is put out to bid, an agency will publish a Request for Information to understand the landscape of providers, scope of services offered, and reasonable costs. Private-sector actors respond to these public requests and their answers are analyzed and used to create a Request for Proposals in which the government explains what it needs and then the bidding process begins. When a simplified acquisition process is allowed, the government can simply request quotes for a service or invite sealed bids and award the contract to the lowest bidder.

The federal contracting process is designed to ensure that the people in the U.S. are getting the lowest price for the best service and to prevent political or personal considerations from informing decisions. Staff that are involved in contracts, even tangentially, must declare all potential conflicts of interest and recuse themselves if they ever stand to gain from awarding a contract to a particular company.

Elon Musk has not recused himself from issues that might impact his companies and is already exerting significant influence and sway over federal agencies (Hernandez 2025). There is a real possibility that he could leverage his position to direct lucrative federal contracts to his own companies, rather than to the best provider.

Musk's companies have received a total of \$38 billion in government contracts, loans, subsidies, and tax credits over the last 20 plus years (Butler et al. 2025). The real number is probably even larger, because contracts that relate to national security are not made public. In 2023, his companies were promised over \$3.8 billion in just that year across nearly 344 different contracts. According to the *Washington Post*, Musk's companies recently held 52 contracts with seven agencies, totaling \$11.8 billion over the life of the contracts (Lipton et al. 2024; Butler et al. 2025).

Since the beginning of Trump's second administration, there have been concerns that Musk has or would use his position—directly or indirectly—to secure additional federal contracts. For example, he explicitly attacked a Verizon contract with the Federal Aviation Administration (FAA) worth \$2.4 billion, arguing that Starlink should provide the service instead. Though that contract does not seem to have been canceled, Starlink is leasing its technology for free to the FAA and the White House. It is unclear how Starlink is being used or integrated into ongoing operations, but Musk is clearly signaling his hope to win this contract in the future. When Microsoft offered services for free, it became too expensive for the government to switch providers when, as with all free trials eventually, the company began to charge (Dudley 2025). Musk's company SpaceX is currently proposing to the Pentagon the construction of the "Golden Dome" missile system "as a 'subscription service' in which the government would pay for access to the technology,

rather than own the system outright” (Stone and Taylor 2025).

Another contract that has been under scrutiny is a \$400 million Cybertruck contract for armored vehicles. Under the Biden administration, a contract one hundredth of the size was approved for electric vehicles; Cybertrucks, nearly all of which have been recalled due to safety issues, would have been an unusual choice even for that smaller contract (Lyon 2025). While the administration backtracked once it was questioned, Musk is no doubt seeking additional contracts to bolster flagging sales (Allyn 2025). And individual contracts are just the tip of the iceberg. Musk’s businesses could easily pursue several large contracts across the federal government, including space, telecoms, car, and AI contracts.

Space contracts

In fiscal year 2023, NASA had contract obligations of approximately \$22.3 billion. SpaceX received the second largest amount overall (\$2.25 billion) after only CalTech (GovExec Space Project 2024). However, with access to potentially secret information about his competitors thanks to his new federal role, Elon Musk is poised to claim an even greater percentage of available funds.

Furthermore, the first week of April 2025, SpaceX replaced the United Launch Alliance as the top Space Force contractor for this grant round, winning a contract worth just under \$6 billion (Albon 2025).

Telecoms contracts

Telecommunications is another very lucrative possible area for additional contracts for Musk. The GAO estimates that the government spends approximately \$30 billion each year on telecommunications, mostly by the Department of Defense (GAO 2020). Additionally, the Department of Commerce manages a \$42 billion fund to provide broadband access to the rural United States (Lipton 2025). Under the Biden administration, Starlink was not eligible because the program was prioritizing systems that wired homes directly, as opposed to satellite networks. However, since the 2024 election, the Department of Commerce has changed its criteria, opening up an enormous new source of potential contracts. Musk had criticized the former policy, and it is possible his large donations to Trump may have softened their stance on this issue.

