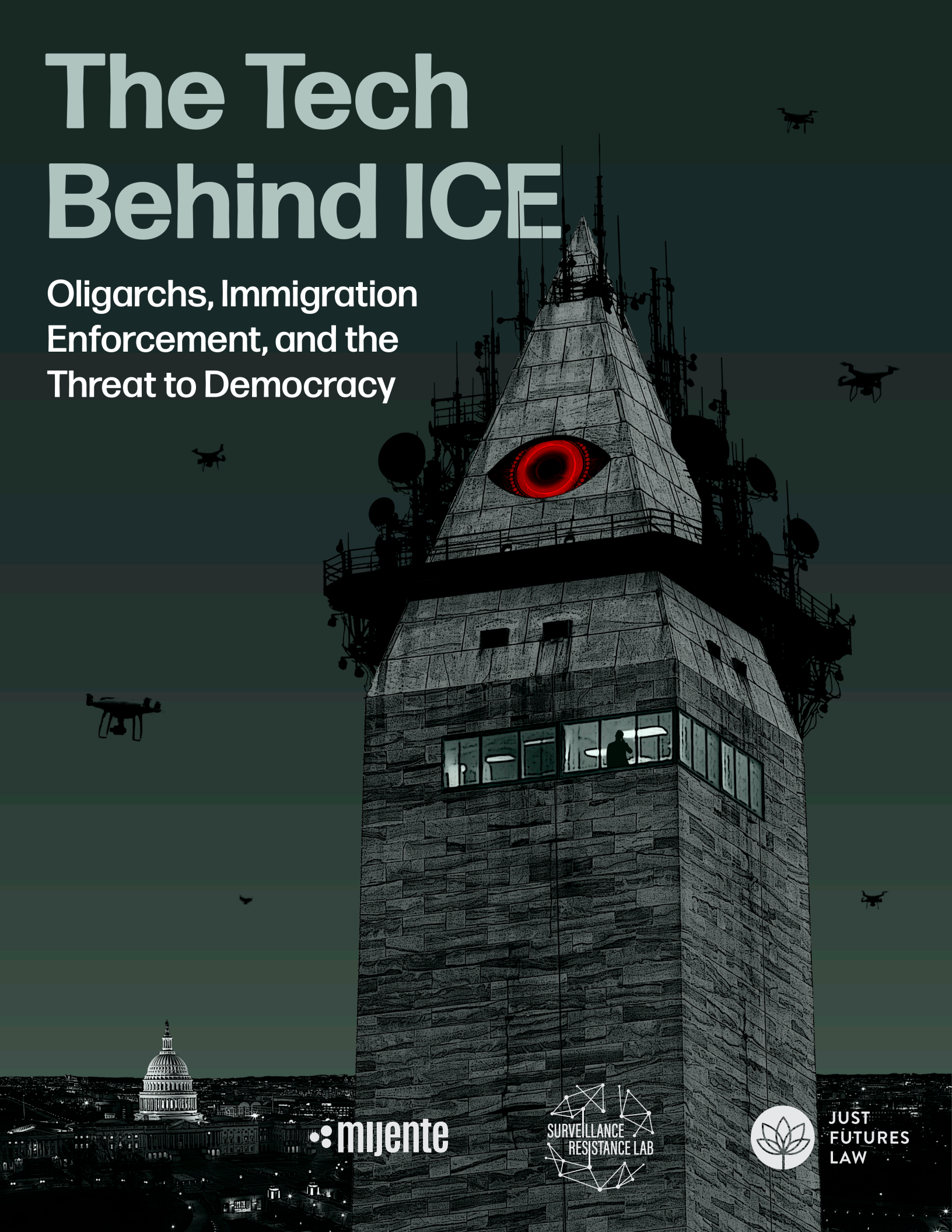
The Tech Behind ICE

Oligarchs, Immigration Enforcement, and the Threat to Democracy



mijente

SURVEILLANCE RESISTANCE LAB

JUST FUTURES LAW

Acknowledgments

This report was commissioned by Mijente, Just Futures Law, Surveillance Resistance Lab (a project of the Collaborative Research Center for Resilience). The writing of this report was led by Mizue Aizeki, Jacinta González, Paromita Shah, and Tania Unzueta.

The factsheet was authored by Hannah Lucal.

The illustrations and graphic design were done by Rodrigo Chazaro. The charts were designed by Valeria Mogilevich. Additional graphics were provided by Mayra Hernandez.

Research for the report was conducted by Empower (empowerllc.net), a research organization dedicated to narrowing the strategic information gap between corporations and civil society stakeholders.

Leah Montagne provided developmental editing, Dawn Marie Paley supported with writing and preliminary copyediting, and Tenaya Nasser-Frederick supported with final copyediting.

Special thanks to Hanna Homestead, Hannah Lucal, Nicholas Kempf, Deepa Padmanabha, and others who generously helped to get this report over the finish line.

Preferred citation: Mijente, Just Futures Law, and Surveillance Resistance Lab, "The Tech Behind ICE: Oligarchs, Immigration Enforcement, and the Threat to Democracy," June 2026

Note: The research for this report started in November 2025, and some of the data and information may not be precise up to the date of publication. We have tried our best to keep up with the rapidly evolving and constantly shifting landscape, but recognize there may be some gaps.

Table of Contents

Executive Summary 5

Introduction 8
- Homeland Security 9
- Key Terms 10
- Our Research 11
- Report Structure 11

1. The Architecture of Authoritarianism 12
- Cruel by Design 12
- New "War on Terror" 13
- Testing Legal Limits 14
- Technology of Control 15

2. Follow the Money: Revolving Door to Corner Office 17
- The Tech Gilded Age 17
- Innovation for "Democracy" 18
- The Future of War 19
- Profit-Driven Policy 21

3. Building the Militarized Police State 27
- More Money 29
- More ICE Police 29
- More Weapons 30
- More Data 30

4. Taxpayer-Funded Surveillance and AI 31
- The DHS Sandbox 33
- Artificial Intelligence in DHS 35

5. Tools of the Surveillance State 37
- 1. Data Brokers 39
- 2. Data Analytics and Databases 41
- 3. Web Scraping and Social Media Surveillance 42
- 4. Facial Recognition and Street-Level Biometric Surveillance 45
- 5. Nationwide Driver Surveillance 48
- 6. Hacking Devices and Spyware 50
- 7. Cellphone Tracking and Location Data 52
- 8. Skip Tracing and Contract Bounty Hunters 53
- 9. Detention and Deportation Tracking Apps 54
- 10. Border Towers and Drones 55

6. Organized Resistance 58
Local Governments 58
Challenge Corporate Power 61
Be Ready for Federal Openings 63
Understand the Systems to Fight Them 64
This Report is a Movement Offering 65

List of Acronyms 66

Appendix: Fact Sheet 67

Endnotes 72

List of Figures

Figure 1 Government awards to surveillance, defense, and AI companies founded by tech oligarchs 20
Figure 2 The money flow to the tech oligarchy's startups 21
Figure 3 Comparison of Trump's budget request for war versus public investment 22
Figure 4 Federal lobbying expenditures by tech oligarchy venture capital firms and portfolio companies (2000–2025) 23
Figure 5 Top 25 spenders on federal lobbying among defense, surveillance, and AI portfolio companies of tech oligarchy firms (2000–2025) 24
Figure 6 Projected ICE and CBP spending under OBBBA (2002-2026) 28
Figure 7 ICE and CBP Budget as of June 2026 29
Figure 8 Awards to surveillance, military, and AI companies funded by the tech oligarchy 31
Figure 9 Contract money awarded to Palantir by ICE 32
Figure 10 Contract money awarded to surveillance tech by ICE and CBP 33
Figure 11 Annual ICE contract money to key data brokers (2018-2025) 40
Figure 12 Contract money ICE awarded to Clearview AI 47
Figure 13 Contract money awarded to Cellebrite by ICE and CBP 50

List of Tables

Table 1 Political Contributions 22

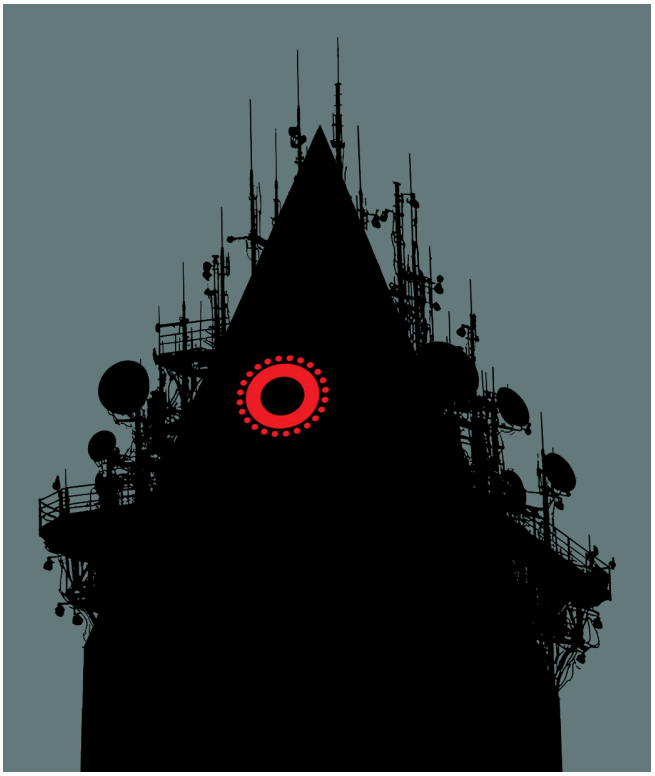
Executive Summary

At this moment, a dangerous convergence of two trends threatens democracy. The first is the Trump administration's aggressive acceleration of the use of technology and artificial intelligence to rapidly expand immigration enforcement and military force. The second involves an unprecedented amassing of economic and political influence by a small group of tech oligarchs.

The Department of Homeland Security (DHS) has provided a clear pathway towards the current administration's active construction of a new security state. This security state is defined by enormous military power and DHS interior policing power, while state projects dedicated to social good are dismantled. Simultaneously, a handful of tech oligarchs, including venture capitalists and executives who hold or orchestrate massive federal contracts, have embraced militarism and are developing technology tools towards the application of DHS's mission, which generally aligns with their own corporate and political ambitions. These tech oligarchs are increasingly positioned not only to direct government decisions on technology, but to make those decisions from within government itself, influencing agendas on policing, bordering, and militarism, as well as the planet and democracy.

As in our 2018 report, "Who's Behind ICE? The Tech and Data Companies Fueling Deportations,"[1] we are focused on the US immigration policing apparatus, which consists primarily of US Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP). CBP polices the circulation of people and goods across US borders and has the authority to arrest non-citizens within 100 miles of US boundaries. ICE has the authority to investigate and arrest non-citizens throughout the US interior and orchestrates the immigration detention and removal (deportation) systems. Throughout this report we refer to ICE and CBP, but also to DHS, which houses both agencies. This is because the immigration policing components of DHS have dominated this department's mission, communications, and budget.

This analysis is grounded in an understanding that immigration enforcement and "national security" have long served as the justification for increasingly authoritarian systems that erode civil liberties, weaken democratic protections, normalize mass surveillance, and deepen environmental and social harm in communities across the country. What's different in this moment is the way in which the authoritarianism of these systems has been deepened and unleashed. This report examines how DHS has laid the foundation for this authoritarian moment. We reveal how this moment creates an accelerated danger, as a power-hungry tech oligarchy becomes increasingly influential, and identify the major actors, corporations, monies, and mechanisms involved. This report also describes some of the most important strategies available to non-violently resist the entanglement of big tech, immigration enforcement, and militarism. Confronting this threat requires a clear understanding of the convergence of agendas and where their power can be disrupted.



1. The Architecture of Authoritarianism

The Trump administration's aggressive agenda builds on decades of expanding DHS power, militarized policing, and bipartisan "national security" governance embraced by previous administrations. Immigration policing, when carried out under a domestic terrorism framework, functions as both the justification and testing ground for a police-state infrastructure powered by massive federal investments in surveillance systems, AI technologies, biometric tools, drones, detention infrastructure, and militarized enforcement operations. The Department of Justice (DOJ)—the agency charged with enforcing US laws for everyone in the country—has become DHS's law firm: fixated on expanding DHS's policing powers, dismantling core due-process protections, and defying the courts' attempts to rein in DHS.

2. Follow the Money: From Revolving Door to Corner Office

The insidious influence of big tech and other monied interests in government is not new—but a fundamentally new chapter has begun. A key sector of tech funded by venture capital has positioned itself as visioning and directing the war machine and asserts that AI is vital to US national security and the economy. The influence of venture capitalists can be seen in how they are increasingly embedded in government, how they have transformed military procurement, and how they ensure their tech and their corporations become mission critical to the functioning of US homeland security governance.

Trump-aligned tech oligarchs like Peter Thiel, Marc Andreessen, Elon Musk, and others have used their immense wealth and political influence to shape the federal government through campaign contributions, lobbying, corporate partnerships, and direct relationships inside the administration. At the same time, the federal government has poured massive public investment into AI infrastructure, surveillance systems, defense technologies, and data centers with little transparency or public accountability.

3. Building the Militarized Police State

Since its inception, DHS has grown its policing power to realize its extremely broad and ambitious mandate. This includes rapidly expanding its policing personnel (ICE and CBP) and increasing cooperation and information sharing between DHS and civilian agencies, most notably local, state, federal police, and international police counterparts.[2] Trump's One Big Beautiful Bill Act boosted ICE funding from around $10 billion per year to over $85 billion, while the CBP also received a funding boost of over $60 billion. In addition to growing the power of its policing force by expanding boots on the ground—notably by enlisting thousands of local police—it has also significantly grown its arsenal of weapons and tech tools. The ability of DHS to surveil and arrest immigrants through tax, Medicaid, and other data has grown with the involvement of data brokers and the Department of Government Efficiency (DOGE).

4. Taxpayer-Funded Surveillance and AI

Billions in public money are going to DHS surveillance, including for artificial intelligence enabled tech, without any outside mechanisms for compliance and oversight. These dollars generate massive revenues for tech oligarchs and their companies, expanding the immigration enforcement complex economy. Between 2020 and 2025, the federal budget for DHS has increased from around $1.5 billion in 2020 to $6 billion in 2025 (see **Figure 1**). This funding sustains an ecosystem of small startups that are creating even more invasive surveillance technologies and attracting the interest of corporations that primarily focus on the military. The 2027 military budget reconciliation request from the Trump administration earmarks $53.6 billion for new unmanned tech and $46 billion for AI infrastructure. This money infusion has rapidly expanded the DHS AI inventory; it also has shaped DHS's policy on AI use as the astronomically increased budget has brought in Silicon Valley tech startups who see the lack of oversight and unmonitored government contracts as a research and development cash cow for their AI startups.

5. Tools of the Surveillance State

ICE and CBP are not only immigration policing agencies, they are also central pillars of the new security state with a rapidly expanding surveillance apparatus powered by AI-driven technologies, private contractors, and massive data-sharing systems. Through biometric databases, facial recognition, mobile phone extraction, license plate readers, drones, social media monitoring, and data broker networks, DHS agencies are building a surveillance infrastructure designed to identify, track, profile, and target people at an unprecedented scale.

Although these systems are often justified through immigration enforcement and racialized narratives around "security," their architecture extends far beyond immigrants. The same technologies capable of targeting undocumented communities can monitor the population at large, expanding government power to surveil political activity, dissent, protest movements, and everyday life. Immigration enforcement has become the entry point for a much broader surveillance dragnet that increasingly treats entire communities as data points to be monitored, analyzed, and controlled for profit and political power.

AI acts as an accelerator for some of the most extreme and authoritarian DHS practices, enabling more aggressive apprehensions, prosecutions, deportations, and retaliatory surveillance operations that can result in injury or death. Street-level surveillance and data collection feed massive machine-learning systems capable of generating instantaneous dossiers used for arrests, deportation, targeting, and political repression, including against journalists, legal observers, protesters, and people documenting ICE operations. These systems continue to expand with little to no oversight of their effectiveness, civil rights impacts, accuracy, or long-term consequences.

6. Organized Resistance

Resisting immigration enforcement requires confronting the technological, political, and corporate infrastructure powering mass surveillance, policing, detention, and deportation. Local governments can weaken these systems by ending data sharing with ICE, limiting the expansion of surveillance technologies, strengthening privacy protections, increasing transparency, and creating stronger public oversight over policing and technology contracts.

Communities, organizers, workers, and advocates must also challenge the corporations profiting from surveillance and enforcement through protest, litigation, policy advocacy, investor pressure, public education, and worker organizing inside tech companies themselves. At the federal level, movements must prepare for future political openings by building long-term strategies around investigations, procurement reform, oversight, restrictions on biometric surveillance and AI systems, and limits on government data sharing. Building resistance also requires communities and movements to better understand how surveillance technologies operate locally so they can identify pressure points, expose harms, and organize more effectively against the continued expansion of the surveillance state.

Introduction

In the pre-dawn hours of October 30, 2025, ICE officers and CBP agents in unmarked cars surveilled what they described as a "target-rich" apartment complex in Woodburn, Oregon.[3] Agents monitored vehicles leaving the complex and ran license plates through a license plate reader system, matching a white van to a person they were seeking. After following the van, officers surrounded it and smashed the driver's side window, after ordering people out but without verifying whether the driver was the person they had identified.[4]

That day, over 35 people were detained, many of whom were farmworkers headed to work.[5] The operation—the largest in Oregon up to that day—later drew legal scrutiny, with a judge questioning both the legality of the arrests and the surveillance-driven tactics used to identify and target workers.[6]

Roving masked patrols, biometric scanning, arrests without warrants, enforced disappearances, and violent escalations set the tone for the Trump administration's cruel and violent tactics during immigration enforcement surges in Chicago, Los Angeles, Minneapolis, and Portland. Masked Department of Homeland Security (DHS) agents aggressively assaulted and terrorized communities, undermining constitutional rights and threatening public safety. Citizens and noncitizens engaged in the constitutionally protected activity of filming and recording law enforcement actions have been prosecuted, arrested, and attacked, sometimes with deadly force. These events foreshadowed a broader pattern that would come to characterize the administration's governing approach: the assertion of expansive executive power, the sidelining of oversight, and the treatment of legal constraints as obstacles to be overcome.

But the story of this moment is not only about the expansion of state power. It is also about who is helping build it, profit from it, and shape it from within. At the same time as we are facing an urgent crisis for human rights, democracy, and the environment, an increasingly concentrated handful of tech oligarchs are working in concert with the federal government to grow US militarism and advance the security state. These same tech oligarchs are increasingly well positioned not only to direct government decisions on technology, but to make those decisions from within government itself—no longer content with a revolving door, they're now working from inside a corner office.

This report builds on our 2018 report, "Who's Behind ICE: The Tech and Data Companies Fueling Deportations," which documents the many ways that advanced technologies and tech companies have already become embedded in the immigration policing and migrant control regime in the United States. We have remained steady analysts of the practices and narratives of DHS, and the orientation of each successive administration in growing its power, personnel, and technological reach. Over the past nine years, we have witnessed and advocated against how DHS has whittled away at rights while gaining more and more resources to expand its interior policing power and global reach.

In this report, we analyze how DHS functions as the foundation of a security state that is amassing and exercising increasing control over the US interior. We consider how venture capitalists and executives of large tech companies are being incorporated into this project through large federal contracts and the development of new technologies considered mission critical for DHS. Powerful ties between tech oligarchs and the security state are cemented through lobbying, campaign donations,

But the story of this moment is not only about the expansion of state power. It is also about who is helping build it, profit from it, and increasingly shape it from within.

no-bid contracts, and well-placed transplants in the US government and military. We also analyze the way that new technologies used by DHS, many of which are empowered by artificial intelligence, large language models, and predictive algorithms, are increasingly incorporated in immigration policing in the US interior. In our inventory of DHS's surveillance technologies, we also trace linkages between these technologies, tech oligarchs, the security state, and authoritarian control.

Immigrants remain the primary targets of the surveillance, detention, and deportation systems examined in this report. But the infrastructure built to target immigrants does not stop with immigrants. The same technologies used to identify, track, and deport non-citizens also collect and analyze information about family members, neighbors, coworkers, journalists, protesters, and entire communities. Biometric databases, social media monitoring, location tracking, license plate readers, and AI-powered analytics extend far beyond the border and far beyond immigration enforcement. What is built in the name of controlling migrants increasingly becomes a tool for monitoring society as a whole.

Homeland Security

Born in the aftermath of 9/11, the Department of Homeland Security (DHS) was founded as a key institutional home for the "War on Terror," tasked with overseeing "homeland security"—a vague and overly expansive mandate that has grown policing power domestically and globally.[7] DHS embodies a paradigm of "national security" governance that has allowed the federal government to maximally enforce draconian immigration laws passed in 1996,[8] and to erode or dismantle laws protecting key civil rights as well as basic tenets of democracy, including transparency, accountability, legal norms to protect human rights, and respect for pluralism. The perpetual state of emergency that guides DHS has provided the political cover to divert an unprecedented amount of federal resources into building the surveillance infrastructure and repressive migration control apparatus we are confronted with today.

The perpetual state of emergency that guides DHS has provided the political cover to divert an unprecedented amount of federal resources into building the surveillance infrastructure and repressive migration control apparatus we are confronted with today.

The extremely aggressive agenda being pursued by the Trump administration builds off logics and a policing apparatus that have been embraced and fortified by each administration that has overseen DHS. Over the last 25 years, subsequent administrations have shifted the target, however slightly, on how to define "security" and who is consequently deemed as a "threat."[9] But every administration has invested heavily in furthering the momentum of DHS, building on the idea that more control, punishment, and policing to protect against named threats—however spurious—is legitimate.

DHS has a tremendous amount of power and agency to pursue its mandate due to a criminal legal system that justifies its practices and the leeway that the courts, Congress, and the executive have granted it across presidential administrations. The Trump administration has pushed the boundaries of the law even further, expanding the zone of lawlessness in which DHS operates. Today, the deportation agenda is being weaponized to dismantle rights beyond immigration, including dismantling the social support systems, the states' protection of voter registration records,[10] the suppression of free speech[11] and peaceful protest,[12] and the widespread use of racial profiling[13] and extrajudicial punishment,[14] among others.

Key Terms

Below we define some key terms that we use throughout this report.

We use **"tech oligarchy"** to refer to a group of technology executives, investors, and corporations whose economic power increasingly translates into political power. These tech oligarchs are extremely wealthy and powerful. Many of the companies shaping artificial intelligence, cloud computing, data analytics, and digital infrastructure are no longer simply government contractors. Their executives and investors are increasingly helping shape government priorities, policies, and spending decisions.

Venture capital (VC) plays an important role in this story. Venture capital firms provide financing for startups and early-stage companies. Traditional VC firms like Founders Fund and Andreessen Horowitz, as well as corporate VC firms like Google Ventures and NVentures (Nvidia), are ultimately funded and controlled by Big Tech companies. VC firms invest in portfolio companies, sometimes referred to here as "VC-funded companies," including surveillance, defense, and AI companies that receive government contracts. These companies, some of which are already listed on public markets—or on the verge of being listed—include Palantir Technologies, Anduril Industries, SpaceX, OpenAI, and Anthropic, as well as many smaller, lesser-known startups in different stages of development.

Artificial intelligence (AI) is "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."[15] In the context of immigration policing and national security, AI can increase the speed and scale of surveillance, allowing agencies to process vast amounts of biometric, social media, geolocation, financial, and government data. DHS AI will help make automated decisions on immigration relief and benefits and on decisions relating to targets, arrests, detentions, and deportations. The concern is not AI alone, but how these technologies are being deployed within a rapidly expanding security apparatus that faces limited public oversight and accountability.



Our Research

This report is based on the collection and analysis of a wide variety of sources. Private-sector contracts with federal agencies were monitored on USAspending.gov, while active solicitations were researched on SAM.gov (System for Award Management). Public records requests, sometimes followed by Freedom of Information Act litigation, were submitted by collaborating organizations on various subjects, particularly with the Department of Homeland Security (DHS) and its component agencies, to obtain full copies of government contracts, communications, and related documentation. Government publications such as executive orders and press releases, as well as budget and legislative documents, were extensively consulted, as was the DHS AI Use Case Inventory.

Corporate research on tech-sector investment was conducted using both open-source and proprietary financial platforms, including:

- US Securities & Exchange Commission (SEC)
- State business registries
- Corporate presentations, press releases, and industry publications
- S&P Capital IQ (publicly traded companies)
- Preqin (private equity)
- Crunchbase (venture capital)

Revolving-door research draws on various public sources, including:

- Lobbying Disclosure Act federal database
- Federal Election Commission campaign finance data
- Personal financial disclosures (executive and legislative)

Investigative and industry reporting from a wide variety of journalists was invaluable to the research process for analysis and fact finding. The report also draws on the decades of experience that its authors have in legal and campaign organizing, as well as their colleagues, collaborators, and other human sources.

Report Structure

"The Tech Behind ICE" is made up of six sections. It starts by discussing the centrality of DHS to the growing security state and authoritarianism. The second section charts how powerful actors, who we call the tech oligarchy, and their companies, and technologies have become enmeshed in the federal government. In the third section, we outline how expanded funding and political momentum has enabled DHS to scale up its policing apparatus since the beginning of the second Trump inauguration, fueling its ability to enact mass deportation and associated harms. The fourth section highlights how the funding has been used to grow federal investment in surveillance and policing technologies and the role of DHS as a tech sandbox, and how DHS has been accelerating its use of AI. In the fifth section, we detail key technologies that ICE, CBP, and other DHS agencies rely on. These technologies enable DHS to surveil and exercise force against non-citizens and citizens alike, justified through the lens of homeland security and the threat of "domestic terrorism." The final section of this report examines where these systems are vulnerable and how organizers, advocates, workers, policymakers, and communities can act to challenge them.

1. The Architecture of Authoritarianism

Trump campaigned on a promise to enact a brutal mass deportation campaign.[16] In his second administration, he has dedicated significant financial and political resources to maximize the power of the legal and material apparatus that he inherited. Aided by a legal regime that facilitates mass deportation without meaningful due process, the Trump administration is also pushing the boundaries of the constitution and executive power.

The Department of Justice (DOJ), the agency responsible for enforcing federal law and protecting the rights of all people in the United States, has increasingly operated as an extension of DHS. Rather than serving as an independent check on government power, DOJ has focused on expanding DHS's enforcement authority, weakening due process protections, and defending DHS and White House officials from judicial scrutiny and oversight.

Cruel by Design

This moment is ripe with abusive and extreme government actions. Under the guidance of presidential advisor Stephen Miller,[17] the second Trump administration has aggressively pursued avenues to maximize its border control and deportation agenda. While they are certainly pushing the boundaries, and at times arguably violating laws,[18] their ability to enact their agenda is facilitated under the "rule of law," due to the existence of extremely punitive and restrictive US immigration laws. The US currently has a draconian governing immigration because of two major legal watersheds: first the extremely exclusionary and punitive immigration laws passed in 1996 and the deterioration of rights[19] following the founding of DHS in 2003. The 1996 laws increased border policing, enhanced penalties for unauthorized entry, and significantly grew the ability of the government to exclude, detain, and deport people at a mass scale through provisions such as mandatory detention and deportation. The creation of DHS turbocharged the government's power to enforce these laws, and its paradigm of "homeland security" governance activated broad corporate interest.

In 2025, Immigration and Customs Enforcement (ICE) acting director Todd Lyons stated, "We need to get better at treating this like a business." Lyons said he wanted to see a deportation process "like [Amazon] Prime, but with human beings."[20] With the second Trump administration, the power of DHS and its immigration enforcement agencies has only expanded. In the third section of this report, we address dramatic increases in ICE and CBP's budgets, personnel, and overall infrastructure to deport more people faster. The administration's efforts to accelerate deportations have taken multiple forms: pressuring people to self-deport[21] through attrition and fear;[22] closing avenues to remain legally; new arrangements to deport people to "third countries;" expanding expedited removals and eroding the immigration courts—to name just a few.

Even as DHS claims it is adhering to policy, it continues to hollow out internal safeguard sub-agencies, including the Office of Civil Rights and Civil Liberties (CRCL).[23] It recently laid out plans to decrease the size of the Office of the Inspector General (OIG), a watchdog agency that performs audits of DHS personnel and contracts, and operations policies.[24] It has also substantially undermined the immigration courts, complicating demands for "due process" in this politicized court system.[25]

In 2025, Immigration and Customs Enforcement acting director Todd Lyons stated, "We need to get better at treating this like a business." Lyons said he wanted to see a deportation process "like [Amazon] Prime, but with human beings."

New "War on Terror"

Trump was reelected on a campaign based on narratives of criminalization, exclusion, and state violence enacted with brute force. His second presidency exhibits a culmination of the "War on Terror" while also intensifying and pushing its boundaries. The founding of DHS in 2002 normalized the centrality of migration policing and deportation in US governance, as well as the determination of what is "national security" and who is and is not a "terrorist" in the executive branch.[26] The ongoing "War on Terror" revealed that broad categories of people—such as Muslims, non-citizens, people protesting state violence—can be subject to indefinite detention, cruel treatment, exile, or even death, with few or no legal protections so long as they can be labeled as "threats."

The power of DHS has been further expanded through the government's framing of unauthorized migration as a national security issue, which legitimates a military response. To achieve its maximalist program, the administration's approach includes conflating migrants with "potential terrorists, foreign spies, members of cartels, gangs, and violent transnational criminal organizations, and other hostile actors with malicious intent."[27] In 2025, the administration called for the deportation of hundreds of alleged gang members, stating they were conducting "irregular warfare" against the United States."[28] The president invoked the Alien Enemies Act, which was passed in 1798 and last used during WWII, allowing presidents to intern or expel foreign nationals from an enemy state without a hearing or due process. The Alien Enemies Act was used to deport primarily Venezuelan nationals to the Terrorist Confinement Center (CECOT) mega prison in El Salvador, without presenting any evidence.[29] According to a 2025 report by Human Rights Watch, people were tortured during the two months they were incarcerated in El Salvador.[30]

Beginning with the prosecution and removal proceedings against pro-Palestine activist Mahmoud Khalil[31] and the September 2025 Executive Order that declared "Antifa" a domestic terrorist organization,[32] the administration has issued several executive orders[33] and policies that collapse national security, counterterrorism, and political opinion into a single, dangerous framework that risks silencing dissent, eroding civil liberties, and hardening an authoritarian style government.

On September 25, 2025, the Trump Administration released its most comprehensive framework, National Presidential Security Memorandum–7 (NPSM-7), which offers a chilling view of the creation of the new "domestic terrorist." People, institutions, foundations, or entities that espouse views that are "anti-American," "anti-capitalist," or "anti-Christian" could face investigations or reprisals by the multi-jurisdictional Joint Terrorism Task Forces (JTTFs).[34] In the 2027 budget request to Congress, the administration requested funds for a new FBI crime center focused on a set of "indicators" of potential domestic terrorism. On top of this, a 2026 counter-terrorism strategy memo provides that DHS will play a key role in identifying and neutralizing "violent secular political groups whose ideology is anti-American, radically pro-transgender, and anarchist."[35]

As DHS scans social media for "anti-American" content[36] and DOJ initiates investigations of people critical of ICE on social media,[37] these memos herald the use of even more invasive AI-enabled surveillance that will enable repression and retaliation by the Trump Administration against anyone deemed a threat to its agenda.

Labeling speech, conduct, or groups as "anti-American" because they are "anti-capitalist," "pro-migration," or "pro-racial-justice" has laid the groundwork for categorizing people as "domestic terrorists," enabling surveillance, detention, deportation, and the destruction of lives and communities under the guise of security.

Testing Legal Limits

The Trump administration's extreme migration goals are not taking place in a vacuum. Rather, they are fueling brutal attacks on our core institutions and universal rights. Under the Trump administration, DHS has unleashed a campaign of violent practices and retaliatory tactics that have been well documented by journalists, human rights observers, and city officials. In short, DHS's implementation of their mass deportation project has injured or killed more people than they disclose[38] and this year, more people have died in immigration detention than in all previous years following 2004.[39] CBP and ICE shot at over a dozen people between September 2025 and February 2026.[40] By the end of April 2026, sixteen people had died in immigration custody alone, exceeding the total number of deaths in 2024.[41]

From the outset it was clear that the administration's most public immigration enforcement efforts targeted cities and states that had passed sanctuary city policies, often led by Democrats[42]—a clear retaliatory attack on the administration's political opponents and protections for immigrants.[43] These attacks most recently culminated in Operation Midway Blitz (Chicago), Operation Metro Surge (Minneapolis/St Paul), and others. When the constitutionality and violence of these efforts were challenged, instead of providing independent federal oversight, DOJ functioned as DHS's law firm, justifying increasingly extreme operations and tactics such as the killing of protesters and observers like Renee Goode and Alex Pretti.[44]

DOJ has invoked fringe legal arguments—from the lower courts to the Supreme Court—to aggressively unravel due process protections in laws and policies or upend bedrock legal interpretations, such as birthright citizenship, by invoking fringe legal arguments.[45] DOJ, which oversees immigration courts and their judges,[46] has sought to enforce "no bond" detention policies, in favor of keeping people locked up indefinitely, or has deported people to third countries after unilaterally revoking humanitarian protections. These actions taken together center DOJ as a key enabler of DHS's grab for limitless policing power.

