AI and PLANATIR

Several article. . . .

Our country is in dangerous territory--as the march goes forward with AI and the fusing of data by Palantir, a data mining company--the next generation DOGE. This article gives an eagle eye view as to what is happening, as Palantir pools citizen data into a master file on Americans with a composite profile and spreadsheet on each person, merging information from different agencies, "wiring together every government dataset." There will be a dossier on every American.

It is a " a legal blueprint for a vast, centralized surveillance infrastructure — without guardrails, oversight, or external review." The groundwork is being laid right now through Palantir for the "largest surveillance infrastructure" in US history, gutting our 4th Amendment right. It is one of the reasons the Big Beautiful Bill has a section in it where states will not be able to regulate it. PC

https://thenewamerican.com/us/tech/palantir-to-build-centralized-database-on-americans/

Palantir to Build Centralized Database on Americans

by Veronika Kyrylenko June 2, 2025

The Trump administration is quietly assembling a centralized data infrastructure on the American population. To build it, they've enlisted Palantir, a powerful data-mining company with deep ties to the intelligence world. Co-founded by Peter Thiel — Trump's longtime ally and megadonor — Palantir was originally seeded by the CIA to help the government make sense of large, fragmented data sets.

In March, Trump signed an executive order demanding that agencies "eliminate information silos." The language sounds bland, even bureaucratic. But the real implications are sweeping. By ordering agencies to pool citizen data, Trump signaled interest in something once unthinkable: a master file on American lives.

According to *The New York Times*, Trump hasn't spoken publicly about the plan since. But behind the scenes, his administration has moved quickly.

The Order

Signed on March 20, the order is titled "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos." It presents mass data consolidation as a bureaucratic fix. "Removing unnecessary barriers to Federal employees accessing Government data," it reads, will help eliminate "bureaucratic duplication" and detect fraud.

But the order's power lies in its fine print:

- It gives "designated Federal officials" sweeping access to all unclassified agency records, software systems, and data across departments.
- It orders agencies to remove internal sharing restrictions within 30 days, and grants the federal government "unfettered access" to state-level data programs, even if stored in third-party databases.
- It overrides previous executive orders and suspends regulatory safeguards that might slow it down.

Critics say the result is clear: a legal blueprint for a vast, centralized surveillance infrastructure — without guardrails, oversight, or external review.

DOGE

Much of the groundwork has been laid by the Department of Government Efficiency (DOGE), not so long ago led by Elon Musk — Thiel's longtime business partner. Officially tasked with "modernizing federal technology and software," Musk described his mission in deceptively simple terms: "making computers talk to each other."

But beneath that phrase lies a sweeping "AI-first" agenda. As *The New American* has tracked, since its inception, DOGE has been embedding artificial intelligence across federal agencies — automating analysis, standardizing systems, and preparing government data for large-scale consolidation.

Foundry

To continue the implementation of the order, the administration turned to Palantir — the firm built to do exactly this. Since Trump's return to office, Palantir has received over $113 million in federal contracts, plus a new $795 million deal with the Department of Defense (DOD). At the center is Palantir's flagship product: Foundry.

Foundry is not just an analytics tool. It's a full-scale data operating system. Palantir describes it as a "central platform for data-driven decision making and situational intelligence" designed to pull together fragmented sources — from spreadsheets and real-time feeds to legacy federal databases — into a single, unified view.

At its core is Ontology, a semantic engine that turns raw data into high-fidelity, interactive objects. These objects represent real-world entities like people, payments, events, and relationships. Foundry uses them to build composite profiles, simulate outcomes, and automate decisions. Palantir calls it “closed-loop analytics” — in which the system doesn’t just analyze data, it acts on it.

One official told the *Times* that Foundry makes it easy “to merge information from different agencies.” That’s exactly what it’s doing.

Foundry is already embedded in the Department of Homeland Security (DHS), Health and Human Services (HHS), and the Internal Revenue Service (IRS), where Palantir engineers are constructing a searchable database of taxpayer records. Expansion talks are underway with the Social Security Administration (SSA) and the Department of Education.

