

Congress of the United States

Washington, DC 20515

June 17, 2025

Alex Karp
Chief Executive Officer
Palantir Technologies
1200 17th Street, Floor 15
Denver, CO 80202

Dear Mr. Karp:

We write to demand information regarding reports that Palantir Technologies (“Palantir”) is enabling and profiting from serious violations of Federal law by the Trump Administration, which is amassing troves of data on Americans to create a government-wide, searchable “mega-database” containing the sensitive taxpayer data of American citizens.¹

According to press reports, Palantir employees have reportedly been installed at the Internal Revenue Service (“IRS”), where they are helping the agency use Palantir’s software to create a “single, searchable database” of taxpayer records.² The sensitive taxpayer data compiled into this Palantir database will likely be shared throughout the government regardless of whether access to this information will be related to tax administration or enforcement,³ which is generally a violation of federal law. Palantir’s products and services were reportedly selected for this brazenly illegal project by Elon Musk’s Department of Government Efficiency (DOGE).⁴ Several DOGE members are former Palantir employees.

The unprecedented possibility of a searchable, “mega-database” of tax returns and other data that will potentially be shared with or accessed by other federal agencies is a surveillance nightmare that raises a host of legal concerns, not least that it will make it significantly easier for Donald Trump’s Administration to spy on and target his growing list of enemies and other Americans. This potential “mega-database” at the IRS and elsewhere also raises myriad potential violations of privacy laws designed to strictly limit those who can access the tax return records of individuals and businesses, specifically the Internal Revenue Code and the Privacy Act of 1974.

As you are aware, tax returns and return information are subject to strong legal privacy protections under Sections 6103 and 7213A of the tax code.⁵ These laws were strengthened nearly 50 years ago with strong bipartisan majorities of Congress in response to President Nixon’s abuse of the IRS to target his political enemies.⁶ These prohibitions have long prevented political appointees in previous administrations from accessing the private tax records of hundreds of millions of Americans, and allowing the government to create a master database of taxpayer records that will be shared with other government agencies may be in violation of these statutes. Violations of these taxpayer privacy laws, including unauthorized access to or disclosure of tax

1 Sheera Frenkel and Aaron Krolak, “Trump Taps Palantir to Compile Data on Americans,” The New York Times, May 30, 2025, <https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html>.

2 Id.

3 Donald J. Trump, Executive Order 14243: Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, Executive Office of the President, March 20, 2025, <https://www.whitehouse.gov/presidential-actions/2025/03/stopping-waste-fraud-and-abuse-by-eliminating-information-silos/>

4 Frenkel and Krolak, “Trump Taps Palantir.”

5 26 U.S. Code § 6103 - Confidentiality and disclosure of returns and return information; 26 U.S. Code § 7213A - Unauthorized inspection of returns or return information.

6 26 U.S. Code § 7217 - Prohibition on executive branch influence over taxpayer audits and other investigations

returns and return information, can result in criminal penalties, including incarceration. In one recent example, a contractor working for the IRS who leaked taxpayer information was sentenced in 2024 to five years in federal prison.⁷

While Section 6103 of the tax code prohibits any unauthorized disclosure of tax returns or information contained in tax returns, Section 7213A also makes it unlawful for any federal officer, employee, or authorized viewer to willfully inspect a return or return information for a purpose other than one specifically authorized by law, with inspection defined expansively, to include “any examination of a return or return information.”⁸ Therefore, improper inspection of tax return information is illegal, even if it has not been made public or disclosed to anyone.

For inspection of taxpayer information to be lawful, it must be made to or by an authorized person for an authorized purpose. While Treasury employees, such as IRS personnel, can access tax return information for their official duties involving tax administration, such as conducting audits or processing tax returns, they generally may not access them for reasons unrelated to those purposes. In addition, there are significant restrictions on access to tax return information for others in the employ of the federal government, including contractors.

What is more, the Privacy Act of 1974 provides general safeguards against the federal government’s processing of personal information about U.S. citizens and lawful permanent residents. Under the Act, the government is required to, among other things, publish in the Federal Register “each routine use” of personal information held by agencies and describe the users and “purpose of such use.” The government must also publish “the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal” of the information. Further, when data is shared across agencies for use in matching programs, the computer matching provisions of the Privacy Act specify several procedural requirements, including the creation of a matching agreement with specific requirements before that sharing happens.