Excerpt from memorandum implementing National Security Memorandum-7: Countering Domestic Terrorism and Organized Political Violence

Office of the Attorney General, December 4, 2025

"Particularly dangerous are those acts committed by violent extremist groups that threaten both citizens' safety and our country's ability to self-govern. These domestic terrorists use violence or the threat of violence to advance political and social agendas, including opposition to law and immigration enforcement; extreme views in favor of mass migration and open borders; adherence to radical gender ideology, anti-Americanism, anti-capitalism, or anti-Christianity; support for the overthrow of the United States Government; hostility towards traditional views on family, religion, and morality; and an elevation of violence to achieve policy outcomes, such as political assassinations. The recent attacks fueled by these agendas and ideological frameworks require a robust response. The JTTFs shall prioritize the investigation of such conduct."



Judges in federal and immigration courts have accused DHS and DOJ of misrepresenting facts and outright lying,[47] with the majority of these concerns occurring in immigration enforcement related matters.[48] Thousands of lawsuits have been filed against the Trump administration, primarily against new mandatory detention policies that have left thousands of people ineligible for bond.[49] As DHS deploys more invasive surveillance, the agency continues to test the limits of its executive authority against the Fourth Amendment's protection against unlawful searches and seizures and other due process rights by arresting and detaining people without limits and blocking access to their lawyers.[50]

As part of the broader agenda of the Trump administration, DHS, DOJ, and White House are pursuing a radical strategy to criminalize dissenting speech and conduct, which we describe above as the "New War on Terror." These new strategies follow the first Trump administration's practice to directly retaliate against many noncitizens who spoke out against ICE detention or family separation.[51] While the Trump White House pursues personal vendettas against political opponents,[52] the DOJ has initiated investigations of ICE critics and prosecutions of protestors, people who criticized the government, and people arrested during immigration operations,[53] and has accused people of attacking or interfering with officers.[54] DOJ is already prosecuting organizations and people to drain resources, intimidate supporters and allies, and chill dissent.[55] As a result, DHS has been the subject of lawsuits around the country for violating the First Amendment rights of legal observers and journalists, who have found themselves shot at, pepper sprayed, or assaulted.[56]

However, the administration is pursuing a far broader project: building the surveillance and prosecutorial infrastructure to target individuals and groups who hold views opposed by the Trump Administration. Reports of a DHS and DOJ "Antifa" watchlist that collects information on individuals and networks of legal observers, protesters, and dissenters raise profound First Amendment and privacy concerns.[57] Labeling speech, conduct, or groups as "anti-American" because they are "anti-capitalist," "pro-migration," or "pro-racial-justice" has laid the groundwork for categorizing people as "domestic terrorists," enabling surveillance, detention, deportation, and the destruction of lives and communities under the guise of security.[58]

Mahmoud Khalil's attorney called out the government's violation of his First Amendment rights, "Federal courts have already agreed that Mahmoud was targeted for his speech, and there is likely much more evidence of the government's unlawful retaliation that has yet to come to light."[59] A judge described the DOJ prosecution of Kilmar Abrego Garcia as retaliation, specifically "an abuse of prosecuting power," for filing a lawsuit that challenged his detention and removal.[60] This approach reflects a growing pattern in which DHS powers are used not only to police migration but also to discourage criticism of government policy.

Technology of Control

These violations are compounded by new invasive surveillance technologies—from spyware to data brokerage to drones. In Section 5, we document a wider variety of these technologies and how they are used for mass deportations and detentions, spying, and retaliation against those who criticize the government or exercise their constitutional rights against government abuse.

DHS technologies include tools that can hack devices, take face scans and license plate numbers from a distance, and instantaneously deliver personal and sensitive information about a person in seconds.[61] These technologies, many of which are AI-enabled, scan social media accounts to determine if a person can be denied a visa for their political views, analyze license plates to determine if a car participated in ICE watch, and send drones to monitor observers or targets.[62] Because these technologies are rapidly being integrated into operations targeting immigrants—surveillance, arrests, deportations, prosecutions, detention, and border policing—they are enabling the government to expand its capacity to monitor, target, and intimidate political opponents with no transparency or accountability. As DHS ramps up surveillance against ICE critics and legal observers, Tom Homan, DHS's border czar, said he wanted to create a database to make "famous" those "who impede

DHS technologies include tools that can hack devices, take face scans and license plate numbers from a distance, and instantaneously deliver personal and sensitive information about a person in seconds.

ICE."[63] In other words, the tools within the inventory can enable government repression at scale. This is particularly concerning given the activation of "domestic terrorism" as a justification for policing dissent.

Even though many of these technologies are deployed without oversight, metrics, or constraints, tech companies supplying DHS continue to claim that surveillance technologies are benign.[64] Some tech CEOs have positioned themselves as defenders of the Constitution or civil rights even as they received contracts during the peak of immigration enforcement surges in Chicago and Minneapolis. In a disturbing letter to Palantir's investors in February 2026, CEO Alex Karp claimed that Palantir products should be viewed as the best guardians of the Fourth Amendment's protections against unreasonable search and seizure.[65] This bold claim is, at the very least, premature, because current and previous DHS accountability mechanisms rely on DHS and their contractors to police themselves.[66] Critical civil rights questions remain about the impact on civil, privacy, and consumer rights and the likelihood of errors within these programs. There is no mechanism for the public to determine whether DHS unlawfully extracts sensitive information or biometrics, breaks privacy laws, produces systemic errors, or requires consent or a warrant.

In one important example, since last year, ICE and CBP agents have been using Mobile Fortify,[67] an AI-enabled facial-recognition app. Agents use their phones to capture images of peoples' faces, to carry out street-level surveillance and real-time "identity checks," including against legal observers engaged in constitutionally protected activities like the recording of police or immigration enforcement.[68] In Minnesota and Illinois, legal observers reported CBP or ICE agents photographing them and their vehicles with smartphones.[69] In Maine, a First Amendment lawsuit claims DHS used their "significant surveillance capabilities," including Mobile Fortify, to retaliate against and intimidate observers filming ICE arrests and enforcement.[70] During Chicago's Operation Midway Blitz, patrolling CBP agents snapped photos of people's faces to "verify" US citizenship, a practice raising serious legal issues.[71] Across the country, DHS told ICE to watch observers that they then placed in a domestic-terrorist or "Antifa" database; others were told the app functioned like an instant identity check, returning names and addresses immediately.[72] In Chicago, DHS did not ask for consent, used the app on minors,[73] and has not released any policy related to its use of Mobile Fortify, despite multiple Congressional requests. [74]

As DHS agencies deepen their use of predictive technologies, facial recognition, social media monitoring, and data-sharing systems, these tools are increasingly positioned not only against immigrants, but against journalists, organizers, protesters, and political opposition more broadly. The rapid normalization of these technologies signals the expansion of a far more pervasive state capacity to undermine constitutional rights and democratic freedoms on a much larger scale.

DHS's adoption of new technologies for surveillance of immigrant and non-immigrant populations is detailed in the fifth section of this report. More immediately, this report next turns to the power and influence that major actors in the tech sector have in shaping the security state and this authoritarian moment.

2. Follow the Money: Revolving Door to Corner Office

The "revolving door" of elected officials or personnel leaving a government position to work at a corporation, or vice versa, is a well-known pattern of corporate entanglement with governance. Currently we are experiencing a new chapter—corporate executives, including tech oligarchs, are notably embedded within the new administration in ways that arguably give them substantial influence on visioning and directing the security state and the war machine.

This has been accompanied by a marked increase in private capital investment in military technology—in 2024, venture capital invested $31 billion in military-related companies, 33% higher than the previous year.[75] Tech oligarchs, with their sights set on lucrative and stable Pentagon funding, not only benefit from the "revolving door," but now occupy a "corner office."

The Tech Gilded Age

In January, the US Federal Reserve released data[76] showing 1% of the population now control over a third of all wealth in the country.[77] This represents the widest wealth gap registered in the United States since the Federal Reserve began keeping track, and it is the product of bipartisan policy choices that promote a broken tax system and race-to-the-bottom austerity. Billionaire wealth rose over 16% in 2025, after Trump's second inauguration, to its highest level in history, driven in large part by a US stock market in which the "Magnificent 7" tech stocks account for more than a third of total market capitalization.[78] Tech wealth, in particular, has exploded over the past 18 years.[79]

The United States now leads the world in the number of billionaires—900 billionaires, which is around one-third of all billionaires globally.[80] As of June 2026, the world's 10 richest individuals, nine of them based in the United States,[81] held a combined wealth of roughly $2.9 trillion—an amount more than the GDPs of all the countries in the world, except for the top seven.[82] Nine of the richest 10 are tech oligarchs. Analysts have compared the present moment to the Gilded Age, a reference to the 30-year period from 1870 to 1900, which was marked by extreme inequality.[83] Meanwhile, millions of people in the United States are trapped by persistent, multigenerational poverty caused by political and economic disenfranchisement.[84] Economic marginalization is racialized, disproportionately impacting Black and Latinx communities.[85]

Forcing working people to focus on securing the survival of their families on a month-to-month (or day-to-day) basis reduces the capacity of the majority to organize for better conditions. It also gives the wealthiest a free hand to influence law and politics in a manner that favors the concentration of resources at the expense of the majority.

Changes to campaign contribution laws have created a situation in which the richest people in the nation spend unimaginable amounts of money to influence elections and shape the political agenda. Recent reporting reveals a 50-year effort by some of the wealthiest families in the nation to undo any



limits to campaign finance laws.[86] The Supreme Court's Citizens United decision in 2010 lifted caps on campaign contributions by corporations, opening the floodgates for corporate power over democracy.[87]

Recent electoral cycles have seen sectors including cryptocurrency and AI, as well as tech billionaires—many of whom are venture capitalists—emerge as campaign donation heavyweights.[88] These sectors are deeply bound to arms manufacturing and military industries. The first venture capital firm in the US was founded to profit from new technologies developed for use in WWII, and the role of military spending in turning Silicon Valley into a tech hub is well documented.[89]

The influence of astronomically wealthy, power-hungry venture capitalists promises unchecked development of deadly new technologies, a massive expansion of the US military bureaucracy, and US foreign policy primed for more endless war.[90]

Innovation for "Democracy"

In January 2026, the Department of Defense issued its "AI acceleration strategy," encouraging AI implementation and experimentation across the military, supporting investment in AI infrastructure, and the pursuit of major AI-powered projects.[91] Just six months later, research found that venture capital—led by Anduril Industries—has invested billions in military tech, including AI-powered military systems.[92] These investments promise to be rewarded as the 2027 federal budget includes record Pentagon funding estimated at nearly $1.5 trillion.[93]

While the prime contractors still play a central role in US militarism,[94] venture capital firms have been positioning themselves as essential to the "modernization" of the Department of Defense (now rebranded as the Department of War).

Prominent venture capitalist tech innovators have espoused varying theories of what is needed for democracy and the future of US national security, tying their business model to being key providers of technological innovation to the US military and DHS. Palantir's website states: "We built Palantir to ensure the future of the West, not to tinker at the

Some highlights of tech oligarchs and the current administration.



David Sacks

Former COO of PayPal, VC investments in Palantir and SpaceX; Top adviser on AI and cryptocurrency, co-chair President's Council of Advisors on Science and Technology.[161]

Est. net worth: $2 billion.[162]



Marc Andreessen

Co-founder of Andreessen Horowitz (also known as a16z). Involved with staffing for DOGE.[163]

Net worth: $1.9 billion.[164]



Palmer Luckey

Founder of Anduril Industries. Suggested rebranding to "Department of War."165 Now valued at $31 billion, 80% of Anduril's revenue is from US government. A former Anduril employee, Antoine McCord, is now the Chief Intelligence Officer and Chief AI Officer at DHS. McCord was given control over the DHS Office of Biometric Management in August 2025.[166]

Net worth: $5 billion.[167]



Peter Thiel

Venture capitalist with an extensive network (through monetary, social, or work connections) in the current administration, including VP JD Vance; Jacob Helberg, Under Secretary of State for Economic Affairs; Gregory Barbaccia, US Chief Information Officer; Jim O'Neill, Deputy Sec of HSS; and Michael Krastios, Director of Office of Science and Technology Policy, and more.

Net worth: $27.6 billion.[168]



Elon Musk

One of Trump's top donors and hired as a "special government employee" and tasked with running the Department of Government Efficiency (DOGE). Musk's companies' contracts with the federal government are estimated at over $38 billion.[169]

Net worth: $1.2 trillion.[170]

margins."[95] In 2009, its co-founder Peter Thiel wrote, "I no longer believe that freedom and democracy are compatible."[96]

Anduril's 2022 mission document, "Rebooting the Arsenal of Democracy," calls for a new breed of agile tech companies to lead innovation in the US military.[97] Anduril CEO Palmer Luckey, also a longtime Trump supporter, has advocated for the removal of all undocumented immigrants on account of their being a threat to democracy—"we cannot let them stay."[98] Luckey was named the "It Guy of the booming defense-technology industry" in a *New York Times* feature from March 2026.[99] Following the election of Trump in November 2024, Anduril's Luckey expressed that the incoming administration would be good for tech startups.[100] Building its fortune on border surveillance technologies and autonomous fighter jets, Anduril is seen as key to the 21st-century US military. His company has netted over half a billion dollars in federal contracts building AI drones intended for border surveillance and migrant crackdowns.[101] In 2024, Anduril reportedly derived 80% of its revenue from US government contracts.[102]

Andreessen Horowitz launched American Dynamism in 2022, a techno solutionist fund that states that it is "vital" for start-ups to solve "serious American problems"—from national security and public safety to housing and education.[103] The embrace of this vision by the administration came through in 2025 when Vice-President Vance spoke about how the Trump administration is embracing American Dynamism.[104]

Anduril's 2022 mission document, "Rebooting the Arsenal of Democracy," calls for a new breed of agile tech companies to lead innovation in the US military. Anduril CEO Palmer Luckey, also a longtime Trump supporter, has advocated for removal of all undocumented immigrants on account of their being a threat to democracy—"we cannot let them stay."

Palantir CEO Alex Karp's 2025 book *The Technological Republic: Hard Power, Soft Belief and the Future of the West*, outlines his belief that the United States is in an AI arms race, that Silicon Valley must get involved in "fighting violent crime," and that "some cultures have produced vital advances; others remain dysfunctional and regressive."[105] Although Karp claims to believe in freedom and democracy, *The Technological Republic* is best understood as a manifesto for a securitized, militarized, and highly surveilled future.

The Future of War

One indicator of the accelerating tech-military partnership is the recent military appointment of employees from specific tech companies. Last June, the US Army launched Detachment 201, which it dubbed the Executive Innovation Corps, and announced the first intake of Army Reserve Lieutenant Colonels drawn from the tech sector: Palantir's Shyam Sankar, Meta's Andrew Bosworth, OpenAI's Kevin Weil and Bob McGrew from Thinking Machines.[106] An Anduril employee was nominated for Army Under Secretary and sworn in on September 22, 2025.[107]

This is just one manifestation of how tech and venture capital firms have become increasingly integrated within the US government—the outcome of a concerted effort to make technology and military corporations central to modern warmaking.[108]

Months after 9/11, Secretary of Defense and corporate strongman Donald Rumsfeld pushed for increased private sector involvement at the Pentagon, giving "a small group of venture capitalist consultants" access to the largest military budget in the world—an initiative with its roots in the neoliberal turn under President Reagan.[109] Over the decades that followed, venture capital has become even more intertwined with the growing sphere of securitization, surveillance, and tech for war. Two of the most powerful tech oligarchs—Thiel and Musk—were early beneficiaries of the Pentagon's private sector orientation.[110]

The ties between Silicon Valley and the Pentagon run deep.[111] The internet would not exist without US military funding.[112] Palantir and Anduril, both core military contractors—were founded with funding from In-Q-Tel (IQT), a non-profit launched by the CIA, to bridge the gap between the national security establishment and tech innovation.[113]

The Pentagon's flagship AI initiative, the Artificial Intelligence Rapid Capabilities Cell is run by departments that have effectively outsourced it to Palantir, Anduril, and Generative AI companies like Open AI.[114] The people running the initiative essentially serve as proxies for Palantir and Anduril investors, among them David Sacks and Michael Kratsios, who are the co-chairs of the President's Council of Advisors on Science and Technology.[115]

The US Military—Tech's Golden Goose

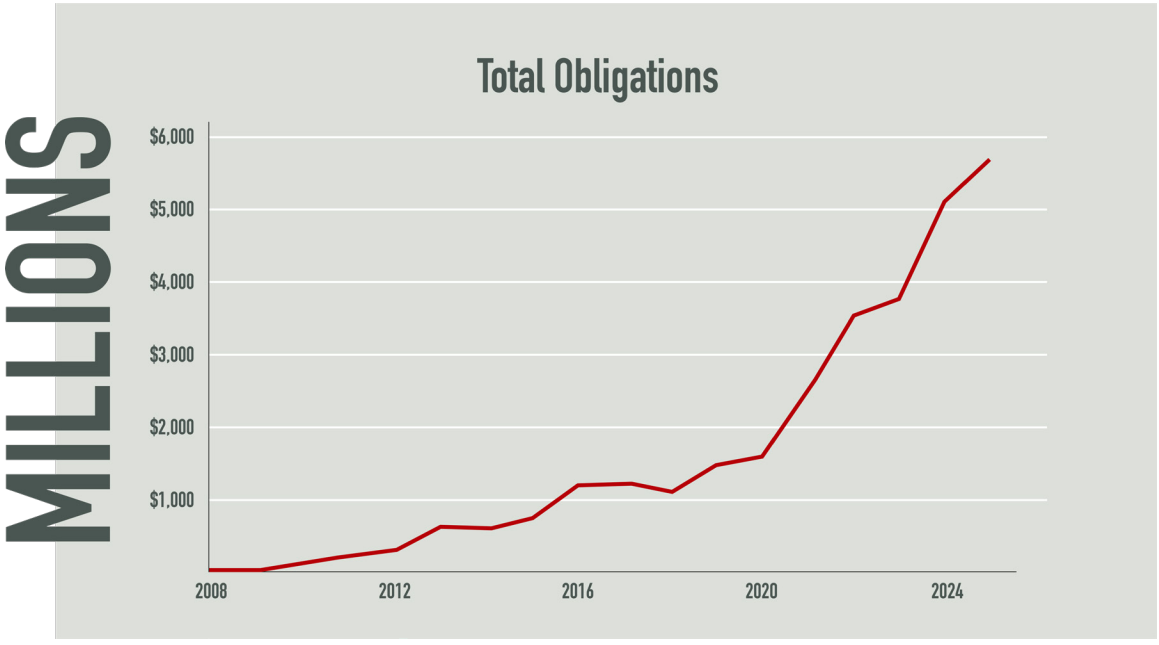
The Trump administration's unprecedented $1.5 trillion military budget request for 2027 is just one more golden goose for the tech interests. It contains a massive increase in funding for new tech, with $53.6 billion proposed for the mass procurement of drones, counter-drone systems, and uncrewed logistics systems; $46 billion for AI infrastructure and "disruptive capabilities"; and $17.1 billion for the unfeasible Golden Dome missile defense project.[116]

As described in section three of this report, a massive expansion in DHS funding is linked to a parallel expansion in new federal contracts for AI, surveillance technology in immigration enforcement, and bordering. Venture capital-funded companies can be expected to land major windfalls from these funds, including those affiliated with the Trump family.[117]

Figure 1 charts total annual funding obligations awarded by the US government to the 100 largest venture-backed startups in generative AI, defense, and security technology, the very firms funded by the very tech oligarch investors mapped throughout this analysis. The trajectory is unmistakable: after more than a decade of modest, incremental growth hovering below $1 billion annually, a steep rise begins in 2020, skyrocketing from nearly $1.5 billion that year to nearly $6 billion by 2025. This explosive growth does not reflect a natural market evolution. It is the material signature of a deliberate campaign by venture capital-funded companies,[118] and accelerated under an administration receptive to their vision.

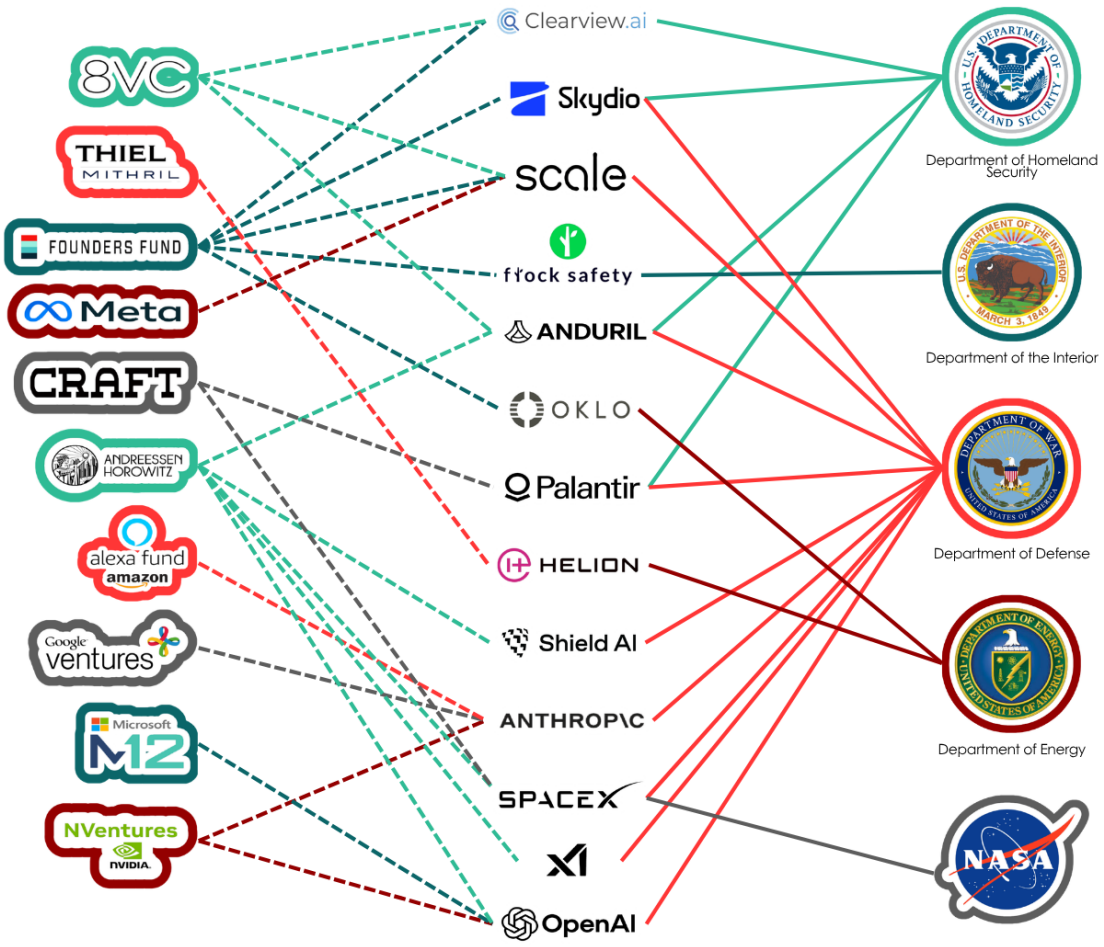
Through various rounds of funding, money flows from venture capital firms—as well as the venture arms of big tech companies—to military and security tech startups. These companies then

Figure 1 *Government awards to surveillance, defense, and AI companies founded by tech oligarchs*



Source: Empower LLC, with data from USAspending.gov and Crunchbase.

Figure 2 *The Money Flow to the Tech Oligarchy's Startups*



Source: Empower

reap the benefits of big government contracts from departments such as DHS, the Department of Defense, NASA, and the Department of Energy, among others. **Figure 2** illustrates some of these money flows.

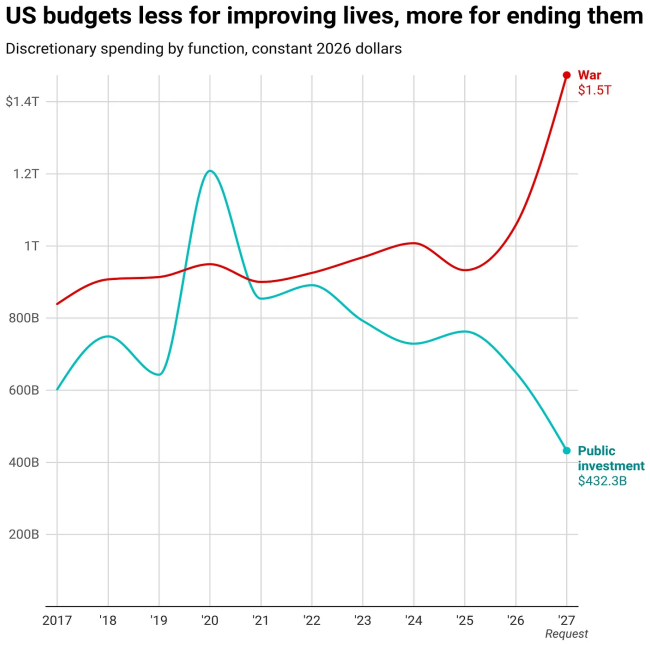
The wealth that the tech oligarchs are gaining through federal funding is coming at great cost to basic human needs and the planet. An analysis of the president's 2026 budget request found that over 75% was for military and police—shifting funding from housing, health, education and what the administration labels "woke programs"[119]—as depicted in **Figure 3**.

The president's current budget request of an unprecedented $1.5 trillion includes a 42% increase for war, further threatening cuts to essential necessities, such as affordable health care and food.[120] Rather than funding militarized solutions, a trillion-dollar budget allocation for human needs could address national nursing and teacher shortages, provide health care to millions, erase all medical debt, replace lead pipes for safer drinking water, build high speed rail, and more.[121]

Policy and Influence

Lobbying and campaign contributions are the two most transparent mechanisms for bending public policy in favor of corporate interests. The constellation of venture capital firms and portfolio companies tied to Thiel, Andreessen, David Sacks, and other investors aligned with the Trump administration have made a concerted effort to gain favorable treatment in matters of regulation and procurement through both avenues.

Figure 3 *Comparison of Trump's budget request for war versus public investment*[180]



Campaign Contributions

The storied images of the tech oligarchs, including Mark Zuckerberg (Meta), Jeff Bezos (Amazon), Sundar Pichai (Google), and Elon Musk (Tesla, X, SpaceX, Starlink), at the 2025 inauguration was understood as signaling their alignment to the Trump agenda.[122]

In 2024, 10 individual wealthy donors supplied nearly half the money raised by Trump's election campaign.[123] Musk, the sole tech figure among the top three individual donors, donated $290 million and was subsequently appointed as a special government employee, given access to the Treasury Department's payment systems, and empowered to restructure federal agencies through DOGE.

Thiel was an early supporter of Trump's presidential bids, donating over $1 million to the 2016 campaign. He went on to donate $15 million each to the 2022 US Senate campaigns of two former employees. In a campaign finance experiment akin to a long-shot VC investment, he donated a record $15 million to a Super PAC supporting 2022 Republican Senate candidate JD Vance in Ohio and another $15 million to one supporting Blake Masters in Arizona.[124] One of his bets paid off doubly, when Vance—a former Andreessen Horowitz-backed entrepreneur who had been cultivated by Thiel's network for years[125]—was selected as Vice President shortly after winning a Senate seat.

Palantir CEO Alex Karp is another major Silicon Valley figure who has been described as moving from "Biden donor to Trump enabler," donating $1 million dollars to Trump's 2024 inauguration.[126] As seen in Table 1, the 2024 Trump campaign saw a wave of new campaign contributions from a cohort of Silicon Valley founders and investors, led by Musk and rounded out by younger multi-billionaires Joe Lonsdale and Palmer Luckey.

Meta, Amazon, Google, and Microsoft, as well as Apple CEO Tim Cook, and OpenAI CEO Sam Altman, all donated at least $1 million to Trump's inaugural

Table 1 *Political Contributions*

Donor	2016 Trump contributions (USD)	2020 Trump contributions (USD)	2024 Trump contributions (USD)
Marc Andreessen	--	--	6,133,700[171]
Ben Horowitz	--	--	2,500,000[172]
Joe Lonsdale	--	--	1,000,000[173]
Palmer Luckey	110,000[174]	1,661,600[175]	400,000[176]
Elon Musk	--	--	290,000,000[177]
David Sacks	--	--	790,100[178]
Peter Thiel	1,497,300[179]	--	--

Source: US Federal Election Commission.

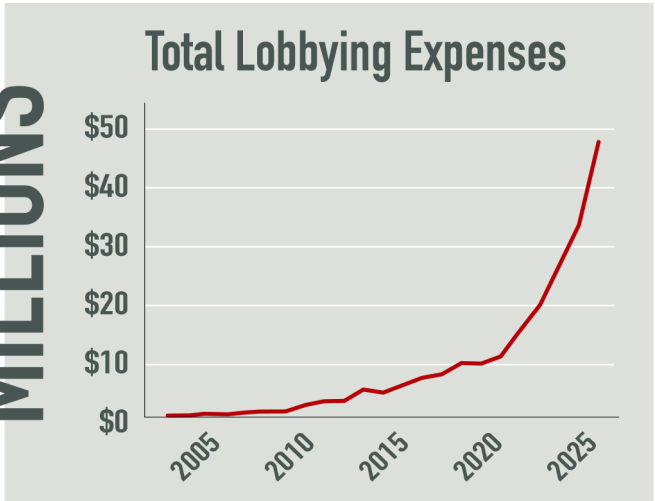
fund.[127] While these big tech companies and CEOs did not make significant contributions to the Trump campaign itself, the coordinated, symbolic gesture to fund the inauguration indicated a dramatic shift and a new political understanding—one that is aligned on tech-sector deregulation to proliferate AI and crypto, as well as growing access to lucrative federal military and DHS contracts.[128]

Lobbying

On the lobbying front, expenditures by the venture capital firms of Trump's highest profile tech allies—Thiel, Lonsdale, Sacks, and Andreessen—and their defense, surveillance, and AI portfolio companies have increased astronomically in recent years, more than quadrupling since 2020 to some $47 million by 2025 (see **Figure 4**). SpaceX and Palantir are leaders in lobbying contributions—Palantir ($9.4 million) and SpaceX ($4.8 million) accounted for 30.5% of 2025 lobbying by these companies ($46.5 million). For purposes of comparison, this is more than big tech cloud giants Google, Amazon, and Microsoft spent on lobbying in 2025, combined.[129]

After SpaceX and Palantir, the top spenders on federal lobbying among companies with venture capital funding are Anduril; aerospace and defense company Shield AI; the venture capital firm Andreessen Horowitz itself; and Sam Altman's OpenAI, which won a $200 million contract with the Pentagon in 2025 (see **Figure 5**). Other notable spenders include Skydio, a major provider of drones

Figure 4 *Federal lobbying expenditures by tech oligarchy venture capital firms and portfolio companies (2000-2025)*



Source: Empower, with data from Lobbying Disclosure Act database

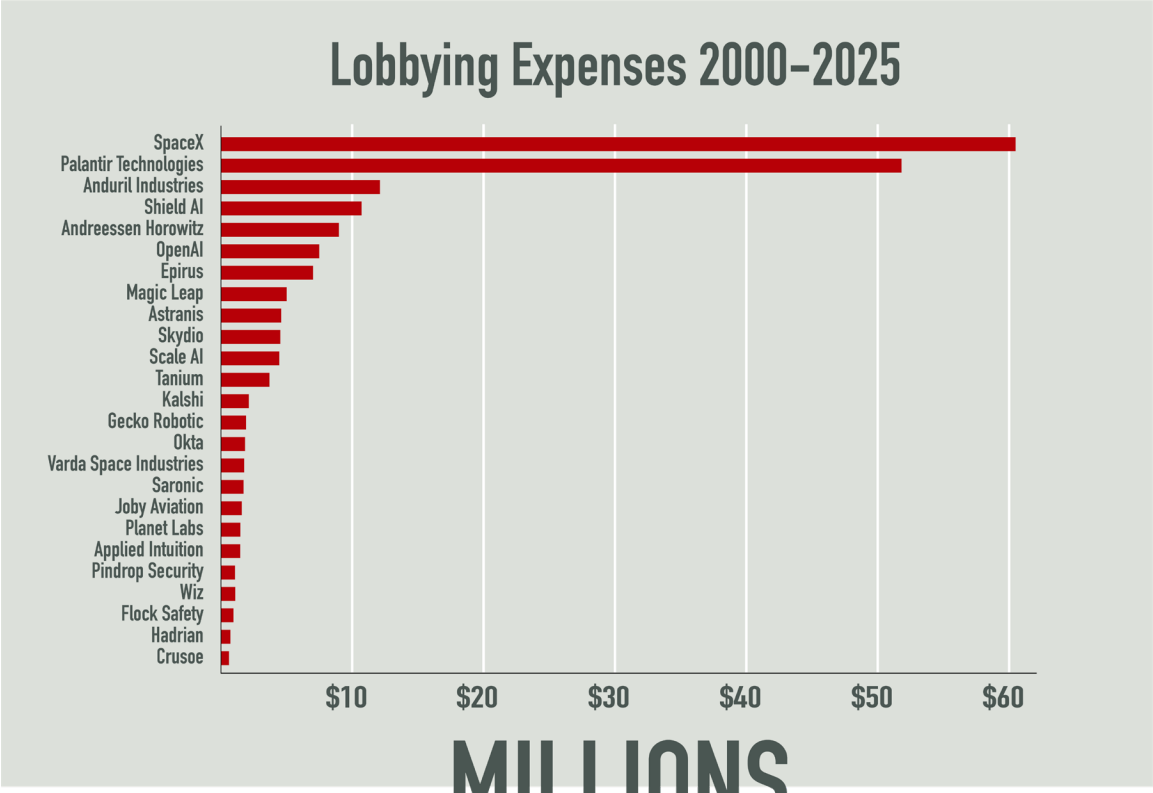
SpaceX and Palantir are leaders in lobbying contributions—Palantir ($9.4 million) and SpaceX ($4.8 million) accounted for 30.5% of 2025 lobbying by these companies ($46.5 million). For purposes of comparison, this is more than big tech cloud giants Google, Amazon, and Microsoft spent on lobbying in 2025, combined.

for ICE and CBP; Scale AI, which signed a multi-million-dollar contract in 2025 with the Pentagon for AI agents to help with military planning and operations;[130] and Flock Safety, a license plate recognition company that has contracts with more than 4,800 law enforcement agencies in 49 states and whose data has been shared by local police officers across the country with ICE.[131]

As shown in the above graphic, the approximately $200 million these companies have spent on federal lobbying since 2000 has netted in nearly $6 billion in federal contracts for the same group of companies.