Palantir and the Deep State

Palantir could be considered the Deep State’s private-sector arm. Founded in 2003 with seed funding from In-Q-Tel — the CIA’s venture wing — Palantir was built to turn surveillance into software, automating what intelligence agencies once did manually.

Before Palantir, analysts sifted through siloed data — satellite feeds, phone logs, visa records, financial reports — by hand. Palantir’s platforms changed that. They ingest fragmented data streams, map relationships in real time, and flag patterns of interest. What once took days of human labor now takes seconds of computation.

Palantir holds contracts with the DOD, CIA, National Security Agency (NSA), FBI, Immigration and Customs Enforcement (ICE), DHS, and HHS. It supports battlefield analytics, predictive policing, and pandemic logistics, and is expanding into financial surveillance through the IRS and SSA.

The company runs two flagship platforms. Gotham, designed for military and intelligence use, helps track insurgents, map networks, and flag suspicious activity. In Afghanistan, it helped identify high-value targets. Domestically, it has been used to monitor U.S. citizens flagged as potential threats — combining drone footage, social media, and classified intelligence into a live, clickable map.

Foundry, its civilian counterpart, powers everything from disaster response and drug approval workflows to vaccine distribution and law enforcement surveillance. It played a key role in Operation Warp Speed (OWS) and continues to support the Centers for Disease Control and Prevention (CDC), Food and Drug Administration (FDA), and police departments via DHS partnerships.

Palantir also supplies the U.S. Army with battlefield intelligence through TITAN, a real-time sensor fusion system, and with logistics forecasting through VANTAGE.

This isn’t enterprise software. It’s the digital nervous system of the national security state — privatized, optimized, and deeply embedded. Palantir doesn’t just analyze information — it defines what matters. And once installed, it becomes indispensable.

A Constitutional Cure for “Fraud, Waste, and Abuse”

A common refrain among proponents of what DOGE has started and what Palantir is set to take to the next level is: *“How else can we find waste?”* Apparently they believe building a panopticon is the only reasonable solution to government inefficiency.

But that logic is backward — and dangerous.

DOGE was initially marketed as a small-government solution. In reality, the administration is now building the largest surveillance infrastructure in U.S. history. It replaces red tape with software, bureaucracy with automation, and decentralization with a centralized brain. That brain is Palantir.

If the goal is truly to stop fraud and abuse, the answer isn’t machine-led centralization. It’s constitutional decentralization.

Instead of wiring together every federal dataset, start *really* dismantling the unconstitutional sprawl, not automating it. Push responsibility back to the states, where programs are closer to the people and misuse is easier to detect. Let local governments handle entitlement verification, program audits, and budgeting. Empower independent inspectors general. Demand transparency from contractors. Enforce real congressional oversight — not automated compliance powered by black-box algorithms.

The Grid That Governs

Another favorite line is: *“But the government already has the data!”*

Yes, it does. But not like this.

Federal data is fragmented, purpose-bound, and legally siloed. Tax returns don’t live next to medical records. Immigration logs can’t be casually cross-queried with Social Security files. These barriers exist for good reason — to prevent abuse, mission creep, and political weaponization.

What DOGE and Palantir are doing is not storing data. They’re fusing it. Turning it into real-time profiles, simulations, and decision loops. This isn’t about merely “having” data. It’s about operationalizing it.

Finally, if fraud were truly the concern, why hasn't DOGE looked into the biggest missing pile of all? The Pentagon has reportedly lost track of over $21 trillion. So far, DOGE's grand data crusade has turned up just $80 million in flagged spending — mostly in diversity, equity, and inclusion and climate-related programs.

What DOGE has started, and what Palantir is now finalizing, is not a war on fraud. It's the construction of a system that fuses surveillance, automation, and enforcement into a single architecture of control.

And once this grid is put in place, it won't just monitor the governed — it will govern. Decisions will be made not by elected officials, but by algorithms. Rights won't be revoked with force, but denied by code. The Constitution won't be torn up — it will be silently bypassed.

And when the lights flicker, there will be no lever to pull.

Veronika Kyrylenko

Veronika is a writer with a passion for holding the powerful accountable, no matter their political affiliation. With a Ph.D. in Political Science from Odessa National University (Ukraine), she brings a sharp analytical eye to domestic and foreign policy, international relations, the economy, and healthcare.