Car contracts

Departments across the government require cars, the majority of which are contracted through the General Services Administration (GSA; defense vehicles follow a separate process). While Ford currently holds a \$8.5 billion contract with GSA, Musk is trying to supply additional vehicles to the federal government. This could be a very lucrative and important lifeline for Musk, given the plummeting sales of Teslas around the globe (Isidore 2025). Trump recently hosted a car show on the White House lawns, touting the benefits

of Teslas, demonstrating the President’s keen awareness of Tesla’s troubles (Ingram 2025).

AI contracts

The federal government is adopting artificial intelligence (AI) tools to help deliver services more efficiently. The Brookings Institution estimates that the potential value of current AI contracts across the federal government is approximately \$4.561 billion (Larson et al. 2024). As Musk seeks to grow xAI, to which he recently sold another one of his companies X (formerly known as Twitter), AI contracts could be another potentially lucrative new area and important revenue stream for Musk (Ortutay 2025).

Due to his privileged role, Musk now has access to secret contracting information on his competitors that should not be available to the competition. This means he can potentially outcompete his rivals and grow the share of federal dollars going to his companies. Additionally, his enormous donations to President Trump are already leading to changes in government policy that benefit his businesses—how much pressure will he exert on career staff, who are already facing illegitimate firings from Musk, in service of his companies?

Overall, what is a reasonable assessment of how much Musk stands to gain? If Musk’s companies became 1.5 times as effective at obtaining federal contracts, that would increase their contract income over the next several years from \$11.8 billion to \$17.7 billion. Were they to become twice as effective at obtaining federal contracts, their contract income would rise to \$23.6 billion.

Beyond using his current position to outcompete or influence decision-makers about existing federal contracts, there’s a very real possibility that DOGE’s dismantling of core government services and functions is setting up a dynamic where federal agencies contract out services and functions that were previously executed by federal employees. Musk would be well positioned to advise and create bids from his companies to secure those contracts.

Identity theft

The changes imposed by Musk and DOGE will likely exacerbate identity theft in the United States. As the *New York Times* has reported, the data accessed by DOGE and Musk capture hundreds of different types of information valuable to identity thieves and scammers (Badger and Frenkel 2025). For example, from just one database (the National Directory of New Hires), DOGE accessed the names, Social Security numbers, personal addresses, wage information, employer names and addresses, and unemployment claims of virtually every single employee in the United States (King 2025).

This information can be enough to start a bank account, file for a fraudulent tax refund, take out a loan, or claim Social Security benefits. This is especially concerning given DOGE’s poor track record for keeping sensitive, confidential data secure. Recently, a National Labor Relations Board (NLRB) whistleblower observed that large amounts of

sensitive data were extracted from the NLRB right around the time DOGE gained access (McLaughlin 2025). In February 2025, 21 employees of the U.S. Digital Service (the precursor to DOGE) resigned, stating that DOGE was “firing technical experts, mishandling sensitive data, and breaking critical systems” (Garrison 2025).

In addition to the potential for data leaks or stolen information, DOGE’s attacks on government services like IRS and Social Security provide an increased opportunity for identity theft and government benefits fraud. For example, sudden changes requiring in-person verification at Social Security were exploited by scammers, who sent phishing messages to recipients “to verify their identity to keep receiving benefits” (Rein and Natanson 2025). The sudden revocation of Social Security numbers legally obtained by immigrants will increase the relative value of stealing valid Social Security numbers, as this increasingly becomes the only way immigrants can file work authorization papers with their employers (Berzon et al. 2025).