One in four federal lobbyists are pushing AI agendas. For example, a little-known group called the Innovative Future Collective, founded in December 2024 by the political fundraising firm Fulkerson Kennedy & Company, has been quietly flying congressional staffers on luxury trips to San Francisco, Los Angeles, London, and New York City.[132] House and Senate gift travel disclosures indicate that these junkets take senior aides to tour AI companies including OpenAI, Meta, Amazon, Palantir, and Anduril, with stays at five-star hotels like London's Marriott Hotel Grosvenor Square. The Innovative Future Collective's Advisory Committee is dominated by corporate interests: of its 15 members, 12 are current or recent corporate lobbyists, including at least six lobbyists for OpenAI and the venture capital firm Andreessen Horowitz. Another advisor is a Microsoft public policy executive.[133]

Figure 5 *Top 25 spenders on federal lobbying among defense, surveillance, and AI portfolio companies of tech oligarchy firms (2000–2025)*



Source: Empower, with data from Lobbying Disclosure Act database

Profit Driven Policy

After systematically dismantling prior policy from the Biden administration, the Trump administration has removed guardrails, eliminated civil rights protocols, and instituted new policies aimed at aggrandizing AI procurement. Two planks underlie these new policies: (1) the creation of a new regulatory framework that incorporates MAGA hostility towards civil rights protections of traditional minorities, and (2) a multi-pronged plan to advance industry friendly AI rules while attacking regulatory measures taken by states. The architects of these policies stand to financially benefit from these policies.

In July 2025, Trump issued an executive order (EO) announcing the end of "Woke AI," through the establishment of "Unbiased AI Principles" that, among other things, required federal contractors to certify that their products comply with the Unbiased AI principles.[134] The new "Unbiased AI Principles," now embedded in all federal AI policy and procurement protocols, claim to adopt "truth-seeking" and "ideological neutrality," without defining what these terms mean. Despite claims that the EO and implementing regulations herald an era of "deregulation,"[135] new ideological requirements tied to the "Unbiased AI principles" guts legacy civil rights and privacy laws in favor of a new expansive regulatory framework.[136] To illustrate an application of the new policy, the Trump administration shockingly described DEI as such:

> *"One of the most pervasive and destructive of these ideologies is so-called "diversity, equity, and inclusion" (DEI). In the AI context, DEI includes the suppression or distortion of factual information about race or sex; manipulation of racial or sexual representation in model outputs; incorporation of concepts like critical race theory, transgenderism, unconscious bias, intersectionality, and systemic racism; and discrimination on the basis of race or sex. DEI displaces the commitment to truth in favor of preferred outcomes and, as recent history illustrates, poses an existential threat to reliable AI."*[137]

In concert with this EO, former crypto czar David Sacks, former Peter Thiel advisor Michael Kratsios, and Secretary of State Marco Rubio co-authored "America's AI Action Plan,"[138] a White House strategy that captures critical infrastructure (including the electric grid via data centers) and recommends investing public dollars for AI innovation so that "America has the most powerful AI systems in the world." Serving as co-chair of the President's Council of Advisors on Science and Technology (PCAST), Sacks is shaping US AI policy with other C-suite executives.[139] He has managed to obtain waivers from the US government to hold hundreds of financial investments in the crypto and AI companies who will benefit from that policy.[140] (David Sacks has made numerous statements about immigration, claiming that the failure of US immigration policy is that we have let in immigrants with "average IQs" compared to Elon Musk of South Africa and Jensen Huang of Nvidia.[141])

The AI action plan echoes the abovementioned Unbiased AI principle executive order by purporting to support "free speech" and "truth" instead of "social engineering agendas." Furthermore, the AI Action Plan instructs DOJ to litigate against state AI laws or policies that conflict with federal policy and proposes eliminating funding for states with their own AI laws and policies that conflict with federal guidance.[142]

Lastly, the Trump administration's "deregulatory" agenda carries deep implications for federal procurement.[143] As the government is now required to procure more commercial systems, companies will rake in huge profits. Procurement over AI systems now faces substantive hurdles because the DHS AI strategy calls for "continuous authorization" without "expiration dates."[144] Additionally, the White House also mandates "promoting the use of commercial options," including AI systems unless they fail "unbiased AI principles" tests or other Trump procurement requirements.[145]

Former crypto czar Sacks, former Thiel advisor Kratsios, and Secretary of State Rubio co-authored "America's AI Action Plan" a White House strategy that [among other things] instructs DOJ to litigate against state AI laws or policies that conflict with federal policy.

Bulldozing Guardrails and Oversight

Immediately after the announcement of its membership in March 2026, the PCAST released a framework for AI policy that pushes for broad preemption of state AI laws and against "open-ended liability" for AI firms.[146] The preemption framework supported by the Trump administration—and written by its "revolving-door" venture capital allies—is designed to override state-level AI safety and privacy protections.[147]

The administration is pushing for a uniform federal framework that would block states like California, Colorado, and New York from enacting their own, often stricter, AI regulations, ensuring that the rules governing AI are written by and for the industry's dominant players, preempting any local experimentation with public accountability.[148] Through a combination of a DOJ-led "AI litigation task force" and other agency audits to ensure that "DEI' is not embedded in AI models, the White House's AI framework simultaneously echoes MAGA and Silicon Valley concerns.[149] In April 2026, DOJ intervened in a lawsuit brought by Musk's xAI against Colorado's anti-discrimination in AI law that imposed risk-mitigation steps for AI systems used in housing, healthcare and finance.[150] A committed Trump loyalist, former Attorney General Pam Bondi's appointment to PCAST suggests that she will orchestrate and broaden the legal strategy to implement the AI Action plan, "placing the former attorney general at the center of the White House's expanding artificial intelligence agenda."[151]

Meanwhile, the same investors are molding the administration's position on cryptocurrency, with Sacks having led the administration's 2025 crypto-related executive orders in his role as Chair of the President's Working Group on Digital Assets

Markets.[152] As part of the same push for pro-crypto legislation, Andreessen and Horowitz have poured tens of millions of dollars into the bipartisan, pro-crypto Fairshake PAC for federal elections alongside Coinbase and Ripple Labs, startups in which their venture capital firm, a16z, was a major early investor.[153]

In late 2025, Andreessen founded a new federal PAC called Leading the Future, alongside Joe Lonsdale and OpenAI's Greg Brockman, which is modeled after the Fairshake PAC but focused on AI legislation. The group was reportedly met with frustration from the White House, given its bipartisan orientation. One White House official opined that "any donors or supporters of this group should think twice about getting on the wrong side of Trump world," as "we are carefully monitoring who is involved."[154] Notably, Lonsdale has not made any reported contributions to the PAC despite reportedly being a co-founder.[155]

The boldness of this initiative—funded with over $125 million as of May 2026—indicates that firms like Andreessen Horowitz may already be imagining themselves as the tail that wags the dog on AI and crypto policy heading into the 2026 midterms.[156] This comes as an April 2026 Politico poll indicates that "more than half of Americans say they have never and would not consider buying or trading cryptocurrency," and "a 43% plurality say the risks of [AI] technology outweigh the benefits," showing just how important it will be to buy legislators' support on these issues.[157]

Trump has also implemented a deregulatory agenda with the vision of cementing US dominance through a privately funded data center boom and an AI arms race against China. Google, Microsoft, Amazon, and Meta spent an estimated $360 billion on AI data centers in 2025 alone.[158] These data centers are currently being built, opaquely, in clusters where there is cheap land, cheap energy, and major tax incentives—regardless of the well-documented health, environmental, or economic costs.[159] Concomitantly, the Trump administration has been gutting the Environmental Protection Agency through mass firings and the elimination of its research and development arm.[160]

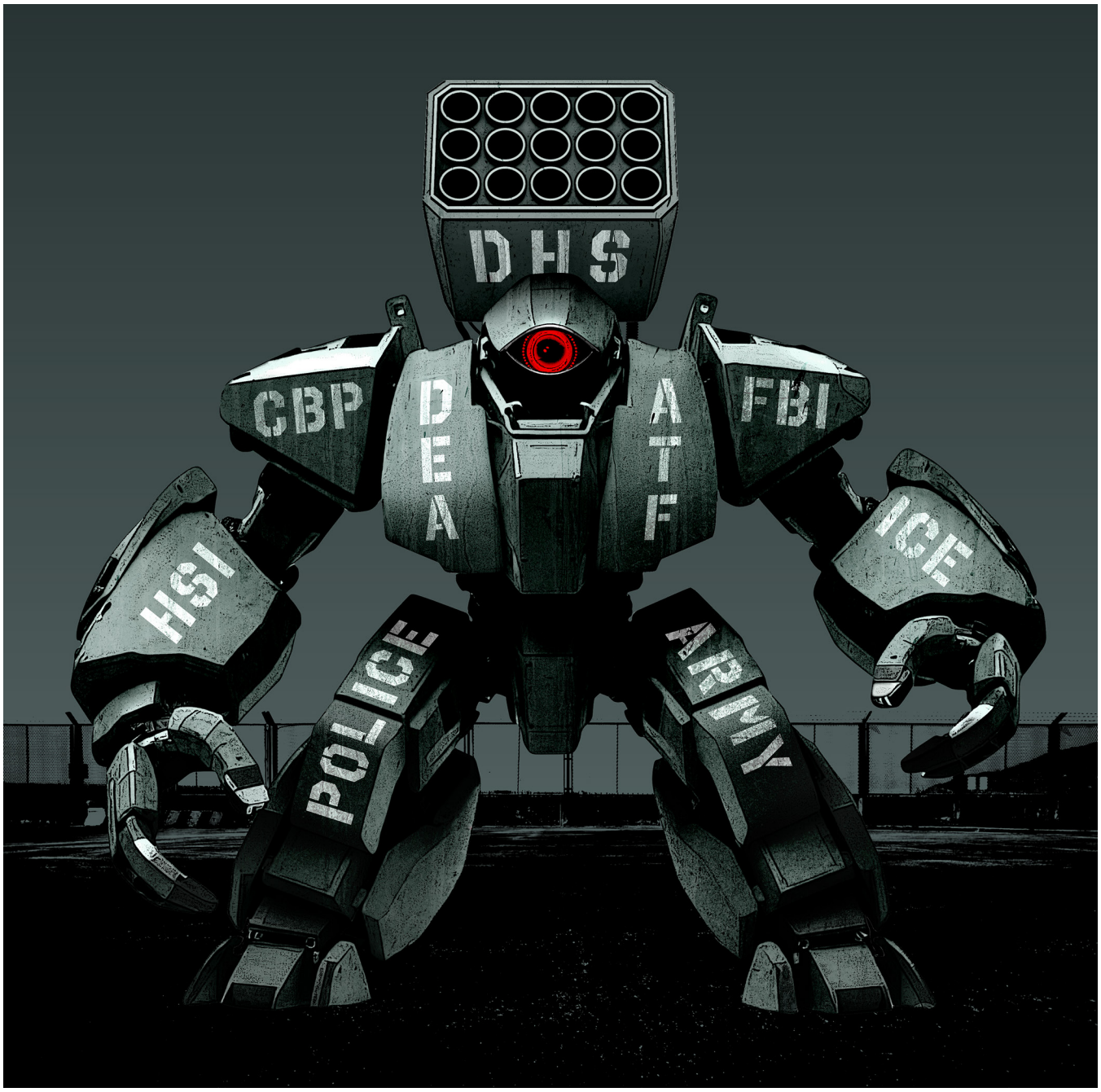
So far, this report has documented the growing authoritarianism expressed through DHS's immigration enforcement and the growing alliance between tech and the Trump administration—especially in the realms of national security and homeland security. In the next section of this report, we demonstrate how these pieces come together: how the tech sector's deep entanglement with the security state is supercharging DHS's authoritarian immigration enforcement powers and accelerating a transformation of the United States into a militarized police state.

3. Building the Militarized Police State

Immigrant policing is the perfect pretext to further intensify the surveillance model, and this has been scaled by direct legislative mandates and continually increasing pots of funding.

Over the last two decades, the federal government has steadily expanded the legal authority, funding, personnel, and technological infrastructure necessary to build a far more militarized system of domestic policing and surveillance. Successive administrations have normalized extraordinary levels of enforcement, information-sharing, and security spending in the name of national security, border control, and narrow notions of public "safety."

Since its inception, DHS has been growing its policing power to realize its extremely broad and ambitious mandate. This includes building substantial policing personnel (ICE and CBP) through



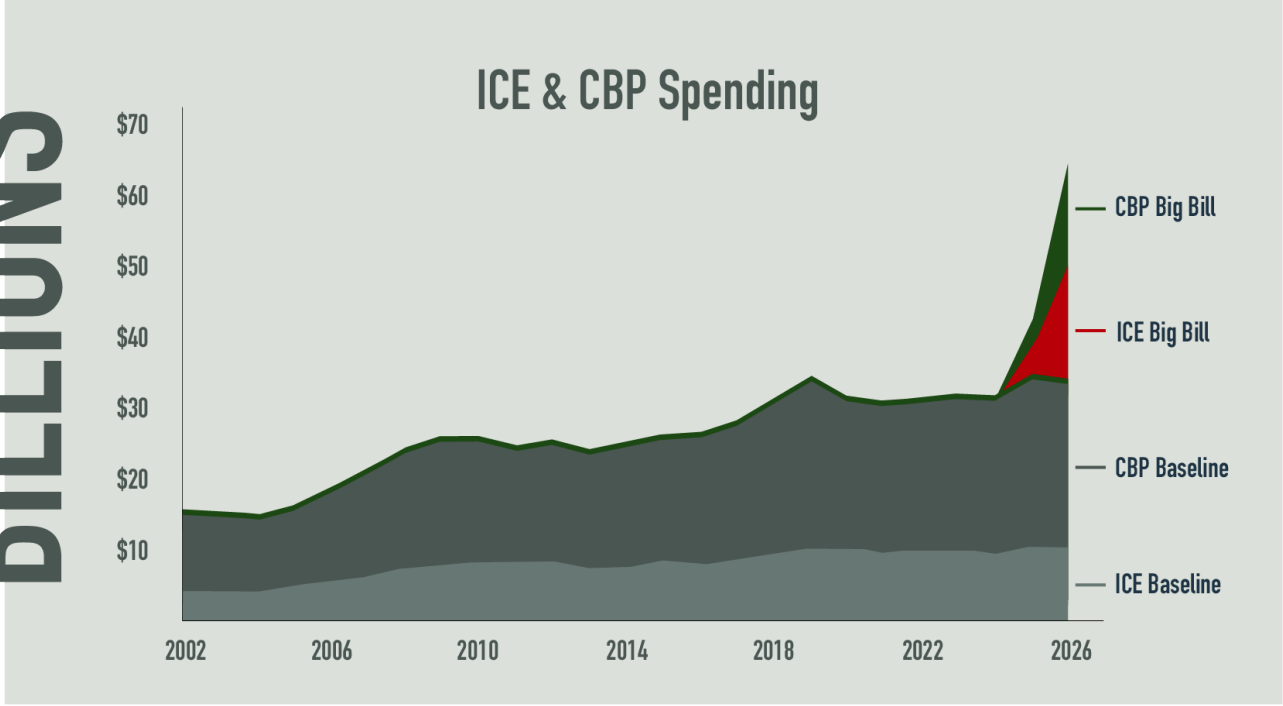
"force multipliers" that increase cooperation and information sharing between DHS and civilian agencies,[181] and most notably, local, state, federal police, and international police counterparts.[182] The federal government has crafted a system of wide-ranging surveillance—including by building a network of intelligence fusion centers[183]—and diverted federal funding and weapons to key partners in its efforts to expand the reach of DHS into local and state police departments.[184]

The use of the criminal legal system has been critical for DHS, which has pushed for maximal information sharing and collaboration between local and state police and ICE. The fights against 287(g) agreements and other police collaboration with ICE (through the DHS "Secure Communities" program and compliance with ICE detainer requests) have become a key site of immigrant rights advocacy.[185]

While local police have been found to arrest people for routine traffic violations, for example, in order to turn them over to ICE, 287(g) further empowers police by giving them authority to arrest people for suspected immigration violations. A February 2026 study found participation in 287(g) has grown by 900% under the new Trump administration. This effectively means upwards of 15,800 police officers and sheriff's deputies nationwide can participate directly in ICE surveillance and arrests. The June 2026 budget reconciliation bill pushed through by the Trump administration—the second such bill to increase DHS funding in less than a year—included $350 million specifically for ICE operations in cities and states that do not participate in 287(g) agreements.[186]

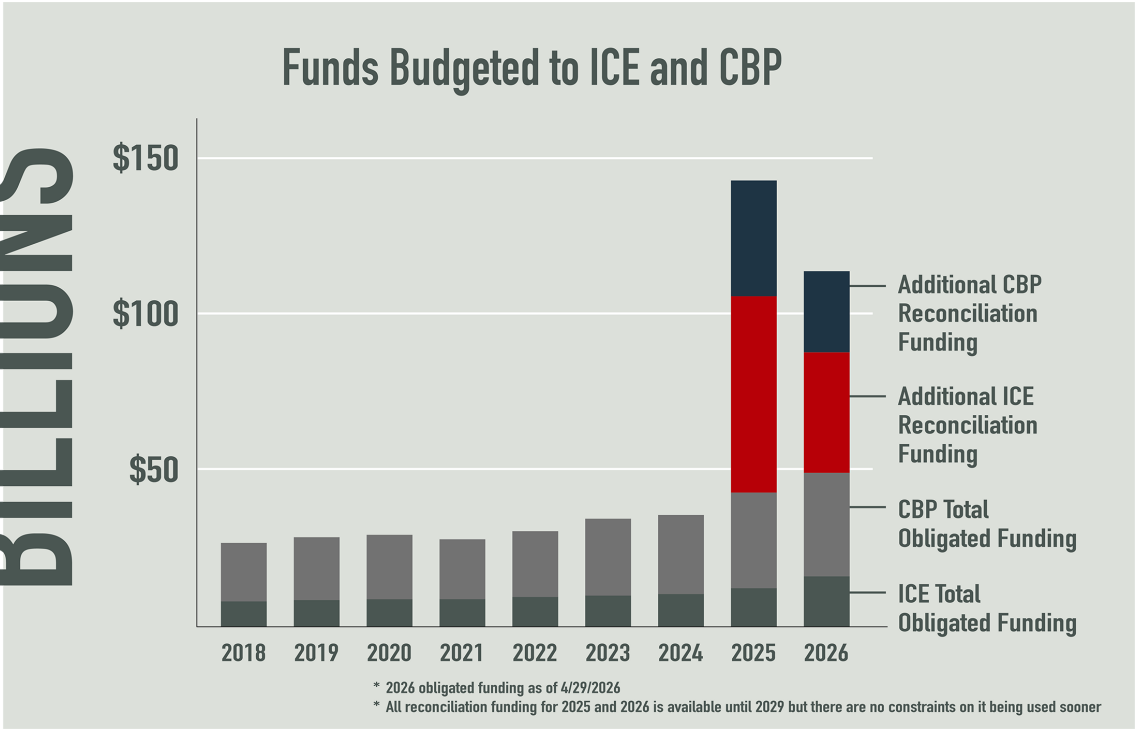
The federal government has crafted a system of wide-ranging surveillance—including by building a network of intelligence fusion centers—and diverted federal funding and weapons to key partners in its efforts to expand the reach of DHS into local and state police departments.

Figure 6 *Projected ICE and CBP spending under OBBBA (2002-2026)*



Adapted from Institute for Policy Studies[206]

Figure 7 *ICE and CBP Budget as of June 2026*



Source: USA spending.gov and American Immigration Council.

More Money

In July 2025 and June 2026, DHS received two massive budget increases forced through by the Trump administration using the reconciliation process. The One Big Beautiful Bill Act (OBBBA), passed in July 2025, and the Secure America Act, passed in June 2026, provided a huge boost for the militarized police state. These bills dramatically expanded federal deficits, while simultaneously providing the financial architecture to enact Trump's core immigration policies of mass deportation and detention, underpinned by an unprecedented expansion of surveillance. The bills also provide for outstanding funds to integrate AI into various government departments, most notably into military technologies—translating directly into lucrative contracts for the private firms aligned with the administration.[187]

Despite deep cuts elsewhere, in 2025 DHS received an additional $191 billion through the OBBBA, primarily for immigration enforcement, including $74 billion for ICE and $64 billion for CBP.[188] Some $6 billion of the CBP spending was earmarked directly for border surveillance technology. As seen in **Figure 7**, some of this funding has already been obligated under the 2025 and 2026 budgets. Then, less than a year later, the June 2026 Secure America Act provided an additional $38.5 billion for ICE and $26 billion for CBP, including $5 billion for border security technology and screening using AI.[189]

The scale of this redirected capital is staggering and immediate. In the two quarters following the passage of OBBBA, ICE spending on contracts more than doubled to $3.7 billion, while CBP's spending increased sevenfold between the first and second halves of 2025, with a surge of nearly $2.7 billion in new contracted work reported in January 2026 alone—more in a single month than in the entire first half of 2025.[190] The June 2026 reconciliation bill will surely result in even more dramatic spending increases on private-sector military and surveillance technologies by ICE and CBP.

More ICE Police

The most visible domestic showing of Trump's stated goal of deporting one million people a year[191] has been the aggressive and cruel high-profile mass deportation operations in cities like Minneapolis,

In the two quarters following the passage of Trump's landmark bill, ICE spending on contracts more than doubled to $3.7 billion, while CBP's spending increased sevenfold between the first and second halves of 2025, with a surge of nearly $2.7 billion in new contracted work reported in January 2026 alone—more in a single month than in the entire first half of 2025.

Chicago, and Los Angeles. The president has wielded the military and ICE as a threat to further his agenda, treating them as his own personal police force.[192]

Six months after signing the OBBBA in July 2025, the White House announced that it had grown its workforce 120% after hiring more than 12,000 officers and agents in an unprecedented hiring push.[193] This recruitment process included a series of bonuses and pay increases, including a $50,000 signing bonus.[194] While most agencies saw staffing reductions driven by the Department of Government Efficiency, DHS's workforce grew by 6%, up to 271,927 employees.[195] Starting with dozens of officers dedicated to raid arrests in 2003,[196] ICE has grown into a heavily militarized force of tens of thousands, equipped with the tools of warfare to deploy against American communities. The scale of this buildup is stark and will grow even more, as detailed below.

More Weapons

According to a February 2026 report by Senator Adam Schiff, ICE and CBP committed to spending more than $144 million on weapons, ammunition, and accessories in the first year of President Trump's second term.[197] In just one year, ICE's spending on weapons surged by over 360%—from $16 million in 2024 to more than $76 million in 2025—while CBP's contracts for weapons more than doubled, from $33 million to $68 million. The weapons contracts lay out even greater spending in the future.

DHS's growing weapons arsenal extends to a vast array of "less-lethal" crowd control devices—which have been deployed with increasing frequency against US citizens. In 2025, ICE and CBP awarded more than $25 million in contracts for chemical munitions, TASERs, pepper sprays, and pepperball guns. In September 2025 alone, ICE and CBP obligated more than $11 million for TASER weapons and supplies from Axon Enterprises, following a federal judge's finding that federal agents had "unleashed crowd control weapons indiscriminately and with surprising savagery" against protesters in Los Angeles weeks earlier.[198]

In section 5, we detail DHS uses of technology tools for its mass deportation agenda.

More Data

DHS has scaled up deportation targeting through unregulated and unprecedented data sharing with DOGE, previously led by Elon Musk, which is harvesting and commingling federal data held by the IRS, Social Security, Medicaid, Housing and Urban Development, and many other agencies.[199] Through DOGE, DHS officials hope to potentially access information that could lead to the removal of seven million suspected noncitizens.[200] DOGE posited various reasons to justify the improper access, including a long debunked claim of widespread noncitizen voter fraud.[201] DOGE has yet to release any findings regarding purported election fraud, and speculation is rising that DOGE made massive data errors.[202] After Musk's departure, the mission of DOGE was reportedly carried on by Office of Management and Budget Director Russell Vought, a key architect of Project 2025.[203] Although DOGE's mandate sunsets on July 4, 2026, DOGE employees have joined other agencies while continuing to have access to sensitive data.[204] Despite multiple lawsuits, "DOGE affiliates appear to be digging in for the long haul—and Silicon Valley shaped fingerprints remain all over the way agencies continue to be run."[205]

4. Taxpayer-Funded Surveillance and AI

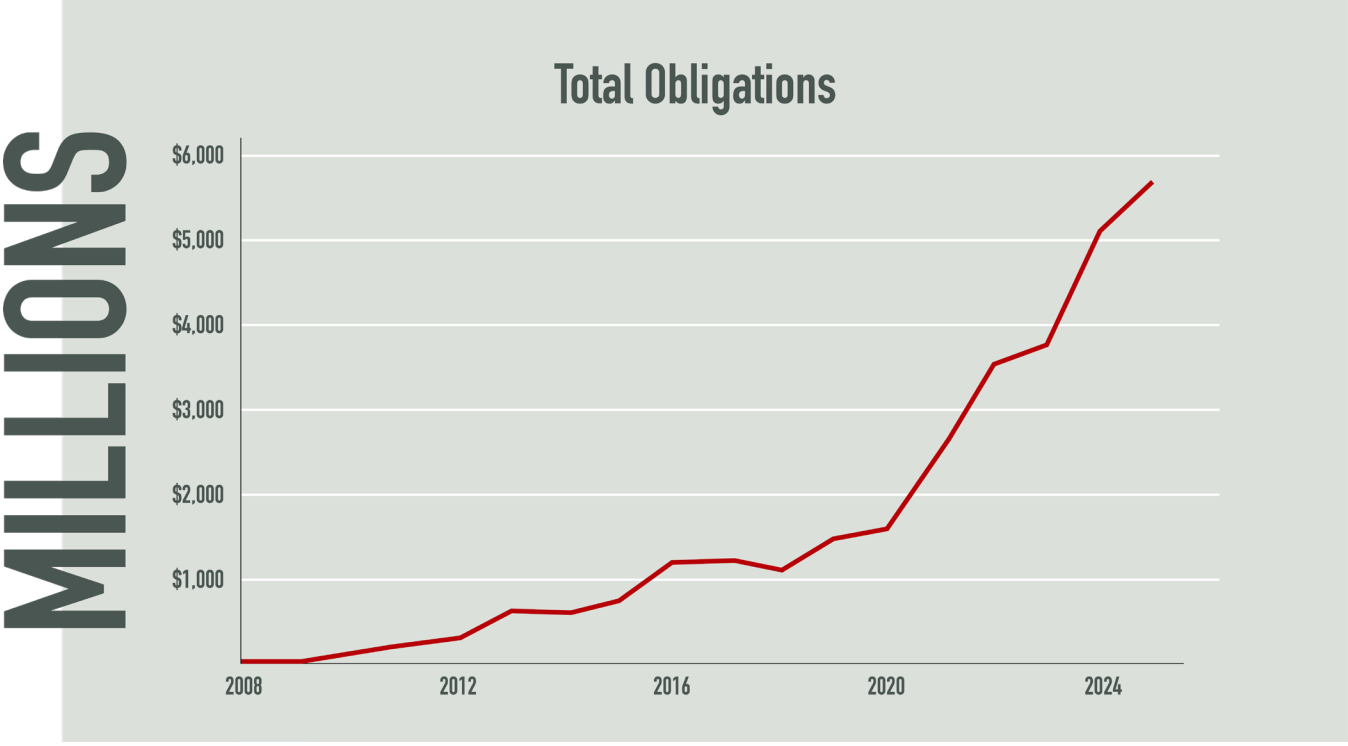
The federal government is diverting tens of billions of taxpayer funds to immigration enforcement while massively decreasing money for public health infrastructure, medical research, housing support, food support for families and children, and other public needs.[207]

The impact of new public capital for DHS surveillance and AI is immense. The federal government's partnership with tech venture capital firms has funneled federal contracts to tech and AI companies, further aligning Silicon Valley with the administration's national security and homeland security agenda. In this section, we will explore funding for companies providing contracts for DHS, the federal government's goals for AI-enabled immigration-focused surveillance along with DHS sandboxes where even more invasive surveillance tech capabilities are being dreamed up.

Figure 8 tracks total annual obligations awarded to the 100 largest venture-backed startups in generative AI, defense, and security technology. The trajectory is unmistakable: after more than a decade of modest, incremental growth hovering below $1 billion annually, obligations begin a steep ascent in 2020, skyrocketing from nearly $1.5 billion that year to nearly $6 billion by 2025.[208]

From July 1 to December 31, 2025, immediately following the passage of Trump's landmark bill, ICE spending on contracts more than doubled to $3.7 billion. CBP's spending increased sevenfold in the second half of 2025 as compared to the first half, followed by a surge of nearly $2.7 billion in new contracted work reported in January 2026 alone—more in a single month than in the entire first half of 2025.[209] A March 2026 investigation by WIRED found that ICE and CBP spent $515 million on products from tech giants in the last few years alone.[210] Our own analysis of ICE and CBP contract awards for surveillance tech companies also demonstrates shocking growth.

Figure 8 *Awards to surveillance, military, and AI companies funded by the tech oligarchy*



Source: Empower LLC, with data from USAspending.gov and Crunchbase.