Veronika's work is driven by a belief that freedom is worth defending, and she is dedicated to keeping the public informed in an era where power often operates without scrutiny.

ANOTHER ARTICLE ON PALANTIR: GUTTING THE FOURTH AMENDMENT

https://thenewamerican.com/us/politics/constitution/palantirs-database-would-gut-the-fourth-amendment/

Palantir's Database Would Gut the Fourth Amendment

by Joe Wolverton, II, J.D. June 2, 2025

Once again, the American people find themselves betrayed by those they entrusted with the preservation of their liberty. The recent exposé in *The New York Times* reveals that President Donald Trump — supposed champion of the Constitution — has instead gleefully erected the very apparatus of tyranny our Founders warned against: a surveillance leviathan that threatens to render the Fourth Amendment an empty parchment.

According to the *Times*, the Trump administration has not only deepened its relationship with Palantir — a Silicon Valley behemoth built on the promise of

rummaging through private data — but has laid the technological groundwork for merging data across federal agencies. Under the cloak of "government efficiency," Trump signed an executive order in March directing that data silos be obliterated. The result? A monstrous machinery capable of compiling bank accounts, medical records, student debt, and disability status into a single dossier on every American.

Let us make no mistake about what this means: It is the construction of a general warrant in digital form. Our Founding Fathers fought a revolution to free us from the oppressive tyranny of general warrants — those vile instruments that allowed British agents to rummage through Colonists' homes and papers without cause or oversight. The Fourth Amendment was ratified precisely to slam the door on such abuses. It declares, in no uncertain terms, that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated," and that "no Warrants shall issue, but upon probable cause." What, then, are we to call this modern effort to aggregate the private lives of Americans in the hands of bureaucrats? I call it an electronic general warrant — a warrant that seeks everything about everyone, everywhere, all at once.

Harmless "Efficiency"?

And let us not delude ourselves with the notion that this is merely a harmless effort at "efficiency." Efficiency, in the hands of an unrestrained government, is simply the iron heel on the neck of the people. Trump's order to eliminate "information silos" and "streamline data collection" is Orwellian "newspeak" for a gross violation of the Fourth Amendment and an assault on the very principle of limited government. It is an invitation to tyranny: a temptation for political witch hunts, for the punishment of dissenters, and for the advancement of an agenda that places government prerogative over the natural rights of the governed.

This is not a Republican problem or a Democratic problem; it is a constitutional crisis. Yet we are told by the apologists of the surveillance state that Palantir is merely a "data processor," not a "data controller." How convenient. This thin semantic defense crumbles under the weight of reality. A processor that can "find hidden things" in the data of every American is not a neutral party — it is the handmaiden of Leviathan. And when the executive branch — any executive branch — has the power to compile a "master list" of personal information on its citizens, history teaches us that abuse is not a possibility, but an inevitability.

Danger of General Warrants

Let us recall the wisdom of James Otis, that great champion of liberty who denounced general warrants in 1761: “It is a power that places the liberty of every man in the hands of every petty officer.” Substitute “Palantir engineer” or “DOGE bureaucrat” for “petty officer” and Otis’ warning rings truer than ever. The Trump administration’s efforts to merge data from the IRS, Social Security Administration, Department of Homeland Security (DHS), and even the Department of Education into a single, searchable database is a direct affront to the principle that a man’s papers — be they in his desk or on his server — are his own, immune from rummaging by government snoops without probable cause.

Consider the implications: with a few keystrokes, the federal government could create a comprehensive profile of any American — complete with financial records, medical histories, social connections, and ideological affiliations. And let us not pretend this is idle speculation; the *Times* itself reports that Palantir’s software is being deployed at DHS, IRS, and even Immigration and Customs Enforcement to monitor not only migrants but, by extension, every American whose data is held by the federal leviathan. The temptation to wield this power for political vendettas is simply too great. The Fourth Amendment was written to prevent precisely this: “The right of the people to be secure” means nothing if bureaucrats and political operatives can rifle through the digital lives of citizens under the guise of “efficiency” or “national security.”

Who Is Guarding the Fourth Amendment?