Identity theft is already a widespread, costly social problem. Nearly one in ten (9%) people in the United States were victims of identity theft in 2021, according to the Bureau of Justice Statistics National Crime Victimization Survey—a comprehensive survey that fielded questions about identity theft to about 133,000 residents ages 16 and over (Harrell and Thompson 2023). If the victimization rate stayed the same, 25.1 million people experienced identity theft in 2024 (see **Table 1**).⁶

In 2021, about 59% of identity theft victims experienced an average personal financial loss of \$1,160 (Harrell and Thompson 2023). Perpetrators of identity theft used personal information to open a new financial accounts or misuse existing bank or credit card accounts. Victims also incurred other types of costs, like bounced checks and legal fees. Assuming victims experienced similar losses in 2024 and after adjusting for inflation, we estimate that total personal financial losses due to identity theft were \$19.7 billion in 2024.

These large sums may underestimate financial losses due to identity theft; some private-sector researchers have estimated that the aggregate costs of identity theft amounted to \$27 billion in 2024 (Pitt 2025). In addition, personal costs understate the total social costs of identity theft. The estimated personal costs exclude any losses to commercial entities like stores and banks, as well as efficiency losses, as resources are diverted to resolve identity theft related problems. For example, employees will spend fewer hours working and more time dealing with financial problems. Indeed, Harrell and Thompson (2023) found that victims spend about 4.6 hours of time trying to resolve a single incident of identity theft. At estimated 2024 rates, Table 1 shows that this implies over 116 million hours were spent attempting to resolve financial or credit problems associated with a single identity theft incident.

Table 1 also provides a range of increased costs due to an increase in the prevalence of identity theft—a likely scenario given the unprecedented access and carelessness of Musk and the DOGE team. If victimization rates were to increase by 50%, 37.7 million people would be affected by identity theft annually. A doubling of these rates would bring the number of affected people each year to 50 million, with total personal losses reaching \$39.4 billion annually.

Table 1

Identity theft could affect 50 million people annually if current rates double

Estimated identity theft in 2024 at current rates and under possible increases

	Current rates	50% increase	100% increase
Number of victims, annual	25,120,000	37,681,000	50,241,000
Total dollars lost, annual	\$19,705,606,000	\$29,558,409,000	\$39,411,213,000
Total hours spent resolving a single incident	116,258,000	174,386,000	232,515,000

Notes: The estimate of victims is the 2024 Census resident population, ages 16 and above, using the 2021 victimization rate, mean dollars lost (adjusted for inflation since 2021), and mean hours spent from Harrell and Thompson's analysis of Bureau of Justice Statistics data (2023).

Sources: Authors' analysis of Bureau of Justice Statistics data, the chained CPI-U, and Census population estimates.

Economic Policy Institute

Conclusion

Trump's removal of certain ethical standards for federal service, his establishment of DOGE, and his appointment of Elon Musk as a special government employee have not only created opportunities for Musk and others to personally profit from public service, but have also increased the risks of U.S. individuals having their personal data mishandled or their identity stolen. Trump has allowed Musk and DOGE unprecedented access to personal and proprietary information across multiple federal agencies that could be enormously beneficial to Musk's business dealings.

Elon Musk, as a special government employee, should have filed multiple ethics forms, received briefings, and worked to address all conflicts, whether by recusing himself or divesting from certain assets. Instead, Trump stated that Musk will identify his own conflicts—a conflict of interest, in and of itself—and there is no evidence from the White House that he has filed any ethics forms. Further, Congressional Republicans have blocked attempts for oversight of DOGE and Musk (Nihill 2025). The guardrails that are usually in place to protect the public from compromised government decision-makers have been removed or disregarded to allow the richest man in the history of the world to influence U.S. government policy. All of this while Musk could potentially profit from access to personal data and federal contracts and potentially cost working people in the U.S. \$39.4 billion annually in personal losses related to identity theft if data is mishandled.

Acknowledgements

The authors wish to acknowledge Patrick Oakford and Cassandra Robertson for their contributions to the research and development of this paper.