The Role of Palantir

Palantir has been particularly successful in AI procurement expansion. Palantir initially obtained funding from the Central Intelligence Agency's venture capital arm, In-Q-Tel, in 2004—effectively gaining an entryway into government procurement.[243] Since Trump took office in January 2025, the company has received over $1.8 billion in government funding,[244] half of this from the Army.[245] Palantir signed a $10 billion Enterprise Service Agreement with the Army in 2025, for anticipated but uncommitted spending over the next 10 years.[246]

Palantir money from ICE has also ballooned during Trump's second term: the company's annual allotment from the agency quadrupled to $81 million in 2025, and rose again to $97 million from ICE in 2026 (see **Figure 9** below).[247] In February 2026, DHS cemented this relationship with a $1 billion blanket purchase agreement, a contracting vehicle that allows DHS agencies—including ICE and CBP—to skip competitive bidding for new Palantir products and services.[248]

The agreement came as Palantir faced internal unrest following the killing of a Minnesota nurse by ICE agents—an event that reportedly prompted staff to flood company Slack channels demanding answers about their technology's role in immigration enforcement. CEO Alex Karp responded with a nearly hourlong video that failed to address direct questions about how Palantir's tools power ICE.[249]

The evidence from federal procurement records demonstrates how deeply Palantir has embedded itself in government operations, to the point where agencies formally declare they cannot function without its proprietary platforms. In September 2025, when the Department of Homeland Security awarded Palantir a $30 million task order to create the ImmigrationOS platform for ICE—described in greater detail in the next section of this report—it issued a limited-source justification asserting that Palantir is the "sole source capable of providing the necessary supplies and services."[250] The justification argued that Palantir's existing Investigative Case Management (ICM) system made any alternative vendor incapable of delivering the required capabilities without delays. ICE further warned that switching vendors would disrupt ongoing investigations and potentially "compromise national security," citing Palantir's decade of accumulated institutional knowledge as irreplaceable.[251]

Figure 9 *Contract money awarded to Palantir by ICE*

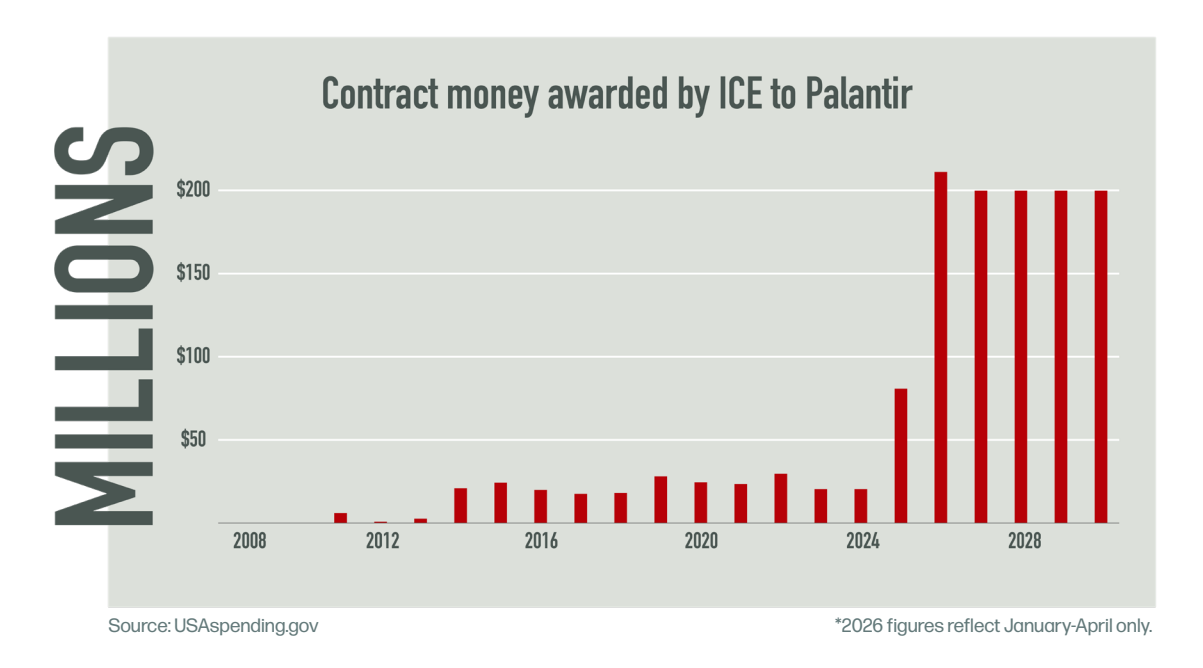
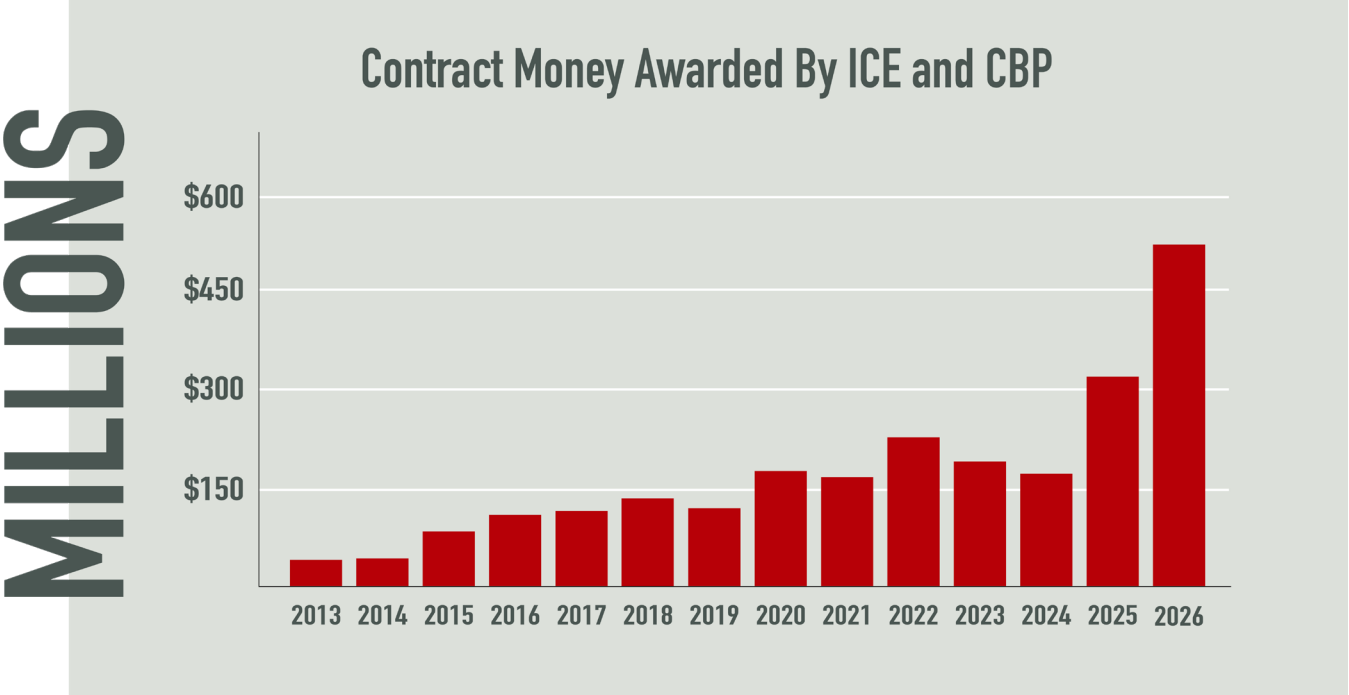


Figure 10 Contract money awarded to surveillance tech by ICE and CBP[252]



Awards granted to Peraton, LexisNexis, Cellebrite, Msab Group, Pen-Link, Thomson Reuters, RELX, Clearview AI, BI² Technologies, Palantir Technologies and Anduril Industries. The 2026 bar reflects January-April only. Source: USAspending.gov.

Figure 10 depicts our analysis of publicly available federal contracts information. We tracked ICE and CBP contracts with 11 surveillance tech companies—Peraton, LexisNexis, Cellebrite, Msab Group, Pen-Link, Thomson Reuters, RELX, Clearview AI, BI² Technologies, Palantir Technologies and Anduril Industries—from January 2013 through April 2026. The analysis in Figure 10 shows a doubling in total contract growth awarded to surveillance tech companies by ICE and CBP in 2025, followed by even more shocking growth in the first third of 2026. Awards in just the *first four months* of 2026 already surpassed total contract money in all of the previous year by 65%. This growth in 2025 and 2026 was driven primarily by massive new contracts growth for Palantir for ICE's data analytics and people-tracking apps and Anduril, for autonomous border towers, drones, sensors, and related AI surveillance systems for CBP.[211]

The federal government's partnership with tech venture capital firms has funneled federal contracts to tech and AI companies, further aligning Silicon Valley with the administration's national security and homeland security agenda.

The DHS Sandbox

DHS does not simply purchase technologies once they have been developed, they have a billion-dollar incubator for surveillance startups. Through a network of funding programs, partnerships, and research initiatives, it actively helps shape the innovation ecosystem that produces the surveillance and enforcement technologies it seeks to deploy. Together, these programs function as a "sandbox," allowing DHS to identify, fund, test, and refine technologies that are directly responsive to its operational priorities.

Over the last two decades, DHS has partnered with domestic and international government agencies to foster a pipeline of technology developed in Silicon Valley by supporting key startups in the surveillance ecosystem. Some of these companies have become major DHS and Pentagon contractors,

including Palantir, Skydio, Anduril, Scale AI, Shield AI, and Databricks, all of which received equity funding or contract money from at least one of various programs housed in or partnered with the DHS Science and Technology Directorate (S&T).[212]

S&T is a department within DHS that answers directly to the Secretary. It houses several divisions, including an Office of Science and Engineering, focused on technology research, standards, testing and evaluation, and an Office of Innovation and Collaboration, focused on external partnerships with foreign governments, universities, and private industry. Industry partnerships are formalized under the umbrella of the Office of Industry Partnerships (OIP), which houses the programs and partnerships through which DHS supports new technology startups in the private sector.

The DHS OIP currently oversees seven innovation funding programs, some of which are not housed within DHS but maintain formal partnerships with the agency. Taken together, these programs function as the "sandbox" for innovation and development that is directly responsive to DHS's technology needs, including surveillance.[213]

Three of these programs have been the most consequential in terms of providing early funding for companies that go on to be major surveillance technology providers:

- Silicon Valley Innovation Partnership (SVIP) provides up to $2 million to startups for prototyping. It has funded more than 60 companies working on projects for DHS such as airport passenger processing and drones.[214]
- The DHS component of the Small Business Innovation Research (SBIR), has provided awards totaling $845 million to over 500 companies since 2004.[215] The term "small business" should be taken with a grain of salt, as Anduril Industries, for example, received SBIR money in 2020, when the company was valued at around $2 billion.[216] SBIR is not hosted within DHS and also works across other federal agencies.



- In-Q-Tel (IQT), a now independent, non-profit strategic investment firm, is perhaps the most consequential. With formal partnerships with DHS and other federal agencies through the IQT Interface Center, IQT provides equity funding, has invested in over 800 companies and currently holds approximately $1 billion in assets. Its growth reflects successful venture exits but also the impact of public funding, having received $114 million in government grants in 2025 alone.[217] IQT has built a very large portfolio of AI startups, in particular, accounting for 148 investments.[218] S&T joined the IQT model as a full member in 2009.

It is important to note that startups can be funded by one federal agency but end up working for another. For example, Anduril received SBIR funding from the Air Force but has been awarded close to $1 billion from CBP for border surveillance towers and related systems[219] (and, in March 2026, a $20 billion enterprise contract from the Army).[220] Palantir, meanwhile, never received DHS funds but relied on seed funding from the CIA's IQT at a time when VC firms in Silicon Valley had not expressed interest in the company.[221]

While DHS innovation funding is not often enough to launch a company to success, small amounts of early funding can prove to be decisive in attracting serious venture capital funding, as was the case with Palantir. Some of the most invasive surveillance technology being funded by DHS SBIR is now going to very small companies that have not yet received large amounts of VC money.

DHS documents leaked in March 2026 to *The Guardian* reveal a list of more than 6,800 companies that have applied for SBIR with DHS, as well as data on more than 1,400 awarded contracts.

These included money awarded during the second Trump administration for technology such as:

- Tools enabling agents to harvest biometric data using cellphones;[222]
- AI to analyze existing airport CCTV feeds and automatically catalog passengers' physical characteristics;[223] and
- AI platforms that would ingest 911 call data, with one promising to identify and predict crime patterns with heat maps.[224]

Artificial Intelligence in DHS

The scale and speed of investment in AI marks a significant shift from just eight years ago, when "*Who's Behind ICE?*" found little evidence of AI being used in DHS technologies. Since then, AI has taken center stage. It now extends into our everyday lives—from getting a life insurance plan, getting electricity, to getting a green card.

Inside the federal government, Congress has passed several laws aimed at advancing US leadership in artificial intelligence, including the implementation of AI across federal agencies.[225] Vendors providing ICE and CBP with AI applications include Anthropic, Palantir, Anduril, Microsoft, Dataminr, Clearview AI, and many others. DHS use of AI now covers areas including generative AI, computer vision, natural language processing, machine learning, and agentic AI. These procurement expenses are part of an IT budget at DHS that amounted to more than $10 billion in 2025.[226] The White House Fiscal 2027 budget shows DHS will hold the third highest IT investment in the federal government—$11.7 billion, which includes AI. The Department of Defense holds the highest investment in AI, seeking $58.5 billion for "continued American dominance in AI-enabled warfare."[227]

DHS has fast-tracked AI adoption since 2019, primarily through executive orders from the Biden and Trump administrations.[228] In 2022, DHS published its first AI inventory of AI technologies that are utilized by DHS employees.[229] At that time, only 20 AI uses were identified across ICE, CBP, and other DHS components, even though DHS claimed it had been using them for years.[230]

Just three years later, DHS identified 238 uses, with over half held by CBP and ICE.[231] Most of these technologies were aimed at accelerating immigration enforcement through invasive surveillance. Over 60 uses remain on an internal inventory which has not been disclosed to the public.[232] DHS has not yet offered reasons as to why it elected to withhold so many uses from the public inventory. Moreover, recent releases from a 2024 Freedom of Information lawsuit on the DHS AI inventory show DHS's process for conditionally approving multiple facial recognition tools despite concerns over adequate testing.[233]

Just three years later, DHS identified 238 uses, with over half held by CBP and ICE. Most of these technologies were aimed at accelerating immigration enforcement through invasive surveillance.

As a result, the rapid expansion of AI within DHS has not been matched by equally robust systems of oversight and accountability. Over the last several years, civil society has investigated these technologies and raised concerns about violations of privacy, personal data misuse, discrimination, bias, and accountability.[234] For example, the report "Automating Deportation" lays out key problems with DHS use of AI, including that artificial intelligence runs the risk of perpetuating and worsening bias and discrimination.[235] The persistence of these concerns reflects a deeper problem: the absence of meaningful oversight over DHS's growing use of AI over various administrations.

A key flaw of the framework created by the Biden administration was that it relied on self-policing to identify and eliminate abuse, bias and discrimination against immigrants, their communities, and millions of others impacted by DHS. In a 2025 report, the DHS Office of the Inspector General (DHS OIG), DHS's independent oversight body, noted the Biden administration's failure to enact "adequate governance processes to monitor the department's AI for compliance with privacy and civil rights and civil liberty requirements."[236] Among other oversight problems, the report also flagged DHS's failure to disclose the full inventory. It concluded that "without appropriate, ongoing governance of its AI, DHS faces an increased risk that its AI efforts will infringe upon the safety and rights of the American people."

Concerns about oversight and accountability identified by DHS OIG in the Biden administration have become even more pronounced as the Trump administration moves to rapidly expand the use of artificial intelligence across federal agencies.[237] Recent GAO findings highlight privacy risks, including exposure of private information. These concerns are compounded by the lack of sufficient resources and comprehensive systems for the agencies to ensure privacy protections.[238] Despite these unresolved concerns, DHS is exploring new advances in AI, including "agentic AI, "[239] a type of AI that can make decisions with minimal human interaction, shifting more decision-making into algorithms that will be less available to the public view.

Current DHS leadership is also invested in heavily expanding DHS use of AI. DHS Chief Information Officer (CIO) Antoine McCord, a former Anduril employee, will oversee the spending of DHS's vast IT budget.[240] In September 2025, McCord released the DHS AI strategy for the next three years, which included features like "continuous authorization of IT systems," replacing "traditional fixed authorization deadlines."[241] Presumably, this means that companies with federal contracts will face fewer procurement requirements. McCord will also be overseeing the Office of Biometric Identity Management,[242] the largest biometric database in the US government, integral to DHS operations. OBIM's significance is explained in the next section, relating to a core DHS data analytics system, the Homeland Advanced Recognition Technology (HART).

This report has outlined the centrality of DHS and its immigration policing project to the security state. It also outlined how the militarized policing and surveillance activities of DHS have been supercharged under the current Trump administration through powerful alliances with tech firms that provide AI and surveillance for national security and homeland security agencies. The dramatic increase of funding for ICE and CBP has been channeled into a larger immigration police force, but also into significant spending increases on surveillance technologies. In the next section, we will examine the technologies that DHS, ICE, and CBP are purchasing and using in militarized immigration policing.

5. Tools of the Surveillance State

ICE and CBP are immigration policing agencies, but they are the primary drivers of the new DHS militarized police state, empowered by increasingly AI-driven surveillance technology. This technological apparatus is designed for the targeting of individuals based on race, ethnicity, and perceived immigration status, but it is also, by its very nature, a surveillance dragnet capable of tracking the population at large—and that is just what it is doing.

DHS's surveillance apparatus also enables increased retaliation and persecution of anyone labeled an opponent of the government, citizens and noncitizens alike. Because surveillance technologies are often unregulated at the state and federal level, they operate without oversight and are deployed without knowledge or consent. Many of these technologies can be used to criminalize First Amendment-protected activity by targeting people for their beliefs, speech, or associations.[253] Individuals can lose anonymity and privacy, sometimes through misidentification by these tracking technologies, or because of their political views. Companies behind these technologies often evade responsibility for human rights transgressions, as many of them operate worldwide and are often not responsive to concerns about human rights violations.[254]

There are several key components to the DHS surveillance dragnet through which virtually everyone residing in the United States moves, both physically and virtually, on a daily basis. Sometimes this surveillance is clearly perceptible, such as when passport scanners and facial recognition pods register travelers' movements through airports, or when ICE agents use the Mobile Fortify app to scan and search biometric characteristics in real time after detaining and questioning people in the streets of our cities. Other times, mass surveillance is not as perceptible, such as when automated license plate readers (ALPRs) snap a constant stream of photos so that every car's movement may be traced by local police, ICE, and any other law enforcement agency. And there are types of surveillance that we cannot see DHS gathering, such as when it is conducting mass social-media surveillance or purchasing all available commercial and government data from data brokers on virtually every US resident.

As described earlier, AI is increasingly central to the DHS surveillance apparatus. AI systems are now accelerating the scale and speed of surveillance by allowing DHS agencies and private contractors to process massive quantities of data in ways that would have previously required thousands of human analysts, often with no public transparency, meaningful oversight, or clear regulation governing how these systems are deployed and used.

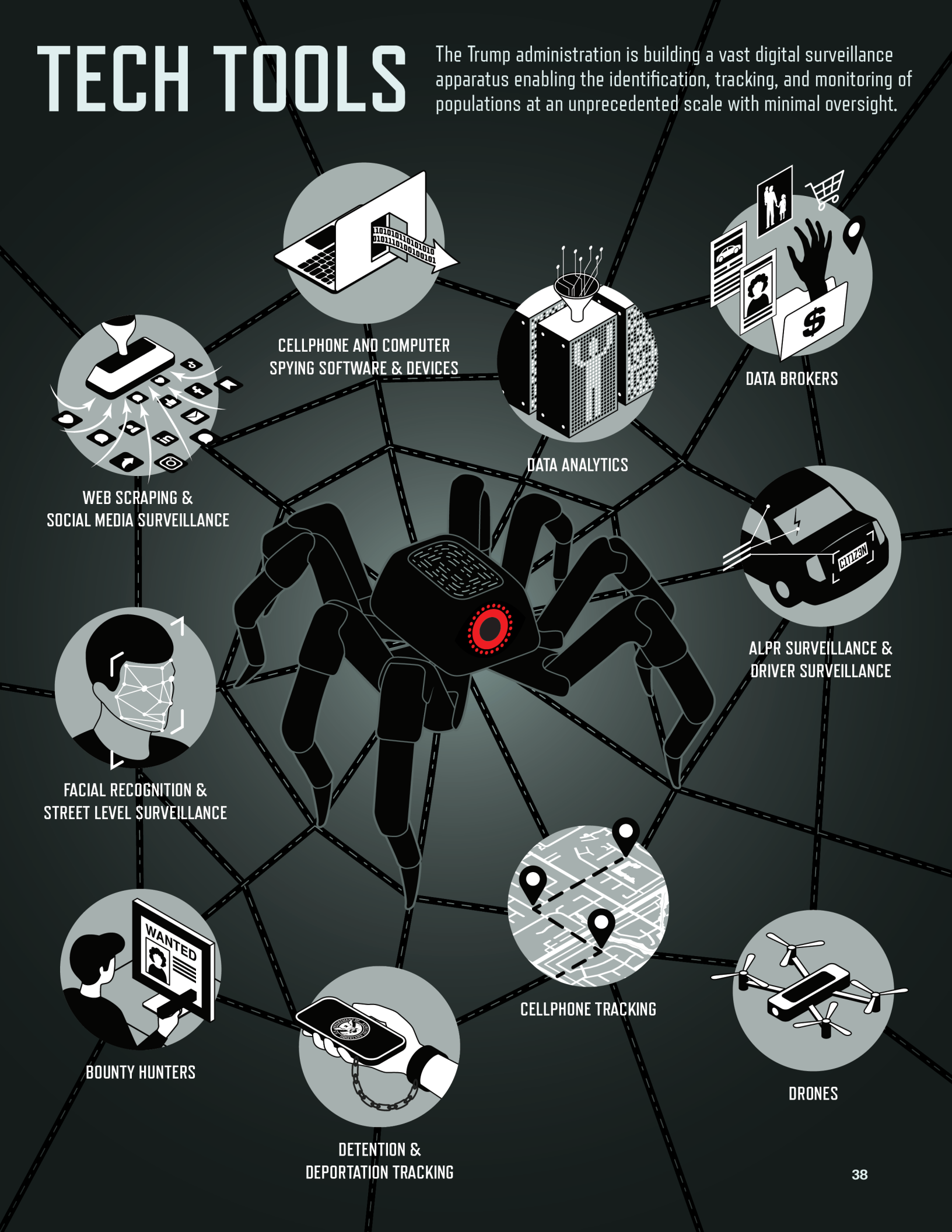
The first step in resisting the militarized policing and supercharged surveillance state in this authoritarian moment is to understand what technologies are involved. Below, we outline the kinds of surveillance technologies that DHS is employing, and some of the tech that is critical to understand. track, and monitor.

It is important to note that although this inventory is based on the best information we can get, it is not complete. ICE and CBP do not provide transparent, consistent or accurate information about their contracts or how the technology is being used.

AI systems are now accelerating the scale and speed of surveillance by allowing DHS agencies and private contractors to process massive quantities of data in ways that would have previously required thousands of human analysts, often with no public transparency, meaningful oversight, or clear regulation governing how these systems are deployed and used.

TECH TOOLS

The Trump administration is building a vast digital surveillance apparatus enabling the identification, tracking, and monitoring of populations at an unprecedented scale with minimal oversight.



1. Data Brokers



What are data brokers?

Data brokers are companies who buy, sell. or share personal and commercial data of all kinds—from location tracking to facial recognition to billing addresses to car registration data—without a warrant, consent, or notice.[255] In the US, only a handful of limited federal and state laws constrain the business model of data brokers.[256]

DHS combines information from data brokers with data shared by the DEA, FBI, IRS, and some state and local governments to target noncitizens.[257] Departments of motor vehicle associations also share or sell driving record data, car title, and registration information, and in some cases most recent address, name, or license plate number.[258] This kind of highly sensitive and personal information ends up in the hands of data brokers, and ultimately with ICE and CBP who might end up purchasing this information through a subscription to a databroker, like LexisNexis's Accurint platform. Even if a corporation does not hold a contract directly with DHS, they can serve as conduits for data sharing. For example, ALPR company Flock Safety was found to be a conduit for informal data sharing between local law enforcement and ICE in 2025.[259] By connecting various data points acquired by data brokers, DHS targets people for surveillance, deportation and arrests. The data broker market overall is pegged at $250-330 billion, meaning that databroker companies make huge profits selling data to DHS.[260]

Key DHS data brokers

LexisNexis Accurint and Thomson Reuters CLEAR are two of the most wide-reaching data brokerage platforms. Both companies started off as purveyors and distributors of legal tools and earned media, but now have AI-enabled functions to access vast repositories of public records, license plate readers, court and arrest information, credit histories, utility bills, and property data. They sell access to government agencies for everything from background checks to investigative targeting, allowing DHS to make connections among disparate records across databases. These connections turn into comprehensive profiles of people, their families, and their "associates" such as employers or schools.

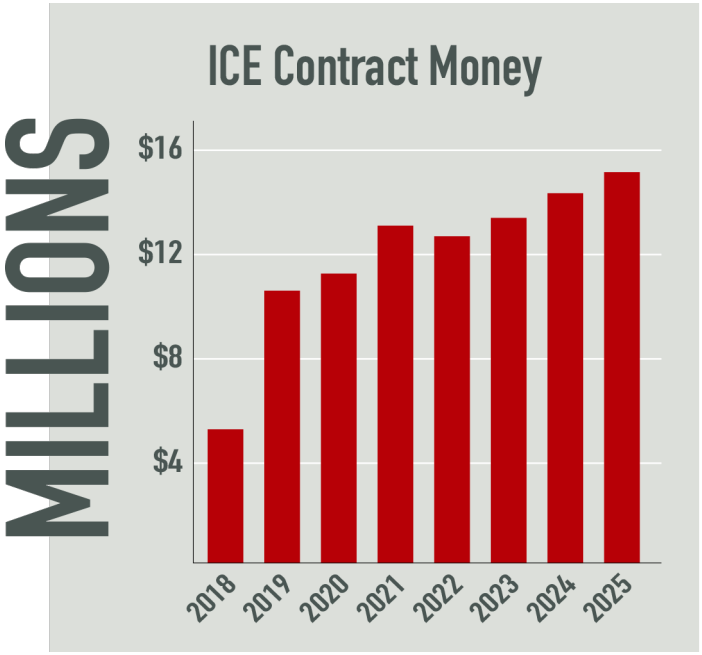
DHS contracts with data brokers

ICE has paid for both CLEAR and Accurint over the years but adopted LexisNexis as its principal data broker in 2021. ICE also awarded a contract to Thomson Reuters in 2021 for a nationwide ALPR database from Vigilant Solutions (since acquired by Motorola Solutions).[261] Moreover, LexisNexis Accurint and Thomson Reuter CLEAR have also historically granted ICE access to Equifax's databases, one of the three largest credit companies in the United States.[262]

Accurint by LexisNexis

ICE holds a contract with LexisNexis (a subdivision of RELX, Inc) for the company's Accurint platform. Accurint connects 37 billion individual records from over 10,000 sources to provide ICE agents with up-to-date phone numbers, addresses, vehicle information, property records, social networking information, license plate reader information, business records, criminal records, bankruptcy data, and more.[263] This includes 290 million people in the United States, covering over 95% of the adult population.[264] Documents provided by ICE in response to a FOIA submitted by Just Futures Law show that ICE agents made quick use of the Accurint platform upon signing a contract in 2021, conducting over 1.2 million searches in just a seven-month period in that year.[265] ICE maintains a $23.3 million agreement

Figure 11 *Annual ICE contract money to key data brokers (2018–2025)*[278]



USAspending.gov.

with LexisNexis for Accurint, active through May 2026,[266] as well as an $8.9 million contract for "risk mitigation services"[267] (It is expected that ICE will renew their contract with LexisNexis). In 2022, CBP followed ICE's lead by signing a $25.7 million contract with LexisNexis through November 2027.[268]

Thomson Reuters CLEAR

Thomson Reuters previously served as ICE's primary data broker before that function was awarded to LexisNexis in 2021. Thomson Reuters now maintains a $22.8 million contract for ALPR services,[269] which by 2019 had already been shown to be used for widespread information sharing between ICE and local law enforcement.[270] Thomson Reuters also provides a "maritime analysis tool and subject matter expert support services" to ICE for $3.8 million,[271] as well as $4.6 million for "risk mitigation services."[272] This tool is purportedly to protect ICE agents from threats, but one Thomson Reuters institutional investor has noted it serves to "track social media accounts to target immigration activists."[273]

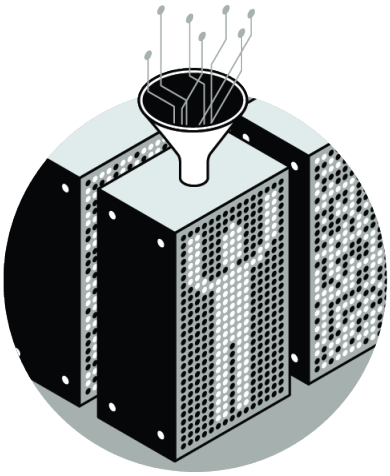
Equifax

Equifax, best known as one of the three major US consumer credit reporting agencies, has quietly become a critical part of ICE's surveillance infrastructure—not only through its credit reporting products, but also through its ownership of Appriss Insights, a company that operates the Justice Intelligence database. Justice Intelligence provides ICE with real-time jail booking and release information from over 2,800 jails and correctional facilities across the US, updating "as frequently as every 15 minutes."[274] This data is particularly valuable for ICE's Enforcement and Removal Operations (ERO), which orchestrates detention and deportation. The Justice Intelligence database allows the agency to locate and apprehend individuals immediately upon their release from local custody—even when those jails refuse to honor ICE detainers or when state sanctuary policies prohibit direct cooperation with federal immigration authorities.[275] Equifax also holds a direct contract for "support services" with ICE's Homeland Security Investigations (HSI).[276]

As seen in **Figure 11**, ICE's financial commitments to commercial data brokers have grown steadily over recent years, reflecting the agency's deepening reliance on private-sector data sources to fuel its enforcement operations. Total obligations to a core group of companies—including LexisNexis (RELX), Equifax, and Thomson Reuters[277]—rose from $4.9 million in 2018 to $14.5 million in 2025. While the three companies listed above account for the largest share of these obligations, the broader ecosystem includes additional data brokers and resellers whose contracts are often bundled into third-party agreements and therefore harder to track.

Equifax, best known as one of the three major US consumer credit reporting agencies, has quietly become a critical part of ICE's surveillance infrastructure.

2. Data Analytics and Data Bases



What are DHS data analytics companies?

Data analytics companies examine and analyze data from data brokers or other sources to find patterns and trends that enable DHS agents to deport and detain on a mass scale. These companies range from small analytics companies to billion-dollar companies, like Palantir, with a wide range of "platforms" and services. DHS also uses multiple systems to mine and analyze its own data that it collects from applications and from commercial sources. Usually, big tech companies help them build these systems.

DHS data analytics platforms:

RAVEn (Repository for Analytics in a Virtualized Environment)

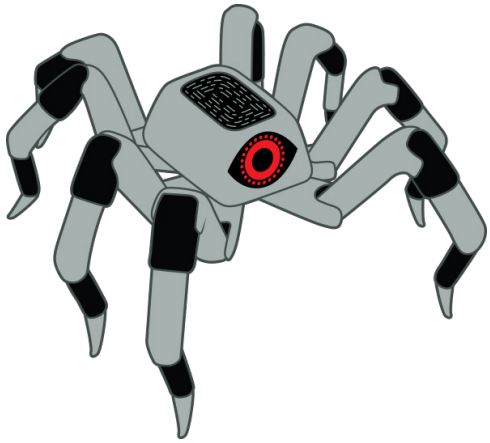
RAVEn is a "big data" platform[279] that performs analytics using artificial intelligence on massive raw datasets, allowing ICE to make sense of information in order to identify targets as well as predict patterns and connections between people and events.[280] RAVEn was designed by Booz Allen Hamilton, Inc., a government contractor that specializes in AI and digital transformation. Unlike its predecessor FALCON—which was a customized version of Palantir's Gotham software[281]—RAVEn was built from the ground up specifically for ICE's HSI division with the stated goal of replacing the older system. The platform ingests data from tens of thousands of sources—including surveillance footage, biometric data, social media, location information from commercial providers, and license plate reader databases—making it searchable, shareable between agents, and graphable by values like time and place.[282] The contracts to build and maintain the system were highly competitive, drawing interest from Amazon, Google, and Microsoft, and ultimately valued at up to $300 million over five years. Booz Allen Hamilton secured the initial development contract in 2018, followed by a $67.8 million data analytics support contract in 2021 that extends to September 2026.[283] RAVEn has already processed hundreds of thousands of immigration documents and workplace audits, and its facial recognition capabilities allow ICE agents to submit images from mugshots, surveillance photos, and confiscated devices to be matched against driver's license records and other government databases—all without notifying the individuals whose information is stored.[284]

HART: The Homeland Advanced Recognition Technology System

The Homeland Advanced Recognition Technology System[285] (HART) is a massive biometric repository that will house over 300 million profiles of faces, fingerprints, and irises[286] within a modern Amazon cloud-based platform capable of processing queries from across the federal government and partnering nations.[287] Originally projected to cost $5.8 billion in 2016, the HART system has seen ongoing cost overruns and problems getting sufficient funding,[288] facing intense scrutiny over privacy and technical challenges.[289] HART is designed to modernize the IDENT database, managed by the Office of Biometric Identity Management (OBIM), which is in charge of storing, sorting, and analyzing data such as facial images, fingerprints, and iris scans. In February 2026, the DHS Inspector General launched an audit of DHS privacy practices, focused on ICE and OBIM, to determine if "data is managed, shared, and secured in accordance with law, regulation, and Departmental policy," amid allegations of broad civil liberties violations.[290]

The primary contractor for the HART database is Peraton, owned by private equity firm Veritas Capital.[291] The company adopted the HART system when it purchased defense contractor Northrop Grumman's government IT business in 2021.[292] Private equity buyouts are a cyclical business in which portfolio companies such as Peraton are purchased and subjected to cost-cutting and profit maximization measures before being resold or stripped for parts, generally on a timeline of approximately 10 years.[293] Having been purchased in 2017 by Veritas, Peraton could soon be sold for a profit.[294] There is no way to predict exactly what will become of HART in the coming years, but as a private equity portfolio holding, the company is being managed with a profit-maximization mandate for investors on an accelerated timeline.