Where are the voices of constitutional fidelity? Where are the congressional guardians of our Fourth Amendment rights? Silence — deafening silence. Meanwhile, Palantir’s stock price soars, as though the Bill of Rights were just another line item on a quarterly report. And yet some former Palantir employees, to their credit, have spoken out. For instance, Linda Xia’s warning that “data that is collected for one reason should not be repurposed for other uses” is a reminder that even within the belly of the beast, conscience has not been wholly extinguished. But conscience alone cannot preserve our liberties; only an informed and vigilant citizenry, jealously guarding their constitutional rights, can turn back this tide of surveillance.

We should remember that the Fourth Amendment was not written to protect criminals from the law, but to protect the people from their government. And now, the government — under the leadership of a man who claims to want to “drain the swamp” — is transforming that government into a swamp monster armed with every piece of data on every American.

This Is Our Fight

If we are to remain a free people, we must denounce this unconstitutional colossus. Congress must refuse to fund this Fourth Amendment demolition derby. State governments must pass laws that prohibit their cooperation with these federal data-fusion centers. And the courts — those so-called guardians of liberty — must remember that the Constitution was not written in pencil to be erased at the whim of executive orders.

The Fourth Amendment is not negotiable. It is not subject to the whims of Palantir's quarterly earnings or Trump's fantasies of an all-knowing bureaucracy. It is the shield of the people, and it is time we took it up once again, before it is reduced to a relic — another artifact of a republic that lost its way.

If the Founding Fathers saw what is being done in their name, they would not recognize the America for which they pledged their lives, fortunes, and sacred honor. Let us honor their sacrifice by rejecting this high-tech tyranny, by repudiating the surveillance state in all its guises, and by reminding our leaders that no executive order — no matter how gilded with the language of efficiency — can repeal the natural right of the people to be secure in their papers and effects.

This is our fight, and it is one we cannot afford to lose.

Joe A. Wolverton, II, J.D.

Joe Wolverton, II, J.D. is The John Birch Society's constitutional law scholar and is the author of three books: The Real James Madison, "What Degree of Madness?": Madison's Method to Make America STATES Again, and The Founders' Recipe, an introduction to the writings of the 37 authors most often quoted by the Founding Generation. He hosts the YouTube channel "Teacher of Liberty" and the TikTok channel "Joe Wolverton JD."

August 4, 2025

Selling Us Rope: Palantir Is Raking In Billions From Washington

The claims that "the company was never ideological", as it spans across Administrations, is a sure sign that it is marching to the drumbeat of Technocracy. Technocracy has a death wish for capitalism and the constitutional republic, and it is encircling the federal government with a web of surveillance. In the meantime, our politicians remain clueless.

Both co-founders of Palantir, Alex Karp and Peter Thiel, are on the steering committee of the Bilderberg group. - Patrick Wood, Editor.

Elon Musk has left government, but another Silicon Valley player is making its mark in President Donald Trump's Washington: Palantir.

The software and data analytics company has garnered at least $300 million in new and expanded business since Trump took office for his second term, helping to make it the S&P's top performing stock of 2025. That includes contracts at the Federal Aviation Administration and the Centers for Disease Control and Prevention, as well as Fannie Mae, according to federal records.

Beyond that, the company is potentially set to earn an order of magnitude more in federal funds. In May, Pentagon leaders allocated up to $795 million more to the military's core artificial intelligence software program, the Palantir-built Maven Smart System, to expand its deployment to all U.S. forces around the world. And late Thursday the Army issued Palantir the company's biggest contract — an agreement to consolidate the military's software procurement over the next decade — at a cost of up to $10 billion.

At the State Department, a Palantir-designed AI system is now helping to write some diplomatic cables in a new pilot program, according to an internal State Department email obtained by The Washington Post. At the Department of Homeland Security, immigration officials reversed earlier plans to ditch some of the company's services when their superiors awarded Palantir a $3o million contract this spring to track immigration enforcement. And at the Internal Revenue Service, an official with Musk's U.S. DOGE Service tapped Palantir to expand an internal project to modernize the agency's data. The contracts were confirmed by five people familiar with processes at the federal agencies, who spoke on the condition of anonymity to avoid retaliation.