Notes

1. 5 C.F.R. § 2635 (2025).
2. 5 C.F.R. § 2635 (2025).
3. 5 C.F.R. § 2635 (2025) and 5 C.F.R. § 9001.105 (2025).
4. [Establishing and Implementing the President’s Department of Government Efficiency](#), 90 Fed. Reg. 8441-8442 (January 20, 2025).
5. [Protecting Americans from Harmful Data Broker Practices \(Regulation V\)](#), 89 Fed. Reg. 101402-101462 (December 13, 2024).
6. In 2024, there were about 276 million residents ages 16 and over according to estimates from the U.S. Census Bureau (2025).

References

- 5 C.F.R. § 2635 (2025).
- 5 C.F.R. § 9001.105 (2025).
- Albon, Courtney. 2025. [“Space Force Issues \\$13.5 Billion in Contracts to 3 Launch Firms.”](#) Defense News, April 4, 2025.
- Allyn, Bob. 2025. [“A New Document Undercuts Trump Admin’s Denials About \\$400 Million Tesla Deal.”](#) NPR, February 24, 2025.
- Badger, Emily, and Sheera Frenkel. 2025. [“Trump Wants to Merge Government Data. Here Are 314 Things It Might Know About You.”](#) *New York Times*, April 9, 2025.
- Berzon, Alexandra, Hamed Aleaziz, Nicholas Nehamas, Ryan Mac, and Tara Siegel Bernard. 2025. [“Social Security Lists Thousands of Migrants as Dead to Prompt Them to ‘Self-Deport’.”](#) *New York Times*, April 10, 2025.
- Butler, Desmond, Trisha Thadani, Emmanuel Martinez, Aaron Gregg, Luis Melgar, Jonathan O’Connell and Dan Keating. 2025. [“Elon Musk’s Business Empire Is Built on \\$38 Billion in Government Funding.”](#) *Washington Post*, February 26, 2025.
- Dudley, Renee. 2025. [“Microsoft Hooked the Government on Its Products with Freebies. Could Elon Musk’s Starlink Be Doing the Same?”](#) ProPublica, April 5, 2025.
- Elliott, Vittoria, and David Gilbert. 2025. [“DOGE Staffers at HUD are From an AI Real Estate Firm and](#)

a [Mobile Home Operator](#).” *Wired*, February 26, 2025.

Federal Trade Commission (FTC). 2014. [Data Brokers: A Call for Transparency and Accountability](#). May 2014.

Garrison, Joey. 2025. “[21 Federal Technology Workers Resign in Protest of Elon Musk’s DOGE](#).” *USA Today*, February 25, 2025.

Government Accountability Office (GAO). 2020. [Telecommunications and Call Centers: Observations on Federal Contracting Practices](#). Report to Congressional Requesters, April 2020.

Government Accountability Office (GAO). 2023. [A Snapshot: Government-Wide Contracting](#).

GovExec Space Project. 2024. “[Top 100 NASA Contractors 2023](#)” (web page). July 19, 2024.

Harrell, Erika, and Alexandra Thompson. 2023. [Victims of Identity Theft, 2021](#). Bureau of Justice Statistics, October 2023.

Hernandez, Joe. 2025. “[Trump Hired Musk as A ‘Special Government Employee.’ Here’s What That Means](#).” NPR, February 13, 2025.

Ingram, David. 2025. “[Trump Turns the White House Lawn Into A Tesla Showroom](#).” NBC News, March 11, 2025.

Isidore, Chris. 2025. “[Tesla Sales Plunge: Biggest Decline in History](#).” CNN, April 2, 2025.

Kamisar, Ben. 2025. “[How the White House is Handling Elon Musk and Potential Conflicts of Interest](#).” NBC News, March 21, 2025.

King, Ryan. 2025. “[DOGE Staffer Marko Elez, Who Had Resigned over Racist Posts, Gains Access to Sensitive Government HR Data](#).” *New York Post*, April 1, 2025.

Larson, Jacob, James S. Denford, Gregory S. Dawson, and Kevin C. Desouza. 2024. [The Evolution of Artificial Intelligence \(AI\) Spending by the U.S. Government](#). Brookings Institution, March 2024.