After years of delays, DHS is projecting that HART will reach initial operating capacity in FY2026, according to 2027 budget projections.[295] However, the White House Homeland Security Council under the second Trump administration is transitioning the management of HART from OBIM to the DHS Chief Information Officer, Antoine McCord,[296] who was appointed to the role directly from his job as an Anduril executive.[297] Elon Musk's short-lived Department of Government Efficiency (DOGE) was reportedly consulted on the program's future.[298] Stephen Miller, the chief architect of most immigration enforcement policies under the Trump Administration, was reportedly responsible for the reevaluation of biometric systems at DHS,[299] including conversations about consolidating control of DHS biometric systems at CBP, as part of a strategy to align biometric capabilities with the immigration enforcement priorities of the Trump administration.[300]



3. Web Scraping and Social Media Surveillance



What are "web scraping" and social media surveillance?

Companies that automatically extract data (information, location, face scans, etc) from websites are involved in "web scraping." These same companies also "scrape" social media profiles for name, pictures, statements, likes/dislikes, etc.

These technologies work behind the scenes, often without our knowledge, consent or a warrant. The administration has supercharged the surveillance of social media and web activity, deploying a suite of AI-powered commercial tools to build profiles and flag individuals for deportation, arrests, detention, or consular processing denials. Many of these companies use AI-enabled software that were previously flagged by the Biden administration for not being in compliance with DHS AI guidance on civil rights impacts, inaccuracies and errors.[301]

DHS web scraping and social media surveillance tools

Zignal

The agency has spent $5.7 million on Zignal licenses, an AI-powered platform that analyzes billions of daily social media posts.[302] ICE reportedly uses Zignal to identify and locate individuals for arrest and deportation based on

(Continued on page 44)

Palantir is one of the largest data analytics companies in the world. It makes several data analytics systems that serve as key infrastructure for ICE and CBP operations.

Investigative Case Management

Palantir's Investigative Case Management System (ICM) is the primary software backbone for ICE's HSI, allowing agents to create, track, and manage criminal case files, evidence, and intelligence across a broad range of activities. The system has long been the "core law enforcement case management tool" used by HSI. ERO also uses the system to manage immigration cases presented for criminal prosecution and queries ICM for information that may support its civil immigration enforcement cases. ICM also plays a key role in information sharing with law enforcement, as it connects to the FBI's National Crime Information Center (NCIC) and Nlets, a state-owned network for information sharing with law enforcement agencies, among other databases.[303] Palantir was first awarded a contract to develop ICM in 2014.[304] The latest iteration of the ICM contract, signed in 2021, is now worth up to $176.5 million after an injection of more than $86 million between April 2025 and March 2026.[305]

ImmigrationOS

Notably, much of the new money awarded by the Trump administration for the ICM contract is in fact dedicated to the development of a separate system, called ImmigrationOS, for ERO—despite being funded through the existing HSI contract on a non-competitive basis.[306] In other words, rather than awarding a competitive contract for the new tool via ERO—which deals with civil immigration enforcement—the administration awarded new federal money on a non-competitive basis using a contract vehicle originally granted for purposes of criminal investigation. According to contract documents, the AI-enabled ImmigrationOS system serves three main functions: streamlining the identification and apprehension of removal priorities, accurately tracking self-deportations with real-time data, and improving deportation logistics.[307]

This tool fuses data from across government datasets—including Social Security files, IRS tax data, and ALPR information—to create comprehensive, AI-driven profiles for enforcement decisions.[308] ImmigrationOS, allows "near real-time visibility" into the movement of migrants in the US.[309] The platform identifies undocumented migrants and "targeted populations," aggregating information from border entries to home addresses, social media activity, and many other personal data points obtained from commercial and government sources.[310] It enables an opaque "deportation by algorithm" system, playing a significant role in the Trump administration's ramp up on family separations, as well as the erosion of due process and asylum processes.[311]

Palantir's ELITE

In January 2026, *404 Media* uncovered the widespread use of a new tool called ELITE, developed under ICE's same Palantir contract, that uses generative AI to extract addresses from government records—including Department of Health and Human Services data. ELITE populates a map with potential deportation targets, brings up a dossier on each person, and provides a "confidence score" on the person's current address.[312] *404 Media* reported that "ICE is using it to find locations where lots of people it might detain could be based," helping agents identify neighborhoods for enforcement raids.[313] DHS has classified high-impact tools like ELITE in its AI inventory as "presumed high-impact but determined not high-impact," arguing that outputs "do not serve as a principal basis for decisions or actions with legal, material, binding, or significant effects on individuals"[314]—a determination that strains credulity given that the tool helps decide which neighborhoods to raid A user guide on ELITE published in part by 404 Media shows how agents get a dossier that includes everything from Unique IDs to "encounter" information.[315]

their expressed views or associations by generating "curated detection feeds" and identifying "threats" from vast quantities of social media data.[316] After moving into the defense and intelligence sectors in 2021 with a Public Sector Advisory Board filled with "top national security experts," the firm has aggressively expanded its footprint across the US government and allied militaries, securing contracts with the Pentagon, the Israeli military, and the State Department before winning its first-ever contract with ICE in 2025. Recently, the company advertised its work with the Israeli military, saying it has provided "tactical intelligence" to "operators on the ground" in Gaza,[317] underscoring its role in both domestic enforcement and global military operations.

ShadowDragon

Similarly, ICE has acquired ShadowDragon licenses,[318] a powerful monitoring tool that has been used by ICE since 2020. ShadowDragon allows analysts to pull a target individual's publicly available data from over 200 websites, social networks, apps, and services simultaneously including mainstream platforms like Facebook,Instagram, other Meta-owned services, as well as Bluesky and OnlyFans. This enables agents to map out a person's activity, movements, and relationships across the web at once, and the tool can even access deleted or historical posts.[319]

Babel Street

Babel Street is a social media monitoring company that allows CBP to search a name, email address, or telephone number and review associated social media posts, IP address, employment histories, and other information.[320] While the company has not held an identifiable contract with CBP since the end of 2024,[321] the 2025 DHS AI Use Case Inventory lists Babel Street as a "high impact" AI tool used by the agency "to conduct targeted queries to aid CBP in open source research to monitor potential threats or dangers or identify travelers who may be subject to further inspection." Specifically, it uses AI for "text detection and translation as well as object and image recognition to provide analysts with possible matches."[322] Another of the company's products, known as Locate X, reportedly allows ICE to monitor and identify cell phones at specific locations, using mobile application data.[323] ICE has an active contract for Babel Street subscription services through a third-party contractor.[324]

Fivecast Onyx

Complementing these other tools, CBP has secured at least six new licenses for Fivecast ONYX.[325] Fivecast can be used to target individuals or events and collect data from mainstream platforms like Facebook and Reddit, as well as fringe communities like 4chan and Gab. The company boasts a "full collection capability"[326] that gathers all available content from a target's social media account and maps their network of connections. Crucially, Fivecast uses AI to detect "sentiment and emotion" in online posts and can be trained to recognize specific concepts or objects in images.[327]

NexusXplore

Beyond monitoring public-facing social media, federal agencies (including DHS and DOD) construct comprehensive dossiers on people by scraping a far wider range of internet activity,

BableStreet (Babel X) is a technology-enabled platform accessed through an internet-based user interface that supports targeting, vetting and screening efforts. Babel Street enables multi-lingual, geo-enabled searches, offers text analytics, and provides access to information maintained on the surface, deep, and dark webs. Babel Street has been part of the OSINT technology stack for more than five years. Information such as social media profiles accessed through the Babel Street platform is often dated, requiring additional research to verify fidelity. Babel enables advanced search, collection, and analysis of publicly available information through a single user interface, facilitating the collection of information regarding people, places, and things across social media platforms, as well as general information held on the surface, deep, and dark web to inform situational awareness and to support CBP law enforcement and national security operations.
Fivecast is a technology-enabled platform accessed through an internet-based user interface that provides insight into a variety of social media platforms including, but not limited to, Facebook, Instagram, Telegram, and Twitter. Fivecast analyzes the strength of connections between social media users, and collects both media and activity information from targeted profiles. Fivecast enables the identification of usernames and profiles through the use of individual names, telephone numbers, age, email address, and location. Fivecast has proven to be one of the most valuable tools in the OSINT technology stack; however, recent programming changes executed by Meta have resulted in a diminished capability on the part of Fivecast to rapidly and fully collect information of interest. Fivecast enables advanced search, collection, and analysis of publicly available information through a single user interface, facilitating the collection of information regarding people, places, and things across social media platforms, as well as general information held on the surface, deep, and dark web to inform situational awareness and to support CBP law enforcement and national security operations.

Excerpt from DHS AI Freedom of Information Act litigation[339]

capturing the digital exhaust of everyday life. NexusXplore is a platform that claims to provide access to over 8 billion public records. According to the DHS AI Use Case Inventory, the tool uses AI modules for text detection, translation, and image recognition to help analysts find possible matches across open-source and social media data in a single interface, potentially identifying unknown phone numbers and emails linked to a target.[328] The tool's official description on its website reveals it functions as a comprehensive search engine that aggregates and correlates data from hundreds of sources, including social media, people search sites, court records, and deep web archives, effectively creating a detailed digital dossier from publicly available information.[329]

RECON

Another web scraping tool is Team Cymru's "Augury" software,[330] also known as RECON, previously used by the US military to track internet usage. The tool provides visibility into over 90% of global internet traffic and is reportedly updated with at least 100 billion new records each day.[331] By tapping into data from internet service providers, it can potentially capture not just browsing data, but the contents of emails, file transfers, and other communications, effectively creating a detailed record of a person's private online life without a warrant.[332] The tool was acquired by ICE in September 2025.[333]

Tangles

Also in September 2025, ICE acquired another sophisticated tool to scrape and analyze data from the deepest corners of the web: PenLink's Tangles tool.[334] Tangles was originally developed by Cobwebs Technologies, an Israeli firm founded by former members of Israeli military special units, before being acquired by PenLink in 2023.[335] It is an AI-powered platform that automatically scrapes the open, deep, and dark web to construct comprehensive dossiers. It links social media activity, contact information, financial records, and geolocation data to build a complete picture of a target and their network.[336] Complementing this is PenLink's PLX, a tool for the live interception of communications, also acquired by the agency in September 2025. As outlined in a PenLink privacy impact assessment, PLX can collect and analyze data from a vast array of sources, including direct connections to telecommunications data, social media, and messaging services, providing real-time insights into a target's communications.[337] As has been seen before, the integration of these companies into the state apparatus is reinforced by a constant revolving door: in June 2025, PenLink appointed Derek Maltz, a former Acting Administrator of the DEA, to lead its global business growth and strategy,[338] ensuring the company's tools are strategically positioned for federal adoption.

4. Facial Recognition and Street-Level Biometric Surveillance



What is facial recognition and street-level biometric surveillance?

DNA, fingerprints, facial features and irises are considered unique to the individual and contain identifying information. Described as "biometrics," they include body measurements that are used to identify individuals, such as facial scans or iris scans. DNA is acquired through parts of the body—such as blood or hair—and has been used by DHS to establish family relationships. As described above, DHS contains massive repositories of biometric and biographic data upon which they run data analytics.

Face capture and face recognition technologies (FC/FR) involve technologies that detect a face in

a video or image and/or match it against a library of faces. Face recognition technologies compare captured faces against a database to identify or verify the individual. These technologies capture faces in many ways: scraping them from the internet or social media, through street cameras, airports, or data brokers. These technologies operate as street-level surveillance—that is, they acquire biometric and biographic information from people as they go about their daily lives. Advocates and federal oversight agencies have raised concerns over DHS's use of FC/FR technologies and iris scanning technologies.[340]

DHS holds a number of contracts with facial recognition companies. FC/FR technologies account for over 25 different AI use cases at DHS, with 22 held by ICE and CBP.[341] Nearly half FC/FR AI use cases are related to CBP's Traveler Verification Service (TVS), a program that operationalizes biometric collection for individuals entering and leaving the United States by land, air, and sea.

Other AI use cases for FC/FR at DHS have to do with immigration enforcement, such as the Clearview AI and Mobile Fortify tools, detailed below. These newer tools, some of which are used by ICE and CBP and focused on street surveillance, are just part of an emerging slate of experimental new FC/FR tech. DHS's FY2027 budget requests $16 million for Biometrics and Identity Management, $6 million for Biometric Emerging Concepts, and $10 million for Biometrics and Identity Screening for the Border Security and Immigration section of its Science & Technology Directorate. Perhaps most alarmingly, DHS requested funding in FY2027 to develop an operational prototype of "smart glasses" designed to allow "biometric identification of illegal aliens."[342]

Multiple oversight agencies, like the Government Accountability Office (GAO) and civil rights groups have raised concerns with FC/FR focusing on privacy violations, misuse in sharing of photos, and errors.[343] FC/FR technologies allow DHS to not only identify people in public spaces, but also to learn those people's professional roles, religious affiliations, familial connections and friendships, romantic partnerships, personal activities, political views, patterns of travel, and even home addresses, *all without receiving consent, obtaining a warrant, or providing probable cause to conduct a search.* In the last year, ICE has "played a leading role, helping build a large facial recognition database that DHS can use to identify not only people targeted in immigration raids, but also protestors and legal observers."[344]

DHS facial recognition and iris scanning companies:

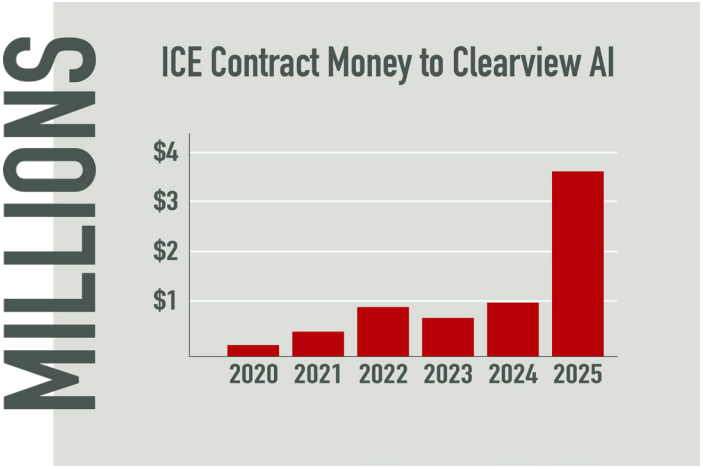
Clearview AI

Clearview AI is just one of several facial recognition products and platforms used by DHS, managed by the department's Office of Biometric Management (OBIM).[345] It is not surprising that Clearview AI, which emerged from Peter Thiel's venture portfolio and is also uniquely invasive, is seeing a dramatic increase in ICE and CBP contract money.

Clearview AI has built the most dangerous facial recognition database in the country. Clearview AI has allowed law enforcement and government agencies to identify, locate, and track people—where they go, who they're with, and what they say—at the touch of a button. The backbone of this powerful technology relies on a vast database of photo images and biometric information illicitly collected by scraping websites and social media. Clearview AI was founded in 2017 and received early funding from Peter Thiel and his Palantir co-founder Joe Lonsdale's 8VC. The platform purports to have over 70 billion photos[346] and includes images "scraped" without consent from websites like Facebook, Instagram, Twitter, LinkedIn, and Venmo. [347]

The company has generated massive public controversy and was sent cease-and-desist letters from Google, Facebook, and Twitter, as well as attracting lawsuits from the State of Vermont and civil society groups, in addition to being deemed in violation of privacy regulations in Canada, Australia, Europe, and elsewhere.[348] Nonetheless, it continues to be used by law enforcement agencies, including ICE and CBP. After a small initial contract in 2020 and subsequent renewals over the next few years, the company received a new contract in September 2025, under the second Trump administration, worth up to $9.2 million,[349] followed

Figure 12 *Contract money ICE awarded to Clearview AI*



Source: USAspending.gov.

by a new $225,000 CBP contract in February 2026.[350] **Figure 12** charts the growth in Clearview AI's ICE contracts, showing an unprecedented new commitment to this invasive—and, in a number of jurisdictions, illegal—technology by an emboldened immigration police force.

NEC and Mobile Fortify

Another facial recognition company working with ICE is NEC Corporation. According to the DHS AI inventory, NEC has developed multiple facial recognition uses for DHS, including Mobile Fortify.[351]

Mobile Fortify[352] is a new facial recognition phone app used by ICE or CBP agents. This app sends facial images, fingerprints, and document photos to CBP-managed biometric systems for matching against hundreds of millions of biometric records.[353] When the app "identifies" someone, it shows biographical and personal data about that person pulled from various places. At a minimum, this includes, for example: name, birth date, citizenship and immigration information—including whether someone has a deportation order—family information, country of citizenship, etc.[354] The tool allows ICE to identify individuals and was classified as a "high-impact" AI system in DHS's 2025 AI Use Case Inventory.[355] ICE officials have stated that they consider an identity "match" in Mobile Fortify to be a "'definitive' determination of a person's [citizenship] status and that an ICE officer may ignore evidence of American citizenship—including a birth certificate" if the app indicates otherwise. In other words, even if you were to provide evidence of citizenship, ICE officials have stated that they will defer to the determination of the app.[356] ICE's deployment of the app during the 2026 Operation Metro Surge and other aggressive operations has caused severe public backlash after being used over 100,000 times in Minnesota, Chicago, and elsewhere.[357] Data collected by Mobile Fortify is stored in DHS traveler systems for 15 years. This kind of street level surveillance will have enormous impacts for US residents. Current laws and policies—from consumer protection to criminal justice—are wholly insufficient to tackle the harms of this type of data extraction. It is not clear what avenues exist to challenge the collection of "AI evidence" since individuals are not aware of, much less consenting to, its use.

In addition to creating the Mobile Fortify app, NEC is the primary contractor for the CBP Traveler Verification Service, which collects biometric data such as facial images of those who cross the US borders. NEC also manages facial recognition for DHS's OBIM, which oversees major DHS biometric programs such as IDENT and its replacement system in development, HART.[358]

BI²

Other lesser-known companies, such as BI², have quietly carved out their own lucrative niches within ICE's expanding biometric surveillance infrastructure. In September 2025, ICE awarded a $4.6 million contract to BI² Technologies LLC for "IRIS biometric recognition technology for offender recognition and access to a biometric information system to allow ICE agents to quickly authenticate the identity of subjects during field operations."[359]

BI²'s flagship products—the Inmate Recognition and Identification System (IRIS) for fixed facilities and the Mobile Offender Recognition and Information System (MORIS) for field operations—capture over 265 unique points from the human iris to generate a biometric template, enabling real-time identification at distances of up to one meter. While ICE justified the award as a sole-source contract,[360] arguing BI² was the only vendor capable of providing these specific systems, the company's path to this lucrative deal was paved

by deep connections to the Trump administration. BI² hired Ballard Partners shortly after Trump's election. This lobbying firm was founded by Brian Ballard, who reportedly has unparalleled entree to the president's inner circle; Ballard Partners managing partner Susie Wiles now serves as Trump's chief of staff, and former Attorney General Pam Bondi is an alumni.[361] According to lobbying disclosures, Ballard Partners' sole focus for BI² was promoting IRIS technology to the Department of Homeland Security.[362] BI² is not the only Ballard client to score a no-bid ICE contract under the Trump administration; other notable clients include Palantir and SNA International.

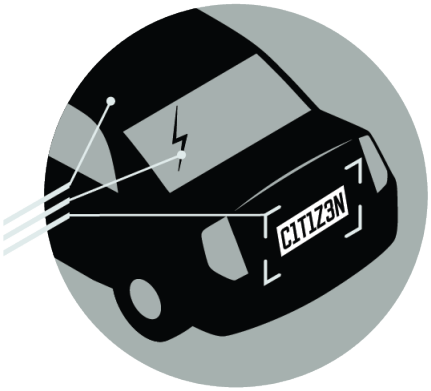
DNA Testing

SNA International

Facial recognition is not the only biometric data that DHS is collecting and using. SNA International won a $25 million DNA testing contract from ICE in March of 2025.[363] This contract is for Rapid DNA testing use by ERO agents to "verify biological relatives," which was piloted in 2019 as a joint ICE/CBP program under the first Trump administration as a means to enable family separation under the guise of combating "family unit fraud."[364]

DNA testing in general was expanded dramatically under the first Trump administration. In March 2020, the DOJ approved a new rule, titled "DNA-Sample Collection from Immigration Detainees," which expanded DNA collection to all ICE and CBP detainees, with limited exceptions, and mandated storage of the collected DNA profiles in the FBI's CODIS biometric database under the authority of the DNA Fingerprint Act of 2005. This led to the addition of 2.6 million DNA profiles to the CODIS database between 2020 and 2025,[365] including an estimated 133,000 migrant teens and children as young as four years old.[366] 2,000 US citizens had their DNA profiles transferred by CBP to the CODIS system, including 95 minors. The overwhelming majority (97%) of cheek swab samples were collected under civil, not criminal, authority. This expansion of genetic surveillance has not been authorized by Congress for citizens, children, or civil detainees.[367]

5. Nationwide Driver Surveillance



What is driver surveillance tech?

DHS is using a variety of technologies to acquire, analyze, and store data from vehicles and their drivers. ALPRs use cameras and software to capture and store vehicle license plate information.[368] DHS uses ALPR data to locate and apprehend individuals. DHS and police are also purchasing data mining technologies that can acquire location data, driving history or any information that a mobile phone shares with a car. This technology can track a person's movements across multiple modes of transit, linking phones to cars and building a comprehensive geolocation profile without ever obtaining a warrant.

DHS and automated license plate readers

Flock

Despite Flock holding no direct contract with ICE, DHS has gained access to its vast network of AI-powered cameras—now deployed in more than 5,000 communities across the country—through an informal pipeline enabled by local law enforcement. Local police departments across the US have performed thousands of Flock lookups explicitly on behalf of ICE, with search reasons listed as "immigration," "ICE," "ICE+ERO," "ICE WARRANT," and "illegal immigration." These searches, which allow officers to pull a target's vehicle movements across Flock's nationwide

database, were conducted by local police acting as informal intermediaries, granting federal immigration authorities side-door access to a surveillance tool they have not contracted for directly.[369] This informal pipeline, enabled by cooperative local police and left untouched by any formal data-sharing agreement, allows ICE to bypass both the competitive procurement process and any public scrutiny that might accompany a direct contract.

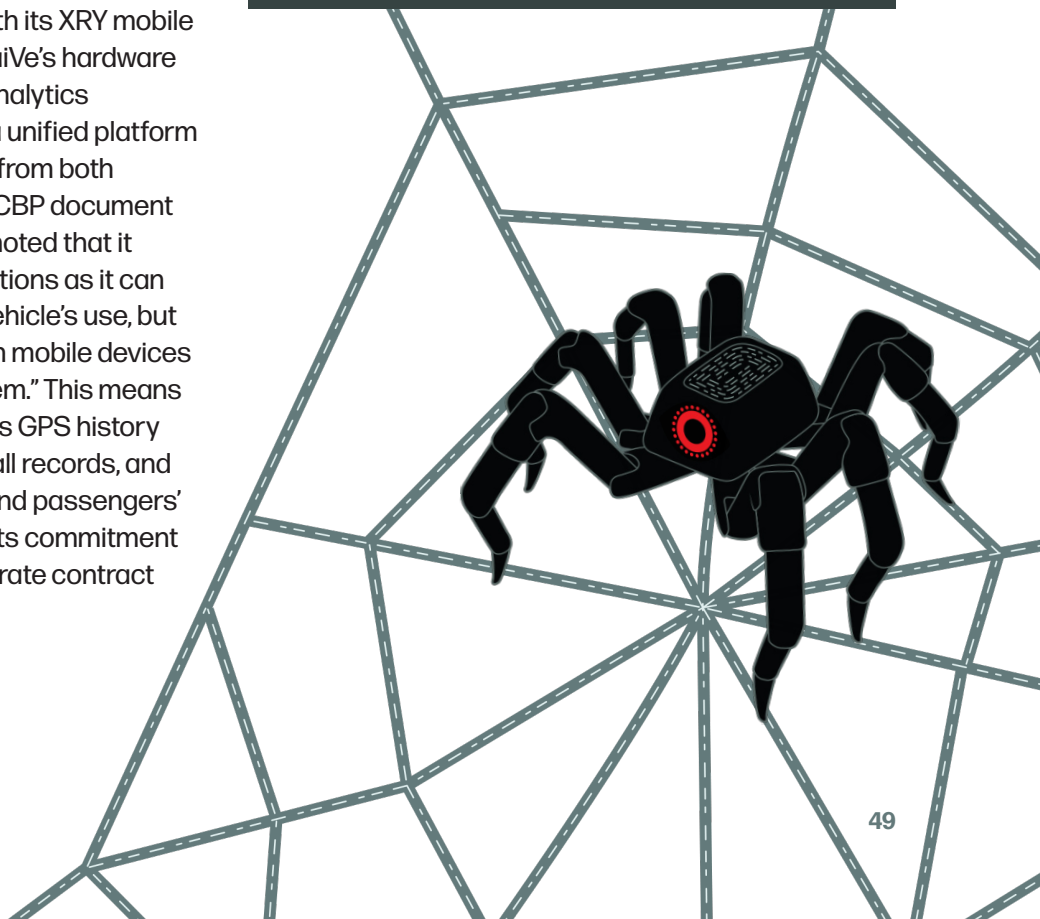
DHS and data mining of car data

Berla iVe

Tools like Berla iVe allow agents to mine data from cars' internal computers, extracting travel histories and device connections from everyday vehicles.[370] Berla iVe is a vehicle forensics system developed by the US-based Berla Corporation. It has been a critical tool for federal enforcement since at least 2018, when CBP identified it as the only commercially available product capable of extracting information from vehicles.[371] Berla iVe and other similar technologies can reconstruct a person's movements across multiple modes of transit, linking phones to cars and building a comprehensive geolocation profile without ever obtaining a warrant. Since 2016, Berla has collaborated with the Swedish forensic firm MSAB, which also supplies ICE with its XRY mobile extraction tools, to integrate BerlaiVe's hardware capabilities with MSAB's XAMN analytics software. Together these create a unified platform for extracting and analyzing data from both vehicles and mobile devices.[372] A CBP document from a 2021 contract with MSAB noted that it would be "critical in CBP investigations as it can provide evidence regarding the vehicle's use, but also information obtained through mobile devices paired with the infotainment system." This means agents can access not only a car's GPS history and trip logs, but also contacts, call records, and messages synced from drivers' and passengers' phones.[373] In 2025, CBP renewed its commitment to the technology with three separate contract awards.[374]

ALPRs and the tech oligarchy

The proliferation of automated license plate readers (ALPRs) from companies like Flock Safety is bound to the broader tech oligarchy ecosystem through ties to venture capital. Peter Thiel's Founders Fund participated in Flock's Series A round of seed funding in 2018 and its more recent Series F round of funding in March 2025, which totaled $285 million alongside other investors.[375]Former Founders Fund partner Geoffrey Lewis now serves as an investor and board observer for Flock.[376]Although there is no evidence of a direct contract between the two companies, the Thiel-founded company Palantir has previously acknowledged being contracted to help a multi-jurisdictional program analyze ALPR data at a time when no laws governed the technology.[377]These connections matter because they point to a shared operational vision across different companies developing surveillance tech for different enforcement bodies: Flock builds the national dragnet of vehicle movement data, and Palantir builds the analytical platforms to make that data legible for enforcement.



6. Hacking Devices and Spyware



What do we mean by hacking and spyware?

Stories of ICE and CBP agents attempting to hack phones and computers are on the rise. In FY2025, CBP searched 55,318 devices, with 2026 Q2 confiscations reaching an all-time high.[378] DHS and the FBI announced investigations into group chats of protesters in Minnesota[379] and Minnesota legal observers and protesters also reported that DHS confiscated their phones.[380] Advocates are concerned that DHS is looking to acquire contacts, messages, location history, passwords, photos, videos, names of associates or other biographical information from phones.

While the use of invasive digital forensics by immigration enforcement is not new, the scale of procurement has intensified under the Trump administration. In 2025 alone, ICE and CBP secured at least 13 separate contracts for mobile extraction tools like Israel's Cellebrite's UFED and private equity-owned Magnet Forensics' GrayKey, with a combined public value exceeding $27 million.[381] ICE also holds other, smaller contracts with companies including FinaleMobile[382] and Arsenal Recon.[383] These tools can crack encrypted phones to retrieve deleted messages, location histories, and call logs—effectively enabling warrantless digital searches.

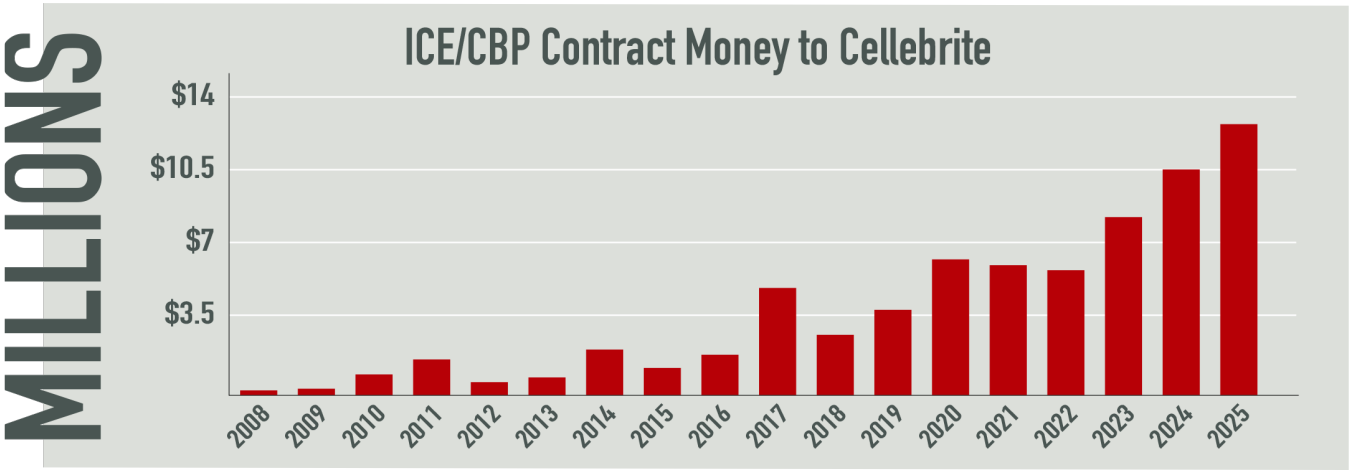
DHS primary device hacking companies

Cellebrite

Both ICE and CBP have contracted with Israeli digital intelligence company Cellebrite since 2008.[384] Cellebrite has, in particular, received over $56 million in federal contracts in 2025-26,[385] primarily for its UFED hacking software that extracts data (including deleted messages and locations) from mobile devices— a primary tool for DHS.[386] ICE alone plans to award an open-ended $100 million contract to the company later in 2026.[387]

In 2020, President Trump pardoned Cellebrite CTO Chris Wade for federal cybercrimes that prosecutors maintained under seal,[388] a move that effectively cleared his record. Wade's subsequent career trajectory proved pivotal: after his pardon, Cellebrite acquired Corellium for $200 million in June 2025 and installed Wade as its Chief Technology Officer.[389] The acquisition carries troubling historical echoes:

Figure 13 *Contract money awarded to Cellebrite by ICE and CBP*



Source: USA spending.gov

leaked documents show that Corellium in 2019 offered a trial of its product to NSO Group, whose Pegasus spyware has been repeatedly caught targeting dissidents, journalists, and human rights defenders worldwide. Corellium also offered its product to DarkMatter, a now-shuttered Emirati cybersecurity company that hired former US intelligence members who reportedly helped it spy on human rights activists and journalists.[390] The combined entity—Corellium and Cellebrite—is developing a new beta product called Mirror, which enables police to create a virtual clone of a seized device and all its data. Mirror creates the capacity for unprecedented intrusion into journalists' and activists' private communications.[391]

GrayKey

Another tool in DHS's hacking arsenal is GrayKey, a device that allows law enforcement to unlock mobile phones and extract their contents. Launched in 2016 by the company Grayshift—co-founded by a former Apple security engineer—GrayKey was developed as a direct competitor to Cellebrite's existing phone-hacking system, UFED.[392] It can bypass iPhone passcodes to retrieve a wide range of data, including deleted messages, photos, location history, and call logs, effectively giving investigators a complete window into a target's private life and associations. In 2023, Grayshift merged with Magnet Forensics, another digital investigation firm, consolidating their capabilities under one roof.[393] ICE has maintained a steady relationship with the technology, with records showing the agency awarded a $3 million contract in mid-September 2025 specifically for Magnet Forensic Software Licenses, and another $90,000 contract specifically for "GrayKey Premier Software renewal licenses for iOS and Android extractions,"[394] as part of its Homeland Security Investigations work. The ability to deploy GrayKey on a large scale means ICE can conduct deep, warrantless searches of phones seized during raids, sweeping up data not only from targets but potentially from friends, family, and associates caught in the enforcement net.