Government work was always core to Palantir's identity. Investor Peter Thiel, along with CEO Alex Karp, co-founded the company with an explicitly patriotic mission in the wake of 9/11. Though Karp is a progressive who has largely supported Democrats, Palantir's striking success over the last six months is a case study in how a changing ethos in Washington — toward cutting costs, embracing AI and empowering the private sector — is benefiting a particular company.

Even as Musk has decamped for his own business enterprises in Texas, a technology-friendly attitude and a newfound openness toward AI experimentation still permeate the administration. This approach, along with Palantir's long history of working with the government and its web of informal connections to the administration and to DOGE, places the software company in a sweet spot, according to people familiar with its Washington expansion.

“They were positioned in the right way at the right time, and they had already built the technology that had the capability to do what the administration is trying to do,” said Matt Pearl, director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) and former director of emerging technologies at the National Security Council.

Unlike other Silicon Valley companies in Trump’s orbit, **Palantir** never eschewed government business. **The firm has been awarded nearly $3 billion in federal funds since 2008, amounting to over 300 contracts spanning Republican and Democratic administrations.** Its software aided the 2011 raid that killed Osama bin Laden and helped organize logistics during the 2021 evacuation of U.S. troops from Afghanistan. CEO Karp recently published a book calling for technology companies to work closely with the state.

That history afforded the software firm a foothold ripe for expansion when Trump and Musk came to Washington under the banner of radical cost-cutting. Long before Musk declared his engineering-first crusade against waste, fraud and abuse in government, Palantir marketed its software for exactly that **purpose**, one it trumpeted on posters in its corporate offices.

The company also has boosted its connections to the Trump administration. This year it hired Ballard Partners and Miller Strategies, two Trump-connected lobbying firms. **Co-founder Thiel is a longtime mentor to Vice President JD Vance.** One of DOGE’s early strategists was another co-founder, Joe Lonsdale, a friend of Musk who has long championed the private sector as an efficient antidote to government excess and who recruited DOGE staff from Palantir’s alumni network. One of the company’s senior counselors is a former Trump official with close ties to White House Deputy Chief of Staff Stephen Miller and who leads a think tank project that seeks to dismantle the administrative state and replace its functions with automation technology.

“Palantir is an exceptional American company,” a senior State Department official said, adding that the department was “proud to partner with them to modernize how we carry out America’s diplomacy.” White House spokeswoman Taylor Rogers said agencies partnering with Palantir reflected the Trump administration’s “high standard when spending Americans’ hard-earned tax dollars.”

Palantir’s growth spurt in government work

Since 2008, Palantir has been paid just under $3 billion through federal contracts — most of that in recent years. Last year the company received more than $615 million.

At least six people who worked with DOGE are former Palantirians: Two — Gregory Barbaccia and Clark Minor — are now chief information officers at the White House and the Department of Health and Human Services, respectively. Palantir Chief Technology Officer Shyam Sankar was named a lieutenant colonel in the U.S. Army Reserve alongside three other tech leaders whose firms have more recently embraced the defense sector. The appointment was granted the day of Trump's June military parade, of which Palantir was a corporate sponsor.

"We are proud to support the U.S. government, especially our warfighters, and our growth reflects growing government AI adoption," company spokeswoman Lisa Gordon said. She noted that Palantir's government business has been steadily growing for six consecutive quarters, not just since Trump retook the White House, and that it "still lags significantly behind our U.S. commercial business."

Yet some federal employees, in interviews with The Post, have suggested the company is getting preferential treatment from Trump officials. Palantir's recent surge in government business has prompted unease among some employees and triggered scattered protests at company offices. Palantir's new ICE contract for tracking immigration violations and deportations has sparked impassioned discussions among company alumni, a dozen of whom wrote an open letter deeming that work a violation of the company's long-standing civil liberties principles. And at least one employee has quit over the company's growing role in implementing the Trump administration's policies.

Palantir rejects the accusation that it is getting any preferential treatment, saying its success is a result of its track record and expertise. The company also says its government activities are in line with its foundational principles, including protecting privacy and civil liberties.