The IRS hiring Palantir to help it establish a “mega-database” of government-held personal data, including sensitive taxpayer data, for seamless processing for a limitless number of purposes blatantly violates the notice, transparency, and procedural requirements of the Privacy Act. As you should be aware, contractors are explicitly covered by many of the Privacy Act’s requirements.⁹ Palantir, including individual Palantir employees, can face civil and criminal liability for violating the Privacy Act.

Palantir's troubling assistance to the Trump Administration is not limited to its work for the IRS. According to press reports, Palantir’s work for Immigration and Customs Enforcement (ICE) includes helping the Administration “leverage data to drive enforcement operations” by “producing leads for law enforcement to find people to deport and keeping track of the logistics of Trump’s mass deportation effort.”¹⁰ Such an opaque tool in the hands of an Administration that openly violates the due process rights of immigrants is a grave threat

⁷ U.S. Department of Justice, “Former IRS Contractor Sentenced for Disclosing Tax Return Information to News Organization,” January 29, 2024, <https://www.justice.gov/archives/opa/pr/former-irs-contractor-sentenced-disclosing-tax-return-information-news-organizations>.

⁸ 26 U.S. Code § 6103(b)(7); 26 U.S. Code § 7213A(c).

⁹ 5 U.S. Code § 552a(m) (explicitly applying the criminal provisions of the Privacy Act to contractors and their employees); 5 U.S. Code § 552a(a)(9) (“[T]he term “recipient agency” means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program”).

¹⁰ Joseph Cox, “Leaked: Palantir’s Plan to Help ICE Deport People,” 404 Media, April 17, 2025, <https://www.404media.co/leaked-palantirs-plan-to-help-ice-deport-people/>; Marisa Franco, “Palantir Filed to Go Public. The Firm's Unethical Technology Should Horrify Us,” The Guardian, September 4, 2020, <https://www.theguardian.com/commentisfree/2020/sep/04/palantir-ipo-ice-immigration-trump-administration>.

to our Constitution. Former acting IRS Commissioner Melanie Krause, acting Chief Counsel Bill Paul, and Chief Privacy Officer Kathleen Walters all appear to have resigned or been reassigned over the IRS's agreement with ICE.¹¹

Furthermore, you have bragged that Palantir enables its military customers to “bring violence and death to our enemies” and that your software is “used by U.S. and allied defense and intelligence agencies for functions like target selection and mission planning.”¹² We are concerned that Palantir's software could be used to enable domestic operations that violate Americans' rights. Donald Trump has personally threatened to arrest the governor of California, federalized National Guard troops without the consent of the governor for immigration raids, deployed active-duty Marines to Los Angeles against the wishes of local and state officials, condoned violence against peaceful protestors, called the independent press “the enemy of the people” and abused the power of the federal government in unprecedented ways to punish people and institutions he dislikes.

The Trump Administration has spent taxpayer dollars on Palantir software at numerous other government agencies and paid it billions of dollars to conduct similar data gathering efforts.¹³ For example, the Department of Defense recently awarded Palantir a \$795 million contract to lead data fusion and artificial intelligence programs throughout the U.S. military, with the possibility to increase the award to \$1.3 billion.¹⁴ Additionally, the Trump Administration has deployed Palantir's Foundry software at the Department of Homeland Security, Department of Health and Human Services, Food and Drug Administration, Centers for Disease Control and Prevention and National Institutes of Health.

Palantir is certainly not the first American company to earn huge profits by enabling violations of human rights by authoritarian governments. For example, IBM sold computers to South Africa's apartheid-era government that the regime used to maintain racial classification records. Before that, the company sold punch card machines that the Nazis used to run concentration camps. Cisco custom-built the so-called “Great Firewall of China,” which enables the Chinese government to conduct surveillance and censorship against its citizens. More recently, Gatekeeper Intelligence Security sold facial recognition technology to the repressive monarchies of Saudi Arabia and the United Arab Emirates and Honeywell helped Egypt's military dictatorship build an AI-powered network of surveillance cameras.