Cellebrite has received over $56 million in federal contracts in 2025–26, primarily for its UFED hacking software that extracts data (including deleted messages and locations) from mobile devices— a primary tool for DHS. ICE alone plans to award an open-ended $100 million contract to the company later in 2026.

DHS and spyware

Paragon

From September 2024 to January 2026, ICE also held a $2 million contract with Paragon Solutions,[395] an Israeli company that allows users to remotely hack into phones, read encrypted messages, access files and data, activate the phone as a listening device, and more—all without the targeted individual ever clicking on a link. The company's "Graphite" spyware has been used to hack the phones of journalists and members of civil society organizations in various countries. Its use was previously placed on hold by the Biden administration after the former President signed an executive order barring the use of commercial spyware that poses a national security risk to the United States, until the Trump administration revived the Paragon Solutions contract in late 2025. ICE has repeatedly offered conflicting information about whether it contracts with Paragon. ICE's contract with Paragon ended in January 2026. However, in April 2026, ICE acknowledged it was using commercial spyware,[396] but did not identify Paragon specifically.[397] In May, DHS told the press that it does not have a relationship with Paragon or its new parent company. It is unclear whether ICE has ceased using Paragon spyware, continues operations under another contract, or uses some other spyware company that ICE has failed to disclose to the public. ICE continues to withhold documentation and information related to their use of these technologies.[398]

7. Cellphone Tracking and Location Data



What is cellphone tracking and location data?

Another example of ICE's indiscriminate surveillance capacity is DHS's use or acquisition of cellphone location data. Location data is a digital record of movement produced by GPS-enabled devices, like a cellphone or a computer. By buying cell phone location, DHS attempts to avoid legal requirements for arrest and apprehension, such as obtaining a warrant. DHS can also acquire location data through data brokers (see above).

Here are some of the ways DHS collects data through cell phones:

- "Stingrays": Formally called cell site simulators, these devices essentially impersonate cell towers to force all nearby phones to connect, sweeping up the data of every bystander in what functions as a digital dragnet.[399] Law enforcement can then use this connection to identify the precise location of a target device and, depending on the simulator's capabilities, potentially intercept calls, text messages, and internet traffic. Unlike data from traditional cell towers, which is often imprecise, these tools provide a much higher degree of accuracy but do so by indiscriminately capturing signals from everyone who happens to be in the vicinity.[400]
- Online advertising data: CBP has also tapped into a vast, largely unregulated source of location data: the online advertising industry. According to an internal DHS document obtained by *404 Media* and published in March 2026,[401] CBP acknowledged for the first time that it purchased phone location data derived from real-time bidding—the automated auction process that determines which ads appear on your phone. This data, sourced from ordinary apps like video games, dating services, and fitness trackers, is collected and repackaged by data brokers, creating what privacy advocates have called a "goldmine for tracking where every person is and what they read, watch, and listen to."[402] CBP ran a pilot program using this advertising-derived location data between 2019 and 2021, but the agency has not confirmed whether it continues to purchase such data.[403]
- Administrative subpoenas: ICE or CBP send requests, often without a warrant, to a person's cell phone carrier (e.g. Verizon), social media companies (e.g. Facebook), or an internet company (e.g. Google) for private account information, including location data. DHS has also asked for information beyond location data, including information that triggers First Amendment concerns. For example, ICE sent administrative subpoenas to social media sites, such as Reddit, Discord and others, requesting information about users who posted about the Los Angeles immigration enforcement surge.[404]
- Geofence warrants: In criminal investigations, law enforcement, such as local police or the DOJ, directs "geofence" warrants to internet or phone companies to collect granular user location information. In short, a geofence warrant demands that the company provide information about which mobile phones were present within a certain geographic area during a specified time frame. Usually, they are used when law enforcement does not know the identities of suspects, only an approximate time and location. The legal landscape around law enforcement's use of geofence warrants is murky at best because it sweeps in phone data from bystanders who happen to be near the target. In April 2026, the Supreme Court heard arguments on the legality of geofence warrants,

and this case will have implications on privacy rights and the ways that law enforcement agencies can use location tracking surveillance technology.[405]

Companies that are helping retrieve location data for DHS

TechOps Specialty Vehicles

In May 2025, the agency awarded an $825,000 contract modification to TechOps Specialty Vehicles LLC, a Maryland-based company, to provide additional "Cell Site Simulator … Vehicles to support the Homeland Security Technical Operations program."[406] This award followed a previous contract in September 2024 for $818,000, demonstrating a sustained investment. According to *TechCrunch*, TechOps Specialty Vehicles integrate surveillance technology—sourced from elsewhere—into customized vehicles, including "Mobile Forensic Labs" and "Mobile Command Vans" designed for "on-site forensic analysis" and "advanced surveillance and mission coordination." The company's president confirmed they integrate cell site simulators but declined to name the manufacturer, citing "trade secrets."[407]

CellHawk

Software like CellHawk further weaponizes location data, transforming static phone records into a tool for persistent, automated surveillance. Developed by the Texas-based company Hawk Analytics, CellHawk is a web-based platform that helps law enforcement to visualize vast quantities of cellular data. According to a 2020 investigation by *The Intercept*, the tool's capabilities extend far beyond simple analysis. Its promotional materials boast of the ability to send email and text alerts "to surveillance teams" the moment a target's phone moves or enters or exits a predefined "Geozone"—which could be as large as an entire county border. This transforms an investigative tool into a real-time tracking system. While the company's website mentions the ability to view maps of the cell towers a target uses most frequently, its brochures sent to potential clients are far more explicit, promising investigators the ability to "find out where your suspect sleeps at night" by analyzing those daily patterns.[408] This is done by, for example, integrating with cell site simulators; using GPS records; and mapping more than 20 phones at once to see how they move relative to another, allowing police to map out an individual's social network and daily routine. In 2025, ICE's Charlotte office purchased CellHawk Software licenses.[409]

8. Skip Tracing and Contract Bounty Hunters



What is a DHS bounty hunter?

As part of the Trump administration's detention and deportation push, ICE has expanded capacity by outsourcing targeting operations to the private sector—this includes independently tracking down and confirming individuals' addresses using lists provided by the agency. Under the scheme, vendors are given a caseload of up to 50,000 "last known addresses of aliens residing within the United States of America," with the mandate to "use all technology systems available" to identify and validate last addresses.[410] Most alarmingly, ICE structures vendor payments around success rates, and these private companies collect bounties for confirmed locations and successful document deliveries, pushing vendors to procure phone numbers, social media footprints, vehicle data, and even photographic evidence of a target's private life at home or work.

In 2025, ICE procured at least 15 different contracts—totaling over $55 million in federal funds committed

through early 2026, with more than $1 billion in potential contract money through 2028—for "skip tracing services."[411] This commercial service is traditionally employed by debt collectors and bail bondsmen to locate individuals who have "skipped out" on financial obligations. Now, for ICE, the vendor's mandate is to deploy a vast surveillance toolkit, including automated data brokers, real-time searches, public records, social media scraping, and even physical reconnaissance to verify immigrants' residence and employment addresses and track "fugitive aliens."[412] The companies doing the skip tracing receive basic biographical information on 50,000 individuals per month, with the mandate of identifying their current address using "all technology systems available," as well as "physical, in-person surveillance," in order for ICE to conduct raids or serve official documents.[413]

Companies involved in skip tracing include:

AI Solutions 87

One of the companies, AI Solutions 87, will provide AI agents to ICE that it says can autonomously track "people of interest and map out their family and other associates more quickly'."[414]

Capgemini

One of the companies that won a $4.8 million contract with ICE for skip tracing work, France's Capgemini, received a swift rebuke from French lawmakers and announced plans to sell its US subsidiary over the deal,[415] under which it stands to make up to $365 million.[416]

B.I. Incorporated

Another company that won a $1.5 million contract is the Colorado-based B.I. Incorporated,[417] subsidiary of The Geo Group, Inc., which has also provided ICE with wrist-worn GPS monitoring technology through its "Veriwatch" product. BI is heavily involved in "alternatives to detention" programs in DHS.

9. Detention and Deportation Tracking Apps



What are detention and deportation tracking apps?

For many years, DHS has required that people install apps on their phones or use wearable devices so that they can track and monitor noncitizens for removal and detention. These continuous monitoring apps, referred to as "digital cages," have been forced on hundreds of thousands of noncitizens. These apps, labeled "Alternatives to Detention," have not resulted in fewer detention beds. In fact, DHS continues to plan for 100,000 detention beds[418] and one million removals alongside the deployment of continuous monitoring apps.[419]

DHS companies involved in detention and deportation tracking apps

Smartlink and Veriwatch

B.I. Incorporated has expanded dramatically under the Trump administration, as it is the main operator of ICE's Alternatives to Detention (ATD) program. The ATD program monitors approximately 180,000 migrants awaiting immigration proceedings through a combination of GPS ankle monitors, the Veriwatch wrist-worn devices, and a smartphone app called SmartLINK.[420] The SmartLINK app requires participants to log their whereabouts at least once a day using facial recognition and GPS tracking, while the newer VeriWatch provides GPS location monitoring, facial matching, and

messaging functionalities, and works similarly to a consumer smartwatch.[421] ICE has already used the location data collected through these tools in enforcement operations; during the first Trump administration, agents followed the GPS location of a woman in the ATD program to help secure a search warrant for a chicken processing plant in Mississippi, leading to the detention of roughly 680 immigrants in a single raid.[422]

CBP One app

The administration has simultaneously moved to weaponize the CBP One app—originally created under the Biden administration as a portal for asylum-seekers to schedule appointments and enter the country legally—as a tool for self-deportation. In March 2025, former DHS Secretary Kristi Noem announced the launch of the CBP Home app, a rebranded version of the same platform, instructing migrants to "leave now" or face arrest.[423] By April 2025, DHS had reportedly revoked parole status for nearly one million migrants who had entered using the app, giving them seven days to self-deport or be apprehended.[424] The tracking infrastructure for these self-deportations is powered by Palantir's ImmigrationOS. Together, these systems form a closed loop: the SmartLINK and VeriWatch devices track those awaiting proceedings; the CBP Home app funnels self-deportations into a trackable pipeline; and Palantir's ImmigrationOS processes the resulting data to identify new targets, score addresses, and map the next neighborhoods to raid.

The ATD program monitors approximately 180,000 migrants awaiting immigration proceedings through a combination of GPS ankle monitors, the Veriwatch wrist-worn devices, and a smartphone app called SmartLINK.

10. Border Towers and Drones



Massive investments are flowing into the border, with a sustained focus on drones and surveillance towers. We have created two sections to address DHS use.

What is a surveillance tower?

Surveillance Towers: CBP surveillance towers are fixed and relocatable towers stationed across the border that can detect, identify, track, and classify items (including humans) around the border. These towers have powerfully invasive surveillance capabilities and use data analytics to help border patrol agents surveil the area and prioritize resources for border enforcement. The "border" spans an area 100 miles from the US physical border, and it remains to be seen how far into the interior these towers will operate.

DHS towers and Anduril

Trump's OBBBA allocated $2.8 billion for surveillance technologies along the southwest, northern, and maritime borders.[425]While this funding covers a range of technologies, the anchor of these surveillance systems are different types of towers installed at regular intervals along the border. Existing infrastructure includes:

- Integrated Fixed Towers (IFTs) developed by Israeli military contractor Elbit Systems. These are 80 to 140 feet tall and are equipped with day and night cameras and a radar that can identify people 7.5 miles away.[426]

- Remote Video Surveillance System (RVSS) from military contractor General Dynamics. These are smaller, relocatable surveillance towers along the Southwest and Northern borders. Some cameras are also mounted on tall buildings or other structures.[427]
- Mobile Video Surveillance Systems (MVSS) consist of a 4x4 truck with telescoping poles in the bed that extend up to 35 feet in the air, outfitted with thermal and video cameras and a laser illuminator.[428]

However, the most important border tower contractor, by far, is now Anduril Industries, founded by Palmer Luckey and backed by Peter Thiel, Marc Andreessen, and even JD Vance personally at one point.[429] The OBBBA requires all new border towers to be designated "autonomous," a requirement specifically designed to favor Anduril's autonomous "Sentry" border towers, which use machine learning software to scan the border region for objects of interest, distinguishing humans from livestock, for example.[430]

As of early 2026, four vendors had already passed the "autonomy test" for border towers,[431] including General Dynamics, which unveiled a new autonomous tower in March 2026.[432] However, the overwhelming beneficiary of this contracting requirement will be Anduril, which is already the main contractor for the operation and maintenance of CBP's AI-driven automated surveillance towers along the northern and southern borders.[433] Anduril received $363.4 million from CBP in the first half of 2026 alone,[434] more than twice the previous year and a figure that would have amounted to more than 15% of the company's total 2025 revenue.[435] The Electronic Frontier Foundation has documented at least 585 autonomous surveillance towers along the US-Mexico border, and CBP has plans to install 1,500 more towers over the next few years.[436]

What is a drone?

Unmanned Aerial Vehicles (UAVs), commonly known as drones, is an aircraft with no human pilot. It is controlled remotely or programmed to fly independently. Originally used by the military, their use is being fast tracked by police departments and federal law enforcement agencies. CBP has flown

The most important border tower contractor by far is now Anduril Industries, founded by Palmer Luckey and backed by Peter Thiel, Marc Andreessen, and even JD Vance personally at one point.

drones, including military grade Predator drones, over protests for racial justice[437] and immigration enforcement surges.[438] Congress has repeatedly flagged concerns with DHS drone deployment.[439]

CBP and ICE drone programs

CBP has had its own small drone program since at least 2020 and currently operates around 500 small drones.[440] The agency has purchased drones from a number of different companies, drawing from a list developed by the Defense Innovation Unit following a July 2025 memorandum titled "Unleashing US Military Drone Dominance."[441] The two drone providers from the so-called "Blue List" that have had the most success in contracting with CBP thus far are Red Cat Holdings (Teal Drones)[442] and the startup Skydio, after smaller contracts for purposes of evaluation with Vantage Robotics and Parrot do not appear to have resulted in larger agreements.[443]

DHS has greatly expanded its investment in drones in order to incorporate them into the policing of the US interior. In early 2026, DHS implemented significant measures to facilitate the acquisition and use of small drones and counter-drone technologies, requesting proposals from private industry for a new $1.5 billion contracting vehicle, as well as a $115 million investment in new drone technologies—to be used at events like the 2026 FIFA World Cup—through the DHS Science & Technology Directorate (as described in Section 4 of this report).[444] Former DHS Secretary Kristi Noem framed the new Program Executive Office for Unmanned Aircraft Systems and Counter-Unmanned Aircraft Systems as part of a "new era to defend our air superiority to protect our borders and the interior of the United States."[445] Concurrently, DHS authorized all department components and state and local partners to "fully combat drone threats" in December 2025.[446]

Skydio

In 2025 alone, CBP awarded multiple contracts for AI-powered drones to Skydio for its Buffalo Sector.[447] The venture capital firm Andreessen Horowitz has participated in nearly every funding round for Skydio. As detailed in Section 2 of this report, Marc Andreessen, alongside Elon Musk, has been actively involved in shaping tech policy and personnel decisions within the administration,[448] exemplifying the direct line between tech oligarchy investment and federal procurement.

ICE has followed CBP in acquiring Skydio's AI-powered drones,[449] capable of detecting individuals from 7.5 miles away and identifying them from nearly a mile,[450] part of a worrying trend in which surveillance technologies justified for border enforcement are seamlessly repurposed for domestic monitoring, including the surveillance of protests and political demonstrations. According to reporting from the Washington Post, ICE has already used small drones to monitor protests over the past year, while CBP has deployed MQ-9 Predator military-grade aircraft drones over anti-ICE demonstrations in Los Angeles.[451] This mirrors a broader pattern: the NYPD, which has adopted Skydio drones exclusively for its Drone as First Responder program,[452] flew multiple X10D aircraft over "No Kings" protesters in Manhattan, logging over 20,000 flights in 2025 and using drone footage to identify and arrest demonstrators.[453] While reporting has not often been able to confirm the make and model of drones used during ICE operations and counter-protest activity, the agency used drones to post footage of anti-ICE protests in Chicago,[454] and drone sightings surged in Minneapolis in early 2026 during protests in that city.[455]

ICE has followed CBP in acquiring Skydio's AI-powered drones, capable of detecting individuals from 7.5 miles away and identifying them from nearly a mile...

This operational expansion has been accompanied by aggressive new federal airspace restrictions on civilian-operated drones that might monitor DHS activities. On January 16, 2026, the FAA issued NOTAM FDC 6/4375, banning all civilian drone flights within 3,000 feet laterally and 1,000 feet vertically of any DHS facility, vehicle, vessel, or convoy. Crucially, the restriction moves as DHS assets move, creating invisible, roving no-fly zones wherever ICE or other agencies operate, with no advance notice or geographic coordinates provided to the public. This creates a two-tier system: the government expands its own surveillance fleet while systematically preventing civilian operators—including journalists—from documenting those same operations.[456]

Taking Stock

In this section we have documented DHS's adoption and scaling of surveillance technologies—including many AI-enabled technologies. Through its use of these technologies, DHS has assumed the capacity to gather intelligence on non-citizens and citizens alike, specific targets for removal and bystanders, and to do so without warrants or meeting any kind of threshold for suspicion. Many of these technologies have been deployed not only against people in removal proceedings, but people who are protesting brutal, violent, or authoritarian immigration enforcement practices. These technologies, therefore, are part and parcel with the strengthening of DHS as an authoritarian arm of the US government.

The fast and dramatic expansion of the ICE and CBP budgets over the past year has facilitated the advancement of ICE and CBP's adoption of these technologies. Moreover, these technologies advance DHS's mission of swiftly growing its deportation dragnet without regard to the constitutional rights of those who are swept up in it. The adoption of these technologies is facilitated by the close relationships between the Trump administration, venture capitalists, and other elements of the tech oligarchy that together make up the new security state.

Our task is to fight back, with this picture in mind. In the next section of the report we outline ways to do just that.

6. Organized Resistance

The surveillance and deportation systems described throughout this report were built through political choices, public investments, and corporate partnerships. They can be challenged in the same way. The technologies that power modern immigration enforcement depend on local government cooperation, private sector participation, taxpayer funding, and public legitimacy. This section outlines concrete strategies for disrupting that infrastructure, from local campaigns and worker organizing to litigation, market pressure, federal advocacy, and political education. While the scale of the challenge is significant, these systems are neither inevitable nor invulnerable.

As immigration enforcement becomes increasingly powered by AI, data sharing, and corporate surveillance, the fight ahead is not only about resisting individual policies or administrations. It is about confronting the infrastructure and logics that makes mass surveillance, policing, detention, and deportation possible in the first place.

The scale of the surveillance, policing, and corporate power outlined here can feel overwhelming. That is not accidental. This political moment has been designed to make people feel powerless and to make resistance seem impossible. The Trump administration and the tech oligarchs aligned with it want the public to believe that an AI-driven security state is inevitable and unstoppable. It is not. These systems depend on taxpayer funded contracts, local government cooperation, and popular buy-in to corporate legitimacy, all of which can be challenged, disrupted, and dismantled through organized collective action.

There are concrete ways to weaken the infrastructure that powers the immigration dragnet and to build power capable of stopping its expansion.

This doesn't mean it will be easy. Defending immigrant communities and building a different future will require coordinated action at every level: local organizing, corporate accountability campaigns, worker resistance inside tech companies, strategic litigation, public pressure, and long-term federal policy fights. But more than anything, meeting this moment will require experimentation, political imagination, and new forms of organizing capable of confronting systems that are rapidly evolving.

Local Governments

1) Dismantle data sharing with ICE;
2) End expansion of surveillance technology;
3) Strengthen privacy protection.

Local governments have a critical role to play in resisting the expansion of the immigration enforcement and surveillance apparatus. While federal agencies like DHS and ICE rely on massive technological infrastructure to carry out enforcement, much of that infrastructure depends on cooperation at the local level. Cities, counties, and states collect and share data, deploy technologies, and approve contracts. Local governments can either deepen their cooperation or help dismantle the systems that make mass surveillance and deportation possible. This means focusing on three interconnected areas: dismantling data sharing with ICE, stopping the expansion of surveillance technologies, and strengthening privacy protections.

Dismantle data sharing with ICE

One of the most immediate ways local governments can limit the reach of immigration enforcement is by cutting off the flow of local data into federal systems. This includes ending contracts that allow information-sharing technologies connected to ICE or DHS, particularly contracts that enable biometric data collection, cross-referencing, or indirect data transfers to federal agencies. Municipalities should also terminate contracts with private data brokers that sell information to immigration enforcement agencies, prohibit local agencies from accessing federal immigration databases, and close loopholes that allow sanctuary protections to be bypassed through third-party vendors or contractors.

These forms of cooperation are often deliberately hidden from public view. Contracts with technology vendors frequently contain buried provisions that authorize data sharing with DHS or grant companies broad discretion over how information is used and disclosed. In many cases, communities only learn about these arrangements after advocates conduct independent contract reviews, file public records requests, or push for audits.

Cook County, Illinois offers a recent example of how these loopholes operate. In 2022, advocates and legal organizations challenged the Cook County State's Attorney's Office over its contract with Appriss, a private technology company that managed jail and custody-related data systems for domestic violence survivors.[457] Although Cook County maintains sanctuary protections intended to limit cooperation with immigration enforcement, the current contract allows information about people in county custody to be shared with third parties connected to DHS enforcement systems. An ongoing campaign has exposed how data sharing can continue even in jurisdictions that publicly identify as protective of immigrant communities, particularly when private contractors operate with limited transparency and oversight.

End expansion of surveillance

Local governments also have the power to stop the expansion of surveillance technologies that deepen policing, criminalization, and immigration enforcement. Over the last decade, local police departments and public agencies have increasingly adopted predictive policing systems, automated license plate readers, facial recognition tools, algorithmic risk assessments, and large-scale data integration platforms. These technologies are often introduced under the promise of efficiency or crime prevention, but in practice they expand the scope of surveillance while increasing the amount of data available to law enforcement and federal agencies.

Cities and counties should cancel predictive policing programs and algorithmic systems developed by companies like Palantir Technologies, whose software has long played a central role in immigration enforcement operations. Local governments should immediately terminate existing Palantir contracts and prohibit law enforcement agencies from collecting, storing, or accessing local data through Palantir systems. They should also halt the expansion of data centers and digital infrastructure, which not only increase local



taxes and resident expenses, but are designed to facilitate mass surveillance and large-scale data consolidation.

Communities should approach other surveillance technologies with similar scrutiny. Automated license plate reader systems operated by companies such as Flock Safety have rapidly expanded across the country, often with little public oversight and confusing information about their data privacy policies. These systems create massive searchable databases of vehicle movement that can be shared across jurisdictions and accessed by agencies involved in immigration enforcement. Law enforcement agencies will rarely argue that they need fewer surveillance tools. The issue is not whether these technologies generate more information, but whether communities are willing to accept the civil rights, racial justice, and democratic risks that accompany widespread surveillance infrastructure.

There are growing examples of municipalities pushing back against these systems. In 2019, San Francisco became the first major US city to ban government use of facial recognition technology.[458] Portland later passed some of the strongest municipal restrictions in the country by limiting both public and private uses of facial recognition in places of public accommodation.[459] More recently, community campaigns in cities including Nashville and Norfolk have challenged or halted the expansion of automated license plate reader programs after raising concerns about data sharing, racial profiling, and immigration enforcement access. These examples demonstrate that surveillance expansion is not inevitable and that organized local pressure can successfully interrupt the spread of these technologies.

Strengthen privacy protections

The most effective way to prevent harmful data sharing is to limit the collection of sensitive data in the first place. Local governments can pass strong biometric privacy protections that give residents meaningful control over how their biometric information is collected, stored, and used. These protections should include clear consent requirements, limits on data retention and sharing, and enforcement mechanisms that allow residents to take legal action when companies misuse their information.

California's privacy protections and biometric privacy laws helped create the legal foundation for organizations to challenge how companies like Clearview AI were building surveillance systems that could later be used by DHS and ICE. In 2020 and 2021, Mijente, Just Futures Law, and partner organizations supported legal action and public records litigation against Clearview AI and federal agencies after it was revealed that the company had scraped billions of photographs from social media and websites without consent in order to build facial recognition databases marketed to law enforcement agencies, including immigration enforcement. The lawsuits and records requests relied in part on state privacy protections to challenge the collection and use of biometric data and to expose how facial recognition technologies integrated into federal surveillance and immigration enforcement systems.

Local governments should build on these examples by requiring public disclosure of surveillance and cloud-storage contracts tied to law enforcement and by creating strong community oversight mechanisms for technology procurement and approval.

Local governments cannot confront these systems through policy changes alone. Surveillance and data sharing are enormously profitable industries, and companies that benefit from them will aggressively defend their position. Technology firms routinely lobby elected officials, spread misleading narratives about public safety, and pressure governments to expand surveillance powers. Countering that influence requires organized community pressure capable of challenging both the political and economic power behind the surveillance industry.

Local governments also have the power to stop the expansion of surveillance technologies that deepen policing, criminalization, and immigration enforcement.

Challenge Corporate Power

1) Protest and name names; 2) Engage in strategic litigation and policy advocacy; 3) Support worker organizing; and 4) Pressure the market.

One of the greatest sources of power these corporations hold is their ability to manufacture necessity, even at the cost of human lives. Surveillance technologies are often introduced as solutions to dangers that companies—along with the government—exaggerate or help construct through fear-based narratives around crime, migration, and public safety. Communities are told that more data collection, more predictive systems, and more monitoring are necessary to stay safe, even when many of these technologies did not exist a decade ago and have never been proven to reduce harm in meaningful ways. Corporations then position themselves as the only actors capable of solving the crises they helped define.

As this report argues, technology corporations are not simply vendors selling tools to the government. Increasingly, they are embedded within government decision-making itself, shaping public policy, influencing procurement priorities, and helping design the infrastructure of modern enforcement systems. But communities across the country have already begun experimenting with these approaches, offering important lessons for broader movements resisting surveillance and deportation infrastructure.

Protest and name names

Public pressure campaigns remain one of the most effective ways to expose the corporations profiting from surveillance and deportation infrastructure. Organizers should continue building protests, public education campaigns, demonstrations, and direct actions that identify the companies and executives responsible for developing, financing, and maintaining enforcement technologies. Part of the power these corporations rely on is invisibility. Most people do not know which companies operate local surveillance systems, where their offices are located, or how deeply integrated they are into government infrastructure.

Mapping local corporate footprints can therefore become an organizing tool in itself. Communities can investigate which corporations maintain headquarters, data centers, office leases, or public contracts in their cities and expose the relationships that connect local governments to immigration enforcement systems. Campaigns against Palantir, for example, have included demonstrations outside company offices, pressure targeting universities and investors connected to the company, and public education efforts linking Palantir's software to ICE operations and deportation systems.

Engage in strategic lawsuits and policy advocacy

Litigation and policy advocacy are critical tools for disrupting unlawful surveillance and data-sharing practices. Advocates can pursue lawsuits challenging the misuse of biometric data, unlawful information sharing, discriminatory surveillance systems, and violations of sanctuary protections. At the same time, local and state governments can pass policies restricting contracts with corporations that facilitate immigration enforcement or operate surveillance systems without public accountability.

Some of the most important victories in this area have come from advocates willing to experiment with new legal and organizing strategies. In 2021, Mijente, NorCal Resist, and multiple individuals filed a lawsuit[460] against Clearview AI, a facial recognition company that built its database by scraping billions of photographs from social media and other websites without consent. Advocates sought to expose how facial recognition technologies were being integrated into immigration enforcement systems. Advocates raised concerns that the technology could be used to identify, locate, detain, and deport immigrants, as well as monitor protesters, journalists, and others engaged in First Amendment protected activities. The Clearview campaign illustrates why experimentation is necessary. Effective resistance increasingly requires combining litigation, public records requests, privacy law, policy advocacy, investigative research, and organizing campaigns to expose systems that would otherwise remain hidden from public scrutiny.

A few other examples: In 2026, Maine residents filed a federal lawsuit accusing DHS of using facial recognition, license plate tracking, and AI-enabled surveillance to identify and intimidate people documenting immigration raids, alleging violations of First Amendment protections.[461] In Oregon, a federal judge ruled that ICE operations involving facial recognition technology and warrantless arrests of farmworkers were likely unlawful after agents used the Mobile Fortify app during enforcement operations later challenged in court.[462] In Chicago, in May 2026 Alderwoman Jessie Fuentes sued the federal government after federal immigration agents handcuffed her while she asked for a warrant for the detention of a community member at a hospital, raising further concerns about aggressive enforcement tactics and retaliation against people documenting or challenging ICE activity.[463]

Support worker organizing

Workers inside technology companies have become an increasingly important force challenging the expansion of surveillance and military contracting. Employees often possess unique knowledge about how technologies are developed, deployed, and marketed, placing them in a powerful position to expose harmful practices and pressure corporate leadership from within.

Over the last decade, thousands of tech workers at companies including Google, Amazon, and Microsoft have publicly opposed contracts tied to military operations, policing, and immigration enforcement. In 2018, Google employees organized against Project Maven, a Pentagon artificial intelligence initiative, leading the company to decline renewal of the contract after widespread internal backlash.[464] Google workers also protested the company's cloud computing work connected to border enforcement and immigration agencies.[465] Employees at Amazon and Microsoft similarly raised concerns about their companies' relationships with ICE and the broader surveillance apparatus, arguing that technologies they helped build were being used to facilitate detention, deportation, and human rights abuses.[466]



More recently, National Nurses United has been educating and organizing members and communities about Palantir's role in the mass deportation machine.[467] In addition to advocating for abolishing ICE, the union has called on elected officials to rescind their donations from Palantir and for hospitals to cut ties[468] with the company.[469]

Workers inside these companies and agencies should continue organizing against technologies used in detention and deportation systems by refusing to build or maintain harmful tools, raising concerns internally, documenting abuses, and supporting collective action and whistleblowing efforts. Organizers and communities outside these institutions should continue building coordinated campaigns that support worker resistance while applying public, political, and economic pressure to challenge the expansion of surveillance infrastructure.

Pressure the market

Corporations involved in surveillance and deportation infrastructure are also vulnerable to financial and reputational pressure. Shareholder resolutions, divestment campaigns, and investor organizing can force companies to publicly disclose contracts tied to immigration enforcement and answer questions about the risks associated with those relationships. Organizers can also pressure institutional investors, universities, foundations, and pension funds to divest from companies profiting from detention, surveillance, and deportation systems.

There are growing examples of this strategy taking shape. Shareholders and advocacy organizations have repeatedly introduced resolutions demanding greater transparency from companies involved in government surveillance and military contracting.[470] Investor campaigns have also targeted banks and private equity firms financing private prison companies involved in immigration detention, contributing to several major financial institutions announcing restrictions on future financing for the private prison industry.[471] These efforts demonstrate that market pressure can increase the political and economic costs associated with participation in surveillance and deportation infrastructure.

Across the country, corporate executives are increasingly being put on notice by immigrant rights organizers, civil liberties advocates, international human rights organizations, and their own workers. Technology companies have the resources and political influence to oppose the systems that criminalize immigrants and expand mass surveillance. Instead, many continue to profit from those systems while attempting to distance themselves from the harms they produce. Challenging that contradiction will require sustained organizing capable of confronting corporate power at every level.

Be Ready for Federal Openings

Even if major change in Washington, D.C. feels unlikely in the current political moment, we cannot cede the federal terrain. The surveillance and deportation apparatus has been built over decades through federal appropriations, procurement systems, intelligence-sharing agreements, and bipartisan investments in policing and border infrastructure. When political openings emerge, whether through changes in administration, congressional pressure, whistleblower disclosures, or broader public opposition, movements must be prepared to act quickly with concrete demands, legislative proposals, and investigative strategies already developed.

That preparation requires building the infrastructure now to advance oversight, restrict enforcement authority, and dismantle the contracts and funding streams that sustain the security state. Advocates, researchers, technologists, organizers, and policymakers should begin laying the groundwork for future federal interventions by developing proposals, conducting investigations, and documenting abuses in ways that can immediately translate into action when conditions shift.