Some Palantir employees have said they feel torn, because the company's growing success is wrapped up in what they see as controversial policies and harsh treatment of government workers whom they have worked alongside. "Economically [the new environment] is good" for the company's business, said a person who works closely with Palantir on government projects, who spoke on the condition of anonymity to avoid retaliation. "But some folks internally are grappling with the question of 'at what cost.'"

An AI transformation at the Pentagon

Nowhere has Palantir's reach into the government been more extensive than at the Pentagon, which is doubling down on AI and its engagement with commercial companies. In addition to raising the contract ceiling for Maven Smart System this spring, the Pentagon also issued a memo ordering greater reliance on commercial companies — a move likely to help Palantir, along with a newer crop of Silicon Valley upstarts.

Palantir's work building data management systems for the military began in 2011 under President Barack Obama, when its software was deployed in Afghanistan's Helmand Province to help the Marines in heavy fighting with the Taliban.

By 2017, the Pentagon had created it first AI effort, Project Maven, and its leaders became interested in advances emerging from Silicon Valley. They were particularly drawn to ImageNet, an open-source repository of labeled imagery, including plants, cats and other everyday objects that early AI software algorithms had identified on their own. Military officials traveled to California and met with executives at Google, self-driving companies and other start-ups to discuss military applications of these technologies. "Instead of, it's a plant … can we say, it's a weapon or a tank or a male or a woman or a child?" said retired Col. Drew Cukor, a Marine Corps intelligence officer, recalling the period. "Can we detect attacks?"

Maven's leaders recruited hundreds of workers to pore through the military's vast troves of collected imagery and painstakingly label tanks, airplanes, infantry and weapons. Then they solicited proposals from several tech companies to build algorithms that would enable computers to visually identify and geolocate those assets.

Google originally won the contract, but internal protests against working with the military — typifying Silicon Valley's attitude toward the defense sector at the time — prompted the software giant to pull out in 2018. Palantir was the next option, Cukor said.

When Palantir started building the software, its accuracy was still very low, Cukor said. "There were times when I was identifying cows as humans. I was identifying clouds as tanks," he said. "These were hard days."

An early version of the Palantir-built Maven tech was used operationally for the first time in 2017 in East Africa by Special Forces pursuing the Islamist group al-Shabab. Then the project was expanded to the XVIII Airborne Corps at Fort Bragg in North Carolina. For years, the head of that unit, Col. Joseph O'Callaghan, kept a framed photograph in his office of a rocket blasting a tank in a demo exercise in 2020, the division's first AI-enabled strike. The AI worked then, as it does now, by suggesting a target to human minders, who confirm the selection and then send a rocket launcher to fire on the mark, he said.

By 2021, Maven's accuracy had improved, but its deployment was still limited. That changed when Russia invaded Ukraine in early 2022. Though the military doesn't publicly acknowledge specific uses of Maven in the battlefield, officials and news reports have referred to the use of the AI program in the Ukraine conflict, as well as recent fighting in Yemen and Iran.

By early this year, the Army was already embarking on a massive expansion of the military program that Palantir's software is part of. Over 20,000 personnel are already using it, and the expanded contract is meant to facilitate its rollout to U.S. military units everywhere and to enhance the "reasoning skills" of the AI. "We've entered into an 'unchained phase' by implementing a whole-of-agency approach to AI transformation," Vice Adm. Frank Whitworth, director of the National Geospatial-Intelligence Agency, said in a speech in May. "And we see that action paying off across the board."

Conversations about raising the contract ceiling for the Palantir software began late last year, as the Biden administration was winding down, said a Defense Department official familiar with the discussions within the Pentagon's Chief Digital and Artificial Intelligence Office (CDAO), who spoke on the condition of anonymity to discuss internal matters. Use of Maven was revving up significantly and the department was running out of Palantir software licenses, the person said, but no action was taken until Trump took office, and he has installed his own leaders at the Pentagon. Biden appointees within CDAO had held back AI development because of safety and reliability concerns, said another person familiar with the debates around AI adoption, who also spoke on the condition of anonymity in order to relay internal matters.

The new administration, by contrast, is turbocharging the use of AI across the military at a moment when the U.S. faces a growing number of global threats.
"The stark contrast [between the administrations] doesn't indicate any wildness or disregard for safety," one of the people said. "What it does show is their willingness to experiment and move faster."

Read full story here...