Lipton Eric. 2025. “[Musk Is Positioned to Profit Off Billions in New Government Contracts](#).” *New York Times*, March 23, 2025.

Lipton, Eric, David A. Fahrenthold, Aaron Krolik and Kirsten Grind. 2024. “[U.S. Agencies Fund, and Fight With, Elon Musk. A Trump Presidency Could Give Him Power Over Them](#).” *New York Times*, October 20, 2024.

Lyon, Peter. 2025. “[Tesla Recalls Nearly Every Cybertruck Due to Potential Crash Risk](#).” *Forbes*, March 23, 2025.

McErlaine, Brendan. 2025. [Tax Preparation Service in the US – Market Research Report \(2015 – 2030\)](#). IBIS World, March 2025.

McLaughlin, Jenna. 2025. “[A Whistleblower’s Disclosure Details How DOGE May Have Taken Sensitive Labor Data](#).” NPR, April 15, 2025.

Nihill, Caroline. 2025. “[House Oversight Republicans Block Democrats’ Inquiry into Musk’s Conflicts of Interest](#).” FedScoop, April 9, 2025.

Ortutay, Barbara. 2025. “[Elon Musk Sells X to His Own xAI for \\$33 Billion in All-Stock Deal](#).” *Associated Press*, March 29, 2025.

Pascal, Alexander, Allison Stanger, Bruce Schneier, Kinney Zalesne, Nick Pyati, Sarah Hubbard, and Vivian Graubard. 2025. “[Understanding DOGE and Your Data](#)”, Harvard Kennedy School, March 31, 2025

Pager, Tyler. 2025. “[Trump, an E.V. Naysayer, Gives Tesla and Musk a White House Exhibition.](#)” *New York Times*, March 11, 2025

Pitt, Jennifer. 2025. [2025 Identity Fraud Study: Breaking Barriers to Innovation](#). Javelin Strategy and Research, March 25, 2025.

Rein, Lisa, and Hannah Natanson. 2025. “[Long Waits, Waves of Calls, Website Crashes: Social Security Is Breaking Down.](#)” *Washington Post*, March 25, 2025.

Research and Markets. 2024. [Data Broker Markets – Forecasts from 2025 to 2030](#). December 2024.

Siddiqui, Faiz, and Jacob Bogage. 2025. “[Some DOGE Staffers Hold High-Powered Jobs at Multiple Federal Agencies.](#)” *Washington Post*, April 14, 2025.

Sherman, Justin. 2021. [Data Brokers and Sensitive Data on U.S. Individuals](#). Duke Sanford Cyber Policy Program, August 2021.

Stone, Mike, and Marisa Taylor. 2025. “[Exclusive: Musk’s SpaceX Is Frontrunner to Build Trump’s Golden Dom Missile Shield.](#)” Reuters, April 17, 2025.

Swan, Jonathan, Maggie Haberman, Nicholas Nehamas, Theodore Schleifer, and David A. Fahrenthold. 2025. “[A Subdued Musk Backs Away From Washington, but His Project Remains.](#)” *New York Times*, April 23, 2025.

U.S. Census Bureau. 2025. “[Annual Estimates of the Resident Population by Single Year of Age and Sex for the United States: April 1, 2020 to July 1, 2024.](#)” National Population by Characteristics: 2020–2024. Last updated April 9, 2025.

U.S. House Committee on Oversight and Reform (COR). 2025. [Letter to White House Counsel David Warrington](#). May 1, 2025.

Wamsley, Laurel. 2025. “[The Government Already Knows A Lot About You. DOGE Is Trying to Access All of It.](#)” NPR, March 11, 2025.

Weissert, Will. 2025. “[Trump Has Canceled Biden’s Ethics Rules. Critics Call It the Opposite of ‘Drain the Swamp.’](#)” Associated Press, January 22, 2025.