Some of the steps that can help prepare for those openings include:

- Launching investigations into the role of major federal contractors, including Amazon and Palantir Technologies, in powering immigration enforcement systems across DHS, ICE, CBP, and other federal agencies.
- Producing public reports mapping the contractual relationships between major technology corporations and federal agencies, including subcontractors, resellers, cloud infrastructure providers, and data brokers involved in immigration enforcement systems.
- Conducting congressional and public oversight hearings examining how predictive analytics, biometric surveillance, investigative case management platforms, AI-assisted targeting systems, and other technologies are used in detention, deportation, and enforcement decision-making.
- Analyzing campaign contributions, lobbying expenditures, and political influence operations carried out by technology corporations and their lobbyists, including how those relationships shape procurement policy, cloud infrastructure decisions, and immigration enforcement priorities.
- Investigating the revolving door between senior DHS officials, intelligence agencies, defense contractors, and technology corporations involved in immigration enforcement and domestic surveillance systems.
- Advancing federal legislation limiting biometric data collection, restricting data sharing between federal agencies and private corporations, strengthening whistleblower protections, and prohibiting federal contracts with companies engaged in unlawful surveillance or civil rights violations.

- Developing strategies to reduce federal dependence on private technology contractors by challenging no-bid contracts, demanding procurement transparency, and exposing how deeply embedded private companies have become within core government operations.

Federal policy change will not emerge automatically from shifts in electoral politics alone. It will require years of groundwork, investigative pressure, public education, coalition-building, and movement infrastructure capable of translating moments of political opportunity into structural change. Technology corporations and federal contractors have enormous financial and political incentives to keep these systems hidden, normalized, and profitable. Millions of dollars are spent on lobbying, campaign contributions, procurement influence, and public relations efforts designed to protect these contracts and prevent meaningful oversight. Communities, advocates, researchers, and elected officials willing to confront these systems will therefore need to fight not only for new policy, but for transparency itself by exposing the corporations driving enforcement infrastructure, documenting the harms these systems produce, and building enough public pressure to overcome the political influence of the surveillance industry.

Understand the Systems to Fight Them

This report offers a dark and challenging assessment of this moment. But we provide this information to ground us in what is at stake, so that we can envision and build a future which values all life and the planet.

Movements resisting surveillance and immigration enforcement must develop a much deeper understanding of the technologies we are confronting, and the power that circulates through them. The current fusion of state and corporate power driving technologies that foster authoritarianism and exclude and repress everyday people, requires that we challenge oligarchs and the ways that they are fundamentally changing the way our democracy operates.

Communities and organizations should create intentional spaces to collectively study and investigate these technologies together. Advocates can no longer afford to organize against immigration policing or criminalization while treating technology as neutral. Political education gatherings, research collaboratives, community audits, and local strategy convenings can help residents, organizers, technologists, journalists, and legal advocates better understand which surveillance tools are operating in their cities, who owns them, how data flows between agencies and corporations, and where local pressure points exist.

Mapping the local impact of these systems can help communities identify which corporations hold contracts with nearby governments, where data centers or offices are located, which public institutions are purchasing surveillance technologies, and what local policies or campaigns could interrupt their expansion. Understanding how these systems work on the ground is therefore essential for effective organizing.

Communities should investigate where local agencies obtain data, how information flows between agencies and contractors, what technologies officers use during raids and investigations, and how surveillance tools are integrated into everyday governance systems like schools, jails, public benefits programs, courts, and transportation infrastructure. This also means building stronger relationships between organizers, researchers, technologists, journalists, lawyers, and workers inside these systems who can help expose how technologies function in practice. Technical literacy should not be treated as a niche specialization reserved for experts. It is now a core organizing skill necessary for defending communities against increasingly digital forms of policing, repression and state control.

A note for those organizing: It is critical that our organizing does not get trapped in narrow debates about how to "improve" or "reform" DHS or ICE. Demanding body cameras, more training, or new oversight mechanisms will not protect our communities from a system built on surveillance, punishment, and removal. These reforms often leave the machinery intact while making it more durable. Our work must continue to shift the public conversation toward the deeper problem: the idea

that some people are disposable and therefore legitimate targets of state violence. This logic shows up in familiar narratives like "the worst of the worst," which are used to justify increasingly extreme policing, detention, and deportation. That framing matters because the infrastructure being built under immigration enforcement is increasingly being used against anyone demanding fairness, equality, and democracy—from peaceful protesters and journalists to lawyers, workers, and communities resisting corporate power. Local organizing must keep making these connections clear.

This Report is a Movement Offering

We wrote this report as an offering to our movements—to sharpen how we understand what we're up against, and strengthen our ability to fight back.

This report is for the frontlines: A tool to carry into meetings with elected officials and government agencies, to ask the hard questions, challenge public contracts, and demand accountability. Organizers can use it to identify the next targets for organizing and disruption. Workers inside these companies can use it to challenge what is being built, raise critical questions, and expose the systems operating from within. Government officials can use it to examine the contracts they hold, identify what must be renegotiated or ended, and take concrete steps to limit the expansion of surveillance and deportation infrastructure. This is for people making safety plans, building campaigns, and confronting ICE abuse. Use it, adapt it, share it—together we can build systems that protect dignity, expand freedom, and keep our communities safe.

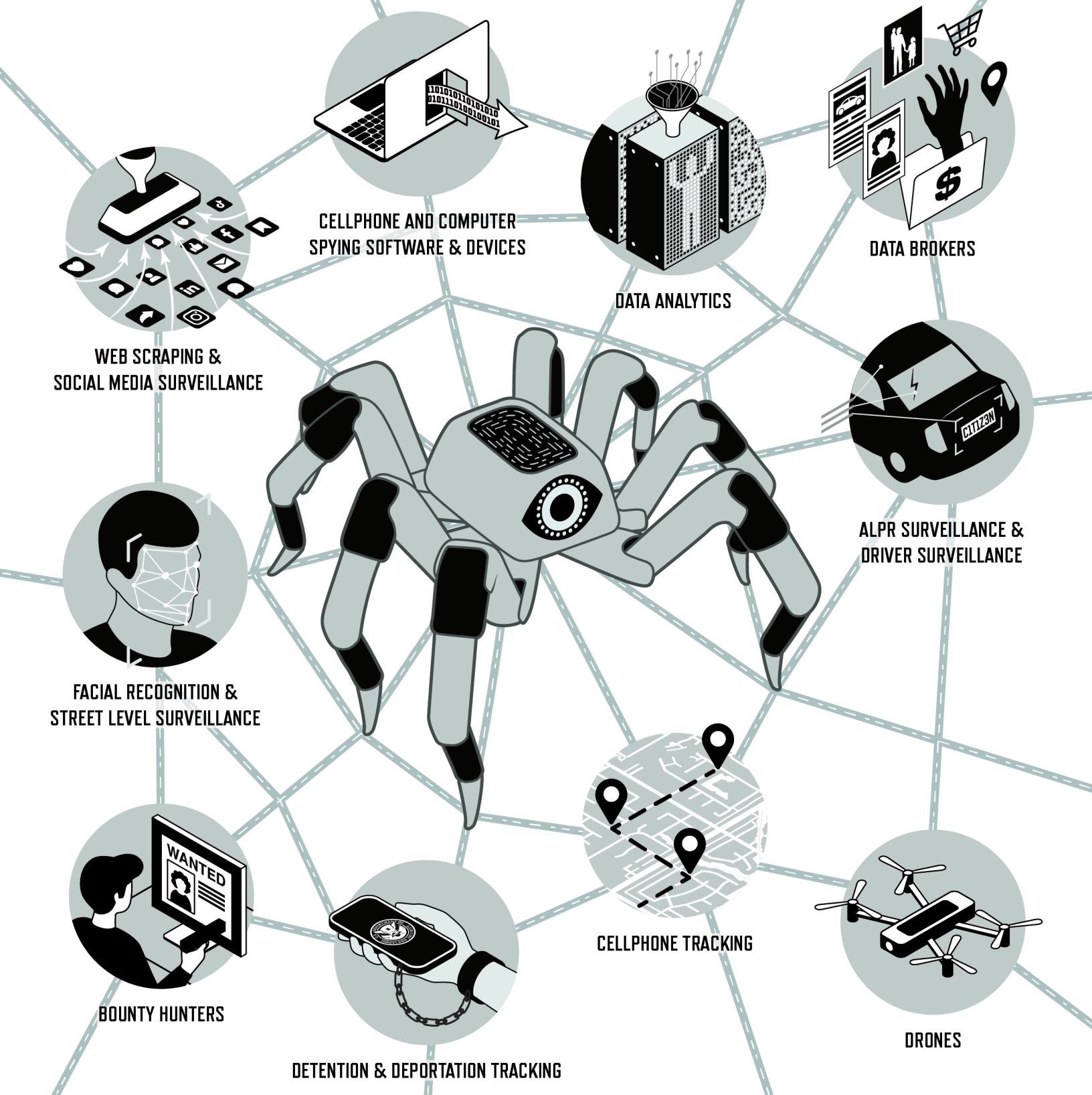
The systems in this report may be vast, but they are not untouchable. They rely on contracts, data flows, political decisions, and public consent—all of which can be challenged, disrupted, and dismantled. Across the country there are people already fighting every day: advocating for policies to stop data sharing with their local elected officials, in community spaces where people are sharing information with each other about the systems and policies that impact them, at the protests and campaigns against the building of data centers, and working in solidarity with human right defenders and journalists being targeted for their work. We must keep these fights at the forefront of our analysis to understand that it is possible to fight the oligarchs and DHS's vision of a future of control and abuse through community power and organized resistance.

List of Acronyms

AI	Artificial Intelligence
ALPR	Automated License Plate Reader
ATD	Alternatives to Detention
CBP	Customs and Border Protection (part of DHS)
DEA	Drug Enforcement Administration
DEI	diversity, equity, and inclusion
DHS	Department of Homeland Security
DOD	Department of Defense aka Department of War
DOJ	Department of Justice
FC/FR	Facial capture/facial recognition
HART	Homeland Advanced Recognition Technology system (DHS biometric data repository, successor to IDENT)
ICE	Immigration and Customs Enforcement (part of DHS)
ICE HSI	Homeland Security Investigations (part of ICE)
ICE ERO	Enforcement and Removal Operations (part of ICE)
ICM	Investigative Case Management (a Palantir product for ICE)
IDENT	Automated Biometric Identification System (DHS biometric repository, predecessor to HART)
OBIM	Office of Biometric Identity Management (part of DHS)
VC	venture capital

ICE's Top 10 Surveillance Technologies

A critical step in resisting the militarized policing and surveillance state is to understand what technologies are involved. Here is a summary of the top 10 categories of surveillance technology that immigration agencies like DHS, ICE, and CBP use to target, criminalize, and deport communities.



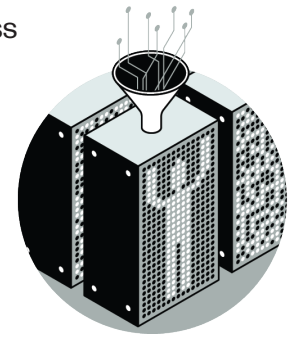
1. Data Brokers



Data brokers are companies that acquire massive quantities of data from thousands of sources and sell the information to housands of customers—including ICE. The data, sourced from both government records and private companies, includes phone numbers, addresses, vehicle registration data, property records, social media information, jail data, and more. Data brokers are a key tool for DHS and ICE to circumvent sanctuary city protections. For example, DHS and ICE have intentionally turned to these private companies to buy up data about local residents, even in jurisdictions where local policy prohibits cooperation or information sharing with ICE.

- ICE's $23 million contract with data broker **LexisNexis** gives ICE access to billions of records on more than 290 million US residents—covering **over 95% of US adults.** ICE uses the data to build detailed profiles on people, their families and networks to fuel deportation efforts. In 2021, ICE conducted over 1.2 million people searches on LexisNexis during just a seven-month period.

2. Data Analytics and Databases



While data *brokers* sell access to raw data, data *analytics* companies aggregate, sort, and find patterns in the data so that ICE can use it to deport and detain on a mass scale.

Palantir is the backbone of ICE data surveillance. Since 2014, ICE has used Palantir technology to analyze data, conduct targeting and raids, and facilitate data sharing with other policing agencies. Palantir's multi-year contract with ICE is now worth up to $176.5 million after ICE added more than $86 million for new surveillance technologies since April 2025. This includes:

- **ImmigrationOS,** a deportation surveillance platform that prioritizes people to deport and tracks "self-deportations" in real time. The platform fuses data from Social Security files, IRS tax data, license plate reader camera data and other sources, promising to create "near real-time visibility" into the movement of migrants in the US.
- **ELITE**, an app that populates a map with the location of potential deportation targets, including a "confidence score" on each person's address. ICE reportedly uses ELITE to identify neighborhoods to raid. The app pulls address data for ICE from various sources, including the Department of Health and Human Services.

3. Web Scraping and Social Media Surveillance



An entire industry makes money by "scraping" the internet to extract data about people—without our full knowledge or consent. Data culled from internet and social media surveillance provides a close look into someone's online (and offline) life, including their relationships, communications, and daily routines. Immigration agents rely on this data to profile and target people. For example:

- ICE and CBP use surveillance products from **Babel Street,** a social media monitoring company that allows customers to search a name, email, or phone number and pull up associated social media posts, IP addresses, job history, and more. ICE reportedly uses **Babel's Locate X** product to monitor cell phones at specific locations (for example, at a protest).
- Since 2025, ICE uses **PenLink's Tangles,** an AI technology that scrapes the internet and "dark web" to create dossiers on people by linking social media activity, financial records, location data, and more. ICE also pays for **PenLink's PLX** technology that can intercept communications in real time using telecommunications data, social media, and more.

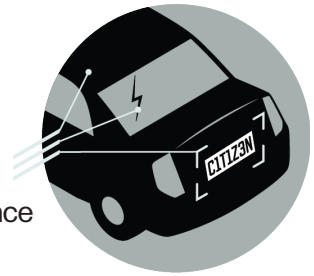
4. Facial Recognition + Street-Level Biometric Surveillance



DHS uses invasive technologies to track people based on unchangeable aspects of their body: their face, iris, fingerprint, DNA, or other "biometrics." Increasingly, ICE deploys biometric technologies in our streets and neighborhoods to intimidate and threaten communities. Two of ICE's key facial recognition technologies include:

- **Mobile Fortify** is ICE's facial recognition phone app for real-time "identity checks" on community members. After snapping an image of someone's face, fingerprints, or identity documents in the app, Mobile Fortify compares the image against hundreds of millions of records in CBP databases, including TSA PreCheck and Global Entry photos, passport and visa application photos, and more. If the app finds a "match"—which could be inaccurate—it will declare the person's name, birth date, whether they have a deportation order, and other personal data.[1]
- **ClearviewAI**'s $9.2 million contract provides ICE with facial recognition technology to investigate "assaults on law enforcement officers," among other things. A company with ties to Palantir co-founder Peter Thiel, Clearview claims to have over 70 billion photos in its database, which includes images scraped from Facebook, Twitter, LinkedIn, Venmo, and other sites.

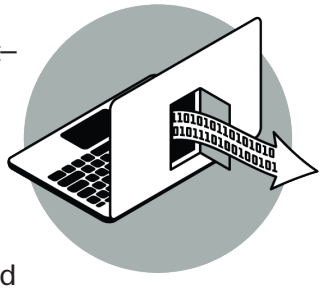
5. Nationwide Driver Surveillance



Nationwide, immigration and policing agencies surveil drivers by tapping into a deep network of **Automated License Plate Readers (ALPRs).** ALPRs are surveillance cameras that record each passing vehicle, often capturing not only the license plate number, but also the time and location, make and model of the vehicle, and photos of passengers. ALPRs are everywhere—from street corners to school campuses to Home Depot parking lots.

- **Flock Safety** deploys ALPR cameras in over 5,000 communities across the US. Flock gives law enforcement customers access to a nationwide Flock database, allowing policing agencies to search for any vehicle's real-time location or travel history. Although ICE has no contract with Flock, local police have conducted thousands of "side door" searches of Flock data on behalf of ICE.

6. Hacking Devices and Spyware



After confiscating a phone—for example, during an arrest—law enforcement agencies use "digital forensic" technologies to bypass passcodes and encryption, unlock a device, and extract its contents, including deleted messages, photos, location histories, call logs, and more. In 2025 alone, ICE and CBP secured 13 contracts for device hacking technologies from companies like **Cellebrite** and **Magnet Forensics (GrayKey).** ICE can use these technologies to conduct warrantless searches of phones seized during raids or protests, sweeping up data not only from targets but also their friends, family, and communities.

1 ICE officials have stated that they consider an identity "match" in Mobile Fortify to be a "'definitive" determination of a person's citizenship status and that an ICE officer may ignore a birth certificate or other evidence of US citizenship if the app states otherwise. In other words, even if you were to provide evidence of citizenship, ICE will defer to the determination of the app.

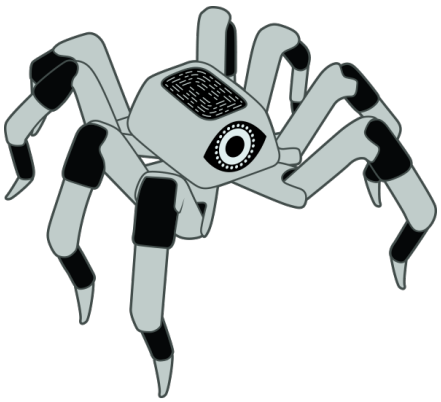
- In addition, ICE uses spyware. ICE recently contracted with **Paragon Solutions** and questions remain as to whether the agency still has access to this spyware tool or another commercial spyware. Paragon's **Graphite** spyware can *remotely* hack into a phone, activate it as a listening device, read encrypted messages from apps like Signal or WhatsApp, and more—all without the user ever clicking a link, or knowing that they are being spied on.

7. Cellphone Tracking and Location Data



DHS uses multiple channels to access location data siphoned off cell phones. For example:

- **Stingrays/cell site simulators:** These devices impersonate cell towers, forcing nearby phones to connect to them and sweeping up their location data. Sometimes, these devices can intercept calls, texts, and internet traffic.
- **Online advertising data:** CBP is now tapping into "adtech" data—location data sourced, in real-time, from ordinary cell phone apps like games, dating apps, and fitness trackers.
- **Administrative subpoenas:** Often without a warrant, ICE sends these requests to companies like Verizon, AT&T, Google, and Instagram to demand private account data on specific customers or users—including IP address or location data.



8. "Skip Tracing" and "Bounty Hunters"



"Skip tracing" traditionally refers to when debt collectors track down people who have "skipped out" on financial obligations. However, ICE pays **"skip tracing"** vendors to locate tens of thousands of people the agency is targeting for deportation. These contractors deploy a vast surveillance toolkit—data brokers, public records, social media data, and even physical reconnaissance—to track down information. ICE structures payments around "success" rates, incentivizing "bounty hunters" to procure phone numbers, social media footprints, and even photographic evidence of a person's private life. In 2025, ICE's 15 different contracts for "skip tracing" services totaled over $55 million, with more than $1 billion in potential contract money.

9. Detention and Deportation Tracking Apps



ICE subjects over 180,000 people to digital surveillance through its "Alternatives to Detention" (ATD) program. Framed as an "alternative" to brick and mortar prison, ATD instead expands ICE's system of punishment via "digital prisons." For example, **Geo Group** subsidiary **B.I. Inc**, the company that runs the ATD program for ICE, uses location tracking and facial recognition to monitor people in ATD through a phone app (**SmartLINK**) and a wrist-worn surveillance device (**VeriWatch**).

- In addition, **CBP's** recently rebranded **Home app** sends migrants and asylum seekers punitive, threatening instructions to "leave now" or face arrest. By April 2025, DHS reportedly revoked parole status for nearly one million migrants who had entered the US using the app, giving them seven days to self-deport or be arrested.

10. Border Towers and Drones



Hundreds of surveillance towers permeate the border, towering up to 140 feet high and equipped with technology to identify people seven miles away. Peter Thiel-backed **Anduril Industries** raked in $363.4 million from CBP in the first half of 2026 alone for **"autonomous" border towers**, which use machine learning to scan the border and identify people and items of "interest" to border agents. CBP plans to install 1,500 more towers in the next few years.

DHS also uses **drone surveillance**—at the border, at events like the 2026 FIFA World Cup, and at protests nationwide. CBP operates around 500 small drones from companies like **Red Cat Holdings (Teal Drones)** and **Skydio.** Some of these drones claim to detect people from 7.5 miles away and identify them from a mile away. During the past year, CBP and ICE used drones to surveil protests, including anti-ICE demonstrations in Chicago and Los Angeles.[1]

*Source: **"The Tech Behind ICE,"** Mijente, Just Futures Law, Surveillance Resistance Lab, June 2026,* https://notechforice.com/tech-behind-ice/

1 Meanwhile, as DHS expands its drone surveillance, it is simultaneously creating new federal airspace restrictions on the use of civilian drones, preventing journalists and the public from documenting ICE operations.

Endnotes

1 Mijente, Immigrant Defense Project, and National Immigration Project of the National Lawyers Guild. *Who's Behind ICE? The Tech and Data Companies Fueling Deportations*. 2018. https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.

2 Center for Constitutional Rights. "ICE Recruits Journalists, Pols, Business Execs to Roleplay Agents at 'Citizens Academy' Programs, Documents Show." October 1, 2024. https://ccrjustice.org/home/press-center/press-releases/ice-recruits-journalists-pols-business-execs-roleplay-agents.

3 Discovery documents, including text chains and immigration charging documents for MJMA and Victor Cruz Gamez v. Hermosillo et al, Case No. 25-cv-02011-MTK, https://innovationlawlab.org/sites/default/files/2026-03/MJMA%20Petr%20Exhibits.pdf in https://innovationlawlab.org/case/m-j-m-v-wamsley.

4 Sam Levin, "Video Shows ICE Arresting Oregon Farm Workers and Using Facial Recognition." https://www.theguardian.com/us-news/2026/may/21/ice-immigration-oregon-facial-recognition?utm_source=chatgpt.com, *British Broadcasting Corporation*, May 7, 2026.

5 Diane Lugo. "Woodburn Residents Say Oregon's Largest Hispanic Community under Attack from ICE." *Statesman Journal,* November 16, 2025. https://www.statesmanjournal.com/story/news/politics/2025/11/16/woodburn-oregon-traumatized-by-ice-raids/87201709007/.

6 Levin, "Video Shows ICE Arresting Oregon Farm Workers."

7 Aaron Bady. "How the US Exported Its Border Around the World." *The Nation*, August 20, 2019. https://www.thenation.com/article/archive/todd-miller-new-book-empire-of-borders-interview/.

8 Bobby Hunter and Victoria Yee. *Dismantle, Don't Expand: The 1996 Immigration Laws*. The Immigrant Justice Network and NYU School of Law Immigrant Rights Clinic, n.d. https://www.immigrantdefenseproject.org/wp-content/uploads/1996Laws_FINAL_Report_5.10.17.pdf.

9 Arun Kundnani. *The Muslims Are Coming! Islamophobia, Extremism, and the Domestic War on Terror*. Verso, 2015; Mizue Aizeki, "Multiplying State Violence in the Name of Homeland Security," in *Resisting Borders and Technologies of Violence,* Haymarket Books, 2023.

10 Jacob Knutson. "Minnesota Lawyers Argue Trump's ICE Invasion Is 'Extorting' State for Voter Rolls Demands." *Democracy Docket*, January 26, 2026. https://www.democracydocket.com/news-alerts/minnesota-attorneys-trump-bondi-ice-operation-extort-voter-rolls/.

11 Arwa Mahdawi. "Want a Green Card? Better Make Sure You Haven't Criticized Israel on Social Media." *The Guardian*, May 4, 2026. https://www.theguardian.com/commentisfree/2026/may/04/trump-green-card-israel-social-media.

12 Rebecca Santana. "Arrest of Palestinian Activist Stirs Questions about Protections for Students and Green Card Holders." *AP News*, March 10, 2025. https://apnews.com/article/mahmoud-khalil-immigration-ice-green-card-trump-deportation-eff078098165bbcd0d2bd315b1a7ca02.

13 Melissa Hellmann. "'It's Like They're Hunting': US Citizens and Legal Residents Report Increase in Racial Profiling by ICE." US News. *The Guardian*, January 22, 2026. https://www.theguardian.com/us-news/2026/jan/22/us-citizens-racial-profiling-ice.

14 Sam Levin. "ICE Violently Arrested a US Citizen and Filmed It 'like a Documentary', Videos Reveal." US News. *The Guardian*, May 15, 2026. https://www.theguardian.com/us-news/2026/may/15/ice-us-citizen-violent-arrest-documentary.

15 15 US §9401 - Definitions.

16 US Department of Homeland Security. "100 Days of Making America Safe Again." *Homeland Security*, April 29, 2025. https://www.dhs.gov/news/2025/04/29/100-days-making-america-safe-again.

17 Zolan Kanno-Youngs, Hamed Aleaziz, Christopher Flavelle, Emily Cochrane, and Glenn Thrush. "Stephen Miller Is Still Pursuing His Immigration Agenda, but More Quietly." *The New York Times*, April 5, 2026. https://www.nytimes.com/2026/04/05/us/politics/stephen-miller-immigration-agenda.html.

18 Muzaffar Chishti and Colleen Putzel-Kavanaugh. "The Trump Administration's Immigration Policies Encounter Resistance in the Courts." *Migration Policy Institute*, March 25, 2026. https://www.migrationpolicy.org/article/trump-courts-immigration

19 Center for Constitutional Rights. "The 9/11 Effect." https://ccrjustice.org/911-effect.

20 Jerod MacDonald-Evoy. "ICE Director Envisions Amazon-Like Mass Deportation System: 'Prime, but with Human Beings.'" *Arizona Mirror*, April 8, 2025. https://azmirror.com/2025/04/08/ice-director-envisions-amazon-like-mass-deportation-system-prime-but-with-human-beings/.

21 Melissa Sanchez and Mariam Elba. "'I Don't Want to Be Here Anymore': They Tried to Self-Deport, Then Got Stranded in Trump's America." *ProPublica*, October 10, 2025. https://www.propublica.org/article/trump-self-deportation-cbp-home-app.

22 Sanchez and Elba. "'I Don't Want to Be Here Anymore.'"

23 José Olivares. "Court Records Reveal Gutting of DHS Oversight: 'Incredibly Dangerous.'" US News. *The Guardian*, March 8, 2026. https://www.theguardian.com/us-news/2026/mar/08/dhs-oversight-court-record-review.

24 Lindsey Wilkinson. "DHS Watchdog Flags Lagging Mobile Device Security, Management." *FedScoop*, May 5, 2026. https://fedscoop.com/dhs-mobile-device-security-management-inspector-general-report/.

25 The immigration court system is not independent, but under the control of the executive branch and consequently complicates what is normally considered "due process". Since January 2025, the administration has politicized the courts, firing more than 113 immigration judges (https://www.reuters.com/legal/government/us-fires-more-immigration-judges-including-two-who-blocked-deporting-pro-2026-04-13/) The administratin is targeting those it views as favorable to protecting immigrant rights—and replacing them with military lawyers (https://www.brennancenter.org/our-work/analysis-opinion/using-military-lawyers-immigration-judges-ill-advised-and-potentially). The administration also created chaos in these courts by arresting people after their case was dismissed by government attorneys. Also see Jain, Amit, Bureaucrats in Robes: Immigration 'Judges' and the Trappings of 'Courts' (June 6, 2019). Georgetown Immigration Law Review, Vol. 33, No. 2, 2019, Available at SSRN: https://ssrn.com/abstract=3400493

26 Elizabeth Beavers. "Terrorizing Migrants: Five Ways Post-9/11 Legal Precedents Paved the Way for Anti-Immigrant Actions in the United States." *Brown University's Costs of War Project,* May 5, 2026. https://costsofwar.watson.brown.edu/paper/terrorizingmigrants.

27 The White House. "Securing Our Borders." January 21, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/securing-our-borders/.

28 Sofia Ferreira Santos. "Alien Enemies Act: The 1798 Law Trump Used to Deport Migrants." *BBC News,* September 3, 2025. https://www.bbc.com/news/articles/cy871w21d3vo.

29 The White House, "Securing Our Borders."

Ferreira Santos, "Alien Enemies Act."

30 "'You Have Arrived in Hell.'" *Human Rights Watch*, November 12, 2025. https://www.hrw.org/report/2025/11/12/you-have-arrived-in-hell/torture-and-other-abuses-against-venezuelans-in-el.

31 Center for Constitutional Rights. "What We Do: Khalil v. Trump." https://ccrjustice.org/home/what-we-do/our-cases/khalil-v-trump.

Debbie Nathan. "The Insidious Doctrine Fueling the Case Against Mahmoud Khalil." *Boston Review*, 2025. https://www.bostonreview.net/articles/the-insidious-doctrine-fueling-the-case-against-mahmoud-khalil/.

32 The White House. "Designating Antifa as a Domestic Terrorist Organization." September 22, 2025. https://www.whitehouse.gov/presidential-actions/2025/09/designating-antifa-as-a-domestic-terrorist-organization/.

33 The White House, "Designating Antifa as a Domestic Terrorist."

34 The White House. "Countering Domestic Terrorism and Organized Political Violence." September 25, 2025.

https://www.whitehouse.gov/presidential-actions/2025/09/countering-domestic-terrorism-and-organized-political-violence/.

35 The White House. "United States Counterterrorism Strategy," May 2026.

https://www.whitehouse.gov/wp-content/uploads/2026/05/2026-USCT-Strategy-1.pdf.

The memo further states that "[w]e will use all the tools constitutionally available to us to map them at home, identify their membership, map their ties to international organizations like Antifa, and use law enforcement tools to cripple them operationally before they can maim or kill the innocent. We will do the same with the state sponsors of such groups and those governments undertaking lethal plots on U.S. soil or against Americans anywhere."https://www.whitehouse.gov/wp-content/uploads/2026/05/2026-USCT-Strategy-1.pdf

36 Just Futures Law. "JFL, AIC v USCIS, DHS (Vetting Immigration Benefit Applicants FOIA)." *Just Futures Law,* March 27, 2026. https://www.justfutureslaw.org/legal-filings/foiatps-p43te.

Camilo Montoya-Galvez. "U.S. Probing Immigration Applicants' Social Media to Identify 'Anti-American' Activity That's 'Beyond the Pale,' Official Says." *CBS News*, October 16, 2025. https://www.cbsnews.com/news/immigration-social-media-anti-american-uscis-joseph-edlow/.

37 Willa Pope Robbins. "Trump DOJ Seeks Names of Social Media Users Critical of ICE." *Mediaite*, May 28, 2026. https://www.mediaite.com/media/news/trump-doj-seeks-names-of-social-media-users-critical-of-ice/.

38 Whitney Curry Wimbish. "A Running Count of How Many People ICE Has Killed and Injured." *The American Prospect*, January 29, 2026. https://prospect.org/2026/01/29/ice-trump-killed-injured-list-dhs-cbp-border-patrol-renee-good-alex-pretti/.

39 Ximena Bustillo. "Immigration Detention on Track for Deadliest Fiscal Year Since 2004." Immigration. *NPR*, March 10, 2026. https://www.npr.org/2026/03/10/g-s1-111238/immigration-detention-deaths-custody.

Casey Tolan Bartlett-Imadegawa, Rob Kuznia, Priscilla Alvarez, Audrey Ash, Catherine E. Shoichet, Michael Williams, Rhyannon. "How Understaffing and DHS Policy Drives Rising Deaths in ICE Detention Centers." *CNN*, May 15, 2026. https://www.cnn.com/2026/05/15/us/ice-immigration-detention-centers-medical-care-deaths-invs-vis.

40 Jon Schuppe and Erik Ortiz. "Trump's DHS Immigration Enforcement Officers Shot 14 People from September 2025 to February 2026. Here's What to Know." *NBC News*, March 4, 2026. https://www.nbcnews.com/news/us-news/ice-shootings-list-border-patrol-trump-immigration-operations-rcna254202.

41 Laura Strickler. "As Immigrant Deaths in Custody Grow, ICE Reduces What Details Are Made Public." *NBC News,* April 15, 2026. https://www.nbcnews.com/politics/immigration/immigrant-deaths-custody-grow-ice-reduces-details-are-made-public-rcna331852.

42 Rebecca Santana. "After Major Enforcement Operations, the Trump Administration Recalibrates Its Immigration Crackdown." *AP News,* May 1, 2026. https://apnews.com/article/immigration-ice-border-trump-mass-deportations-77ca6741fe11ac35852c8b15d3016991.

Colleen Heild. "DOJ Sues New Mexico, Albuquerque over Sanctuary Policies." *Albuquerque Journal*, May 9, 2026. https://www.yahoo.com/news/articles/doj-sues-mexico-albuquerque-over-030200238.html.

Office of Public Affairs. *Justice Department Publishes List of Sanctuary Jurisdictions*. US Department of Justice, 2025. https://www.justice.gov/opa/pr/justice-dep.

The White House. "Protecting American Communities from Criminal Aliens." April 28, 2025. https://www.whitehouse.gov/presidential-actions/2025/04/protecting-american-communities-from-criminal-aliens/.

43 The White House, "Protecting American Communities."

44 Christian Paz, "The White House's Shocking Lies About Minneapolis." *Vox*, January 28, 2026, https://www.vox.com/politics/476807/ice-dhs-cbp-bovino-immigration-stephen-miller-kristi-noem-alex-pretti-nicole-good-mislead-truth. See also Jake Rodriguez, "Federal Agents Search Homes of Ventura County ICE Watch Volunteers." *hoodline,* May 15, 2026, https://hoodline.com/2026/05/early-morning-raids-target-ventura-ice-watch-volunteers/. Lawsuits brought against DHS, CBP or ICE for violations in Illinois (*Case Summary of State of Illinois v. Department of Homeland Security,* Civil Rights Litig. Clearinghouse, https://clearinghouse.net/case/47682/ (last updated 3/12/2026) and Minnesota (Tincher et al v. Mullin, No. 0:25-cv-04669 (D. Minn. 2026), https://www.courtlistener.com/docket/72047643/tincher-v-noem/).

45 Lydia Wheeler, "DOJ Backs Birthright Citizenship Curbs with 'Fringe' Scholarship." *Bloomberg Law*, May 14, 2025, https://news.bloomberglaw.com/us-law-week/doj-backs-birthright-citizenship-curbs-with-fringe-scholarship.

46 Department of Justice, "About the Office: Executive Office of Immigration Review." https://www.justice.gov/eoir/about-office.

47 Kyle Cheney, "Judges Across the Country Rebuke ICE for Defying Court Orders." *Politico*, January 30, 2026, https://www.politico.com/news/2026/01/30/ice-immigration-court-orders-00757894.

48 David J. Bier. "The Administration Misleads & Ignores Courts Most Often in Immigration Cases." *Cato Institute,* January 27, 2026. https://www.cato.org/blog/admin-misleads-ignores-courts-most-often-immigration-cases.

49 "Surge in Immigration Lawsuits Hits Record High in 2026." *Transactional Record Access Clearinghouse*, May 11, 2026, https://tracreports.org/reports/773/.

50 "How ICE Went Rogue: Analysis of the Legal Authorities Governing ICE." *American Immigration Council*, February 11, 2026. https://www.americanimmigrationcouncil.org/fact-sheet/ice-cbp-legal-analysis/.

Sara Tenenbaum. "Group Argues for Special Prosecutor to Investigate Possible Crimes during Chicago's Operation Midway Blitz." *CBS Chicago*, April 24, 2026. https://www.msn.com/en-us/news/crime/hearing-will-decide-if-special-prosecutor-investigates-possible-crimes-during-chicagos-operation-midway-blitz/ar-AA21DQlh.

51 Alina Das. "Protecting Immigrant Activists From U.S. Government Retaliation: Lessons From First Amendment Litigation." *Knight First Amendment Institute at Columbia University,* February 12, 2025. http://knightcolumbia.org/content/protecting-immigrant-activists-from-us-government-retaliation-lessons-from-first-amendment-litigation.

52 Peter Eisler, Ned Parker, Linda So, and Joseph Tanfani. "Trump's Campaign of Retribution: At Least 470 Targets and Counting." *Reuters,* November 26, 2025. https://www.reuters.com/investigates/special-report/usa-trump-retribution-tracker/.

53 Sam Levin. "DoJ Cases against Protesters Keep Collapsing as Officers' Lies Are Exposed in Court." US News. *The Guardian*, February 21, 2026. https://www.theguardian.com/us-news/2026/feb/21/doj-protesters-federal-agents-cases. See also Anderson, Meg. "The Trump Administration Is Increasingly Trying to Criminalize Observing ICE." *NPR*, February 18, 2026. https://www.npr.org/2026/02/18/nx-s1-5699708/ice-observers-impeding-obstructing-interfering.

54 Associated Press. "Justice Department Moves to Drop Charges Against Men Accused of Hitting Ice Officer in Minnesota." *The Guardian*, February 13, 2026. https://www.theguardian.com/us-news/2026/feb/13/justice-department-moves-to-drop-charges-alfredo-alejandro-aljorna-julio-cesar-sosa-celis-ice-minnesota.

55 Sarah N. Lynch. "Southern Poverty Law Center Seeks Dismissal of Criminal Charges, Saying Prosecution Is Vindictive." *CBS News,* May 26, 2026. https://www.cbsnews.com/news/southern-poverty-law-center-seeks-dismissal-criminal-charges-vindictive/.

56 Dennis Romero. "Judge Orders Federal Agents to Stop Pepper Spraying, Retaliating Against Peaceful Minnesota Protesters." *NBC*

News, January 17, 2026. https://www.nbcnews.com/news/us-news/us-judge-orders-federal-agents-stop-pepper-spraying-retaliating-peacef-rcna254514.

Ernesto Londoño. "Pepper-Sprayed While Pinned Down: A Searing Scene Provokes Outrage." *The New York Times,* January 23, 2026. https://www.nytimes.com/2026/01/23/us/minneapolis-man-pepper-sprayed-pinned-video.html.

J. David McSwane. "Two CBP Agents Identified in Alex Pretti Shooting." *ProPublica*, February 1, 2026. https://www.propublica.org/article/alex-pretti-shooting-cbp-agents-identified-jesus-ochoa-raymundo-gutierrez.

57 Nick Turse. "Pam Bondi Admits DOJ Has a Secret Domestic Terrorist List." *The Intercept,* February 12, 2026. https://theintercept.com/2026/02/12/pam-bondi-domestic-terror-list-nspm-7/.

58 Ken Klippenstein. "Trump's NSPM-7 Labels Common Beliefs As Terrorism 'Indicators." September 27, 2025. https://www.kenklippenstein.com/p/trumps-nspm-7-labels-common-beliefs.

59 Lisa Hornung. "Board of Immigration Appeals Rules Mahmoud Khalil Can Be Deported." *UPI*, April 10, 2026. https://www.upi.com/Top_News/US/2026/04/10/board-immigration-appeals-mahmoud-khalil-deported/9741775835407/.

60 Luc Cohen. "Judge Dismisses Kilmar Abrego Indictment, Says DOJ Abused Power." *KSL*, May 23, 2026. https://www.ksl.com/article/51501529/judge-dismisses-kilmar-abrego-indictment-says-doj-abused-power.

61 US Department of Homeland Security. "AI Use Case Inventory Library." Accessed June 3, 2026. https://www.dhs.gov/publication/ai-use-case-inventory-library.

62 Jon Collins. "Drone Sightings Drove Surveillance Fears as ICE Surged in Minnesota." *MPR News*, March 13, 2026. https://www.mprnews.org/story/2026/03/13/minnesota-drone-sightings-drove-surveillance-fears-as-ice-surged.

Howard Altman. "Massive Drone No-Fly Zone Imposed Over Greater Chicago Area (Updated)." *The War Zone,* October 2, 2025. https://www.twz.com/air/massive-drone-no-fly-zone-imposed-over-greater-chicago-area.

63 Fox News. "Homan Pushes to Create 'Database' to Make Those Who Impede ICE 'Famous.'" January 15, 2026. https://www.foxnews.com/video/6387789141112.

64 United States Government Accountability Office. *Artificial Intelligence Acquisitions: Agencies Should Collect and Apply Lessons Learned to Improve Future Procurements.* 2026. https://www.gao.gov/assets/gao-26-107859.pdf.

65 Palantir. "Letter to Shareholders." February 2, 2026.

https://www.palantir.com/q4-2025-letter/en/. See also Matt Novak, "Palantir CEO Insists He Doesn't Support Regime Change Wars (But Supports Iran War)." *Gizmodo*, March 12, 2026. https://gizmodo.com/palantir-ceo-insists-he-doesnt-support-regime-change-wars-but-supports-iran-war-2000732971. (see quote in interview to CNBC, "No one believes it, but Palantir is the most important protector of the Fourth Amendment…" said Alex Karp.)

66 Katya Schwenk. "Big Tech Oversees Itself at Homeland Security." *Jacobin*, March 7, 2026. https://jacobin.com/2026/03/dhs-anduril-biometric-surveillance-tech.

Submission to Request for Comments: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum, OMB-2023-0020-0001. 2023. https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/65708cac891a5f0f0bdbcaa0/1701874860251/OMB+AI+Comments+-+DHS++and+law+enforcement.pdf.

67 *Submission to Request for Comments*

68 *Submission to Request for Comments*

69 Sheera Frenkel and Aaron Krolik. "How ICE Already Knows Who Minneapolis Protestors Are." *The New York Times*, January 31, 2026. https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html.

70 Christopher Brown. "Maine ICE Protesters Sue Noem, Claiming First Amendment Wrongs." *Bloomberg Law,* February 23, 2026.

https://news.bloomberglaw.com/litigation/maine-ice-protesters-sue-noem-claiming-first-amendment-wrongs.

71 Ashley Belanger. "ICE's Forced Face Scans to Verify Citizens Is Unconstitutional, Lawmakers Say." *Ars Technica,* October 29, 2025. https://arstechnica.com/tech-policy/2025/10/ices-forced-face-scans-to-verify-citizens-is-unconstitutional-lawmakers-say/.

72 Jude Joffe-Block. "A New Lawsuit Alleges DHS Illegally Tracked and Intimidated Observers." *NPR*, February 23, 2026. https://www.npr.org/2026/02/23/nx-s1-5722988/dhs-lawsuit-biometrics-domestic-terrorism. Emily Allen, "Maine ICE Observers Say Agents Threatened to Put Them on 'Domestic Terrorist' Watchlist." *Press Herald,* February 23, 2026. https://www.pressherald.com/2026/02/23/maine-ice-observers-sue-say-agents-threatened-to-add-them-to-a-database-of-domestic-terrorists-2/

Belanger, "ICE's Forced Face Scans."

73 Rivera, Mark, Barb Markoff, Christine Tressel, and Tom Jones. "Video Shows Immigration Agents Using Facial Recognition on Minors, Possibly Violating Illinois Law." *ABC7 Chicago,* January 22, 2026. https://abc7chicago.com/post/video-shows-immigration-agents-using-facial-recognition-minors-east-aurora-high-school-possibly-violating-illinois-law/18445490/.

74 State of Illinois and City of Chicago v. Department of Homeland Security et al., Complaint for Declaratory and Injunctive Relief, No. 26-cv-00321 (N.D. Ill. Jan. 12, 2026), 32. https://illinoisattorneygeneral.gov/News-Room/Current-News/001%20-%20Complaint%201.12.26.pdf?language_id=1

Markey et al. to Lyons, Nov. 3, 2025.

https://www.markey.senate.gov/imo/media/doc/follow-up_to_ice_on_frt.pdf

75 Julia Hornstein. "Palmer Lucky Told You So." *Business Insider,* December 18, 2025. https://www.businessinsider.com/palmer-luckey-america-worlds-gun-store-defense-tech-2025-12.

76 Mary Cunningham. "Wealth Inequality in America Just Hit Its Widest Gap in More than 3 Decades." *CBS News*, January 21, 2026,

https://www.cbsnews.com/news/us-wealth-gap-widest-in-three-decades-federal-reserve/.

77 Cunningham, "Wealth Inequality in America."

78 Oxfam International. "Billionaire Wealth Jumps Three Times Faster in 2025 to Highest Peak Ever, Sparking Dangerous Political Inequality." January 19, 2026. www.oxfam.org/en/press-releases/billionaire-wealth-jumps-three-times-faster-2025-highest-peak-ever.

79 Rachel Sandler. "Inside The Trillion Dollar Tech World." *Forbes,* November 10, 2021.

https://www.forbes.com/sites/rachelsandler/2021/11/10/inside-the-trillion-dollar-tech-factory/.

80 UBS Evidence Lab. *Heralding a New Era: How a New Generation of Billionaires Is Shaping Wealth in the US and Globally*. *UBS*, 2025. https://www.ubs.com/us/en/wealth-management/our-solutions/private-wealth-management/insights/billionaires-ambition-report.html.

81 Forbes. "The Top 10 Richest People in the World." June 2026."

https://www.forbes.com/sites/forbeswealthteam/article/the-top-ten-richest-people-in-the-world/

82 World Bank Open Data. "World Bank Open Data." Accessed June 9, 2026. https://data.worldbank.org.

83 Institute for Policy Studies, "Income Inequality."

https://inequality.org/facts/income-inequality/.

84 August Benzow, Kenan Fikri, Joanne Kim, and Daniel Newman. "Advancing Economic Development in Persistent-Poverty Communities." *Economic Innovation Group*, 2023. https://eig.org/persistent-poverty-in-communities/.

85 Institute for Policy Studies, "Income Inequality."

86 Danny Hakim. "A Look Inside the Case That Enshrined Political Pow-

er for Billionaires." *The New York Times,* May 7, 2026. https://www.nytimes.com/2026/05/06/us/politics/buckley-case-supreme-court-billionaires.html.

87 Tom Moore. *The Corporate Power Reset That Makes Citizens United Irrelevant*. American Progress, 2025. https://www.americanprogress.org/article/the-corporate-power-reset-that-makes-citizens-united-irrelevant/.

88 Jessica Piper. "Meet the New Power Players Raising Massive Money for the Midterms." *Politico*, April 17, 2025. https://www.politico.com/news/2026/04/17/ai-crypto-new-campaign-finance-players-00878049.

Donald Shaw. "Musk-Linked 'Dark Money' Group Got a $75 Million Anonymous Donation." *Sludge*, December 19, 2025. https://readsludge.com/2025/12/19/musk-linked-dark-money-group-got-a-75-million-anonymous-donation/.

89 Jamie Martin. "Review: Full Metal Racket." *Book Forum*, 2019. https://www.bookforum.com/print/2602/vc-an-american-history-by-tom-nicholas-22006

April Dembosky. "Silicon Valley Rooted in Backing from US Military." *Financial Times*, June 9, 2013. https://www.ft.com/content/8c0152d2-d0f2-11e2-be7b-00144feab7de.

90 Shana Marshall. "The Military Industrial Venture Capital Complex." *Security in Context,* December 27, 2023.

https://www.securityincontext.com/posts/the-military-industrial-venture-capital-complex.

91 US Department of War. "War Department Launches AI Acceleration Strategy to Secure American Military AI Dominance." January 12, 2026. https://www.war.gov/News/Releases/Release/Article/4376420/war-department-launches-ai-acceleration-strategy-to-secure-american-military-ai/.

92 Marlize van Romburgh. "Sector Snapshot: Defense Startup Funding Hits an All-Time Record as VCs Begin To Eye Exits." *Crunchbase News*, June 2, 2026. https://news.crunchbase.com/defense-tech/startup-venture-funding-all-time-record-ai-anduril/.

93 Sheera Frenkel. "Silicon Valley Bet on War. The Bets Are Paying Off." Technology. *The New York Times*, March 18, 2026. https://www.nytimes.com/2026/03/18/technology/silicon-valley-war-defense-tech.html

US Department of War. "FY 2027 Defense Budget." 2026. https://www.war.gov/Spotlights/FY2027-Defense-Budget/.

94 Alexandra G. Neenan. "Defense Primer: Department of Defense Contractors." *Congressional Research Service,* February 6, 2026. https://crsreports.congress.gov.

95 Palantir. "Careers." Accessed June 7, 2026. https://www.palantir.com/careers/.

96 Peter Thiel. "The Education of a Libertarian." *Cato Unbound*, April 13, 2009. https://www.cato-unbound.org/2009/04/13/peter-thiel/education-libertarian/.

97 Anduril Industries. "Rebooting the Arsenal of Democracy: Anduril Mission Document." *Anduril*, June 5, 2022. https://www.anduril.com/news/rebooting-the-arsenal-of-democracy-anduril-mission-document.

98 Palmer Luckey. "We Cannot Let Them Stay." *X*, January 20, 2026. https://x.com/PalmerLuckey/status/2013831417923567812.

99 Frenkel and Metz, "The Pentagon's Favorite Tech Guy."

100 Kenneth Niemeyer. "Palmer Luckey and Other Defense Tech Leaders See Trump's Victory as a Win for the Industry." *Business Insider,* November 10, 2024. www.businessinsider.com/palmer-luckey-anduril-trump-defense-tech-growth-2024-11.

Morris, Chris, "These Are the Companies JD Vance Has Invested in as a VC (and Beyond)." *Fast Company,* July 17, 2024. www.fastcompany.com/91157500/companies-jd-vance-invested-in-as-a-vc.

101 Adi Robertson. "Palmer Luckey Says He Donated to Pro-Trump Group, but Doesn't Support Trump." *CNBC*, September 24, 2016. https://www.cnbc.com/2016/09/24/palmer-luckey-says-he-donated-to-pro-trump-group-but-doesnt-support-trump.html.

Jeremy Stern. "Palmer Luckey, American Vulcan." *Tablet Magazine,* 2024. https://www.tabletmag.com/feature/american-vulcan-palmer-luckey-anduril.

102 Margaux MacColl. "Exclusive: From $19M to $1.5M, Here's How Much Anduril Pays Top Execs like Palmer Luckey in Cash and Stock." *TechCrunch*, November 26, 2024. https://techcrunch.com/2024/11/26/anduril-salaries-palmer-luckey-other-execs-how-much-do-they-make/.

103 Katherine Boyle. "Building American Dynamism." *Andreessen Horowitz*, January 14, 2022. https://a16z.com/building-american-dynamism/.

104 JD Vance. "Remarks by the Vice President at the American Dynamism Summit." The American Presidency Project, *UCSB*, March 18, 2025. https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-american-dynamism-summit.

105 PalantirTech. "Because We Get Asked a Lot. The Technological Republic, In Brief." *X,* April 18, 2026. https://x.com/PalantirTech/status/2045574398573453312. The White House, "President Trump Annouces Appointments to President's Council of Advisors on Science and Technology." March 25, 2026. https://www.whitehouse.gov/releases/2026/03/president-trump-announces-appointments-to-presidents-council-of-advisors-on-science-and-technology/

106 US Army Public Affairs. "Army Launches Detachment 201: Executive Innovation Corps to Drive Tech Transformation." *US Army,* June 13, 2025. https://www.army.mil/article/286317/army_launches_detachment_201_executive_innovation_corps_to_drive_tech_transformation.

107 Ashley Roque. "Army Undersecretary Nominee Faces Questions About Financial Ties to Anduril." *Breaking Defense*, May 8, 2025, https://breakingdefense.com/2025/05/army-undersecretary-nominee-faces-questions-about-financial-ties-to-anduril.

108 Marshall, "The Military Industrial Venture Capital Complex."

109 Naomi Klein. *The Shock Doctrine*. Henry Holt and Co., 2010, 379.

110 Quinn Slobodian and Ben Tarnoff. *Muskism: A Guide for the Perplexed*. Allan Lane, 2026, 41.

111 April Dembosky. "Silicon Valley Rooted in Backing from US Military." *Financial Times*, June 9, 2013. https://www.ft.com/content/8c0152d2-d0f2-11e2-be7b-00144feab7de.

112 Ben Tarnoff. "How the Internet Was Invented." *The Guardian*, July 15, 2016.

https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf.

113 Erik German. "Meet the CIA-Backed Venture Fund Behind Palantir, Anduril—and a Spy Tool That Might Be on Your Phone." *Fortune*, July 29, 2025. https://fortune.com/2025/07/29/in-q-tel-cia-venture-capital-palantir-anduril/.

114 US Department of War. "CDAO and DIU Launch New Effort Focused on Accelerating DOD Adoption of AI Capabilities." December 11, 2024. www.war.gov/News/Releases/Release/Article/3996199/cdao-and-diu-launch-new-effort-focused-on-accelerating-dod-adoption-of-ai-capab.

115 The White House. "President Trump Announces Appointments to President's Council of Advisors on Science and Technology." March 25, 2026. www.whitehouse.gov/releases/2026/03/president-trump-announces-appointments-to-presidents-council-of-advisors-on-science-and-technology.

116 Valerie Insinna. "Munitions at Risk? Inside the Pentagon's $350B Gamble." *Breaking Defense*, May 8, 2026. https://breakingdefense.com/2026/05/heres-whats-at-risk-if-the-pentagons-350b-reconciliation-gambit-fails.

Ashley Gate and William Hartung. "Donald Trump's Golden Dome Is a Ridiculous Boondoggle." *Jacobin,* November 20, 2025. https://jacobin.com/2025/11/trump-golden-dome-nuclear-defense.

117 Congressman Robert Garcia. "Letter to Inspector General Platte B. Moring." *US House of Representatives: Committee of Oversight and Government Reform*, May 28, 2026. https://oversightdemocrats.house.gov/imo/media/doc/2026-05-08garciatododigretrumpfamilycontracts.pdf.

118 Steven Brill. "Donald Trump, Palantir, and the Crazy Battle to Clean

Up a Multibillion-Dollar Military Procurement Swamp." *Fortune*, April 1, 2017. http://fortune.com/palantir-pentagon-trump.

Slobodian and Tarnoff, *Muskism.*

119 "Cuts to Woke Programs Fact Sheet." In *The President's FY 2026 Discretionary Budget Request, Budget of the United States Government, Fiscal Year 2026*. 2025. https://www.govinfo.gov/app/details/BUDGET-2026-BUD/BUDGET-2026-BUD-2/context.

120 Lindsay Koshgarian. "Trump's Budget Has Endless Funds for War, but Not Much to Help Americans." *National Priorities Project,* April 3, 2026. https://www.nationalpriorities.org/blog/2026/04/03/trumps-budget-has-endless-funds-war-not-much-help-americans/.

121 Hanna Homestead. "A Trillion Dollars for Wasteful Pentagon and No Money for Social Goods We Need and Want." *Common Dreams,* May 18, 2025. https://www.commondreams.org/opinion/1-trillion-pentagon-budget-social-needs.

122 Edward Helmore. "Trump Inauguration: Zuckerberg, Bezos and Musk Seated in Front of Cabinet Picks." *The Guardian*, January 20, 2025. https://www.theguardian.com/us-news/2025/jan/20/trump-inauguration-tech-executives.

Ali Swenson. "Trump, a Populist President, is Flanked by Tech Billionaires at his Inauguration." *Associated Press*, January 20, 2025. https://apnews.com/article/trump-inauguration-tech-billionaires-zuckerberg-musk-wealth-0896bfc3f50d941d62cebc3074267ecd.

Juliana Kim and Bobby Allyn. "Tech Moguls Altman, Bezos and Zuckerberg Donate to Trump's Inauguration Fund." *NPR*, December 13, 2024. https://www.npr.org/2024/12/13/nx-s1-5227874/trump-bezos-zuckerberg-amazon-facebook-open-ai-meta-inauguration-fund.

123 Lawrence Norden and Daniel I. Weiner. "The Rise of America's Broligarchy and What to Do About It." *TIME,* February 12, 2025.

time.com/7221154/rise-of-americas-broligarchy.

124 Brian Schwartz. "Peter Thiel's Picks Masters, Vance Split Key Senate Races in Arizona, Ohio After Billionaire Spent $32 Million on 2022 Midterms." *CNBC*, November 12, 2022. www.cnbc.com/2022/11/12/midterm-results-peter-thiel-picks-masters-vance-see-mixed-results-in-arizona-ohio.html.

125 Eric Revell. "Trump Secures Donations from Two Silicon Valley Venture Capital Billionaires." *Fox Business,* July 16, 2024. www.foxbusiness.com/politics/trump-secures-donations-two-silicon-valley-venture-capital-billionaires.

126 Michelle Goldberg. "Alex Karp Went from Biden Donor to Trump Enabler. Why?" *The New York Times*, November 11, 2025. https://www.nytimes.com/2025/11/10/opinion/alex-karp-palantir-trump.html.

127 Arjun Kharpal, "Corporate America Shelled Out Millions for Trump's Inauguration. Now He's Upending Many of their Businesses." *CNBC,* April 23, 2025. www.cnbc.com/2025/04/23/trump-inauguration-donors-include-meta-amazon-target-delta-ford.html.

128 US Federal Election Commission data.

129 Ashley Gold. "How AI Swallowed Tech Lobbying in 2025." *Axios*, January 23, 2026. http://www.axios.com/2026/01/23/ai-tech-lobbying-2025.

130 Hayden Field. "Scale AI Announces Multimillion-Dollar Defense Deal, a Major Step in US Military Automation." *CNBC*, March 5, 2026. www.cnbc.com/2025/03/05/scale-ai-announces-multimillion-dollar-defense-military-deal.html.

131 Jason Koebler and Joseph Cox. "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows." *404 Media*, May 27, 2025. www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows.

132 David Moore, "AI Boom on K Street: One in Four Lobbyists Now Work on AI," Sludge, March 11, 2026.

https://readsludge.com/2026/02/24/ai-boom-on-k-street-one-in-four-lobbyists-now-work-on-ai/

David Moore. "AI Lobbyists Are Flying Congressional Staffers Around the Country on Luxury Trips." *Sludge,* March 11, 2026. readsludge.com/2026/03/11/ai-lobbyists-are-flying-congressional-staffers-around-the-country-on-luxury-trips.

133 Moore, "AI Lobbyists Are Flying Congressional Staffers."

134 The White House. "Executive Order: Preventing Woke AI in the Federal Government." July 23, 2025. https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government/. Section IV(b)(i).

135 M-25-21 – AI innovation April 3 2025 OMB: https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf; M-25-22 – buying AI April 3, OMB : https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf

136 The White House. "America's AI Action Plan." Accessed July 2025. https://www.ai.gov/action-plan.

US Department of Homeland Security. "Department of Homeland Security Artificial Intelligence (AI) Strategy." September 2025. https://www.dhs.gov/sites/default/files/2025-09/25_0926_cio_dhs_ai_strategy_for_omb_m-25-21_508.pdf.

The White House. "Executive Order: Ensuring a National Policy Framework for Artificial Intelligence." December 11, 2025. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

Director Russell T. Vought. "M-26-04: Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles." *Executive Office of the President: Office of Management and Budget,* December 11, 2025. https://www.whitehouse.gov/wp-content/uploads/2025/12/M-26-04-Increasing-Public-Trust-in-Artificial-Intelligence-Through-Unbiased-AI-Principles-1.pdf.

The White House. "Ensuring a National Policy Framework for Artificial Intelligence." December 11, 2025. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

137 The White House, "Preventing Woke AI in the Federal Government." July 2025. https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government/.

138 The White House, "Winning the Race: America's AI Action Plan." July 2025.

https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

139 Connie Loizos. "David Sacks is Done as AI Czar — Here's What He's Doing Instead." *TedCrunch*, March 26, 2026.

https://techcrunch.com/2026/03/26/david-sacks-is-done-as-ai-czar-heres-what-hes-doing-instead/.

140 Allyn, "Trump Tech Adviser David Sacks."

141 George Packer, "The Venture-Capital Populist: How David Sacks and the New Tech Right Went Full MAGA and Captured Washington." *The Atlantic,* May 4, 2026.

https://www.theatlantic.com/magazine/2026/06/david-sacks-crypto-ai-venture-capital/686941/

142 The White House. "Ensuring a National Policy Framework for Artificial Intelligence."

143 Terry Gerton, "The Trump Administration's First United Agenda is Already Reshaping Federal Regulation," *Federa News Network,* October 29, 2025. https://federalnewsnetwork.com/agency-oversight/2025/10/the-trump-administrations-first-unified-agenda-is-already-reshaping-federal-regulation/.

144 Department of Homeland Security, "Department of Homeland Security Artificial Intelligence (AI) Strategy." September 7, 2025. https://www.dhs.gov/sites/default/files/2025-09/25_0926_cio_dhs_ai_strategy_for_omb_m-25-21_508.pdf.

145 The White House. "Fact Sheet: President Donald J. Trump Restores Common Sense to Federal Procurement." April 15, 2025. https://www.whitehouse.gov/fact-sheets/2025/04/fact-sheet-president-donald-j-trump-restores-common-sense-to-federal-procurement/.

The White House. "Ensuring Commercial, Cost-Effective Solutions in Federal Contracts." April 16, 2025.

https://www.whitehouse.gov/presidential-actions/2025/04/ensuring-commercial-cost-effective-solutions-in-federal-contracts/

146 The White House, "Fact Sheet: President Donald J. Trump Ensures a National Policy."

147 Allison Mollenkamp. "White House AI Framework Pushes for Broad Preemption of State Laws." *Governing*, March 13, 2026. www.governing.com/policy/white-house-ai-framework-pushes-for-broad-preemption-of-state-laws.

148 The Tech Buzz. "Trump Unveils Federal AI Framework Blocking State Regulations." March 20, 2026. www.techbuzz.ai/articles/trump-unveils-federal-ai-framework-blocking-state-regulations.

149 The White House, "Fact Sheet: President Donald J. Trump Ensures a National Policy." See also Taylor Penley. "White House AI Czar blasts blue states for inserting 'woke ideology' into artificial intelligence," Fox News, December 17, 2025. "We don't like seeing blue states trying to insert their woke ideology in AI models, and we really want to try and stop that."

https://www.foxbusiness.com/media/white-house-ai-czar-blasts-blue-states-inserting-woke-ideology-artificial-intelligence

150 "US Justice Department Steps in on Behalf of xAI in Colorado Regulation Case." *Reuters*, April 24, 2026. https://www.reuters.com/world/us-justice-department-intervenes-xai-challenge-colorado-tech-law-2026-04-24/.

151 Ryan Mueller. "Trump Taps Pam Bondi for AI Advisory Council Weeks After DOJ Exist and Epstein Files Backlash." *Business Times,* May 27, 2026. https://www.btimesonline.com/articles/177527/20260527/trump-taps-pam-bondi-for-ai-advisory-council-weeks-after-doj-exit-and-epstein-files-backlash.htm.

152 The White House. "Fact Sheet: The President's Working Group on Digital Asset Markets Releases Recommendations to Strengthen American Leadership in Digital Financial Technology." July 30, 2025. https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-presidents-working-group-on-digital-asset-markets-releases-recommendations-to-strengthen-american-leadership-in-digital-financial-technology.

153 Erin Doherty, Jasper Goodman, Jessica Piper, Daniel Barnes and Brendan Bordelon. "Poll: The Midterms' New Big Players are Pushing Agendas that Voters Don't Fully Support." *Politico*, May 3, 2026. www.politico.com/news/2026/05/03/poll-ai-crypto-super-pacs-voter-skepticism-midterms-00903376.

154 Matt Dixon. "'Slap In the Face': White House Irked By a New $100M Pro-AI Super PAC." *NBC News*, October 24, 2025. www.nbcnews.com/politics/trump-administration/white-house-irked-leading-future-new-100m-ai-super-pac-rcna239392.

155 US Federal Election Commission data.

156 US Federal Election Commission data. See: www.fec.gov/data/receipts/?data_type=processed&committee_id=C00916114.

157 Erin Doherty et al, "Poll: The midterms' new big players."

158 Karen Weise. "Big Tech's A.I. Spending Is Accelerating (Again)." *The New York Times,* October 31, 2025. www.nytimes.com/2025/10/31/technology/ai-spending-accelerating.html#:~:text=Concerns%20mushroomed%20this%20week%20after,$360%20billion%20in%20capital%20expenditures.

159 Mandy Taheri. "Map: Which States are Giving Biggest Tax Breaks for Data Centers." *Newsweek*, June 5, 2026. https://www.newsweek.com/map-which-states-are-giving-biggest-tax-breaks-for-data-centers-12038423.

Jasmine Laws and Daniel Orton. "Map Shows Where Data Centers Are Being Built in Drought-Hit Areas." *Newsweek*, May 29, 2026. https://www.newsweek.com/map-which-states-are-giving-biggest-tax-breaks-for-data-centers-12038423.

Isabel O'Brien, "Data Center Emissions Probably 662% Higher Than Big Tech Claims. Can It Keep up the Ruse?" *The Guardian*, September 15, 2024, https://www.theguardian.com/technology/2024/sep/15/data-center-gas-emissions-tech.

160 Valerie Volcovici. "Trump Administration Terminates 388 EPA Staff." *Reuters,* February 14, 2025, www.reuters.com/world/us/trump-administration-terminates-388-epa-staff-2025-02-14.

161 Bobby Allyn. "Trump Tech Adviser David Sacks Under Fire Over Vast AI Investments." *NPR*, December 13 2025. www.npr.org/2025/12/12/nx-s1-5631823/david-sacks-ai-advisor-investment-conflicts.

162 "David Sacks Net Worth Hits $2 Billion – Inside His Crypto Liquidation Strategy." *Capitaly,* September 19, 2025. https://www.capitaly.vc/blog/david-sacks-net-worth-hits--2-billion---inside-his-crypto-liquidation-strategy.

163 Revolving Door Project, "DOGE Agent: Marc Andreesen," February 21, 2025. therevolvingdoorproject.org/doge-andreessen-marc.

164 Forbes. "Real Time Billionaires." accessed June 21, 2026. https://www.forbes.com/real-time-billionaires/

165 Sheera Frenkel and