Congress will fully investigate and hold accountable Trump Administration officials that violate Americans' rights, as well as contractors like Palantir that profit from and enable those abuses. Accordingly, we request that you preserve any emails, text messages or other records related to Palantir's work for the Trump Administration in anticipation of future litigation and Congressional oversight. Please also provide answers to the following questions no later than July 10, 2025:

1. Please provide a list of all current Palantir contracts with the United States government. For each contract, please provide the following information: the dollar value of the award, the agency that awarded the contract, the name of the Palantir software or product being deployed as part of the contract, and a detailed description of the services being performed as part of the contract.

¹¹ Nathan Layne and Kanishka Singh, “Top IRS Officials Join Chief in Quitting Following Immigration Data Deal,” Reuters, April 9, 2025, <https://www.reuters.com/world/us/us-irs-chief-quit-over-deal-share-data-with-immigration-officials-report-says-2025-04-08/>.

¹² Palantir Technologies Inc., “Q3 2024 Earnings Call Transcript,” The Motley Fool, November 4, 2024, <https://www.fool.com/earnings/call-transcripts/2024/11/04/palantir-technologies-pltr-q3-2024-earnings-call-t/>; Alexander C. Karp, “Our Oppenheimer Moment: The Creation of A.I. Weapons,” The New York Times, July 25, 2023, <https://www.nytimes.com/2023/07/25/opinion/karp-palantir-artificial-intelligence.html>.

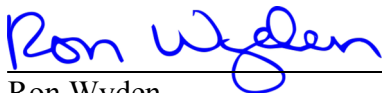
¹³ Frenkel and Krolik, “Trump Taps Palantir.”

¹⁴ Sandra Erwin, “Pentagon Boosts Budget for Palantir's AI Software in Major Expansion of Project Maven,” SpaceNews, May 22, 2025, <https://spacenews.com/pentagon-boosts-budget-for-palantirs-ai-software-in-major-expansion-of-project-maven/>.

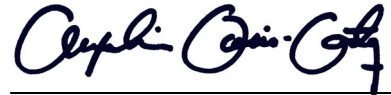
2. Has Palantir sought or received assurances from the U.S. government that its executives, board members, and employees will not be held responsible for violations of federal law, including the internal revenue code?
3. Has Palantir provided insurance coverage or commitments to pay legal costs and fines to any of its executives, board members, or employees in connection with the company's work for the U.S. government or any foreign government.
4. What services, features, or assistance, if any, has the Trump Administration requested and Palantir declined to provide, due to concerns related to privacy, civil liberties, or potential violations of federal, state, or international law.
5. Is Palantir aware of the requirements placed on agencies and contractors by the Privacy Act of 1974? Have you advised the government of those requirements, or offered to assist in their compliance? Do you believe the government is currently satisfying its requirements under the Privacy Act?
6. Does the company have a "red line" for potential violations of human rights, U.S. law or international law by the Trump Administration that would result in Palantir terminating its services for the U.S. government?
7. How many Palantir employees have quit since January 20, 2025, citing the company's work for the Trump Administration?

Thank you for your attention to this important matter. Should you have any questions please do not hesitate to reach out to us or our staff.

Sincerely,



Ron Wyden
United States Senator
Ranking Member, Committee on
Finance



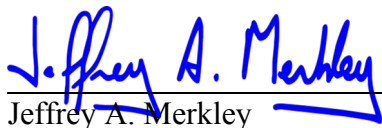
Alexandria Ocasio-Cortez
Member of Congress



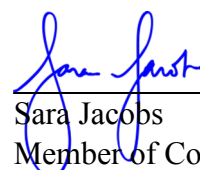
Elizabeth Warren
United States Senator



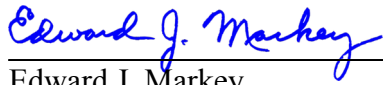
James P. McGovern
Member of Congress



Jeffrey A. Merkley
United States Senator



Sara Jacobs
Member of Congress



Edward J. Markey
United States Senator



Rashida Tlaib
Member of Congress



Summer L. Lee
Member of Congress



Paul D. Tonko
Member of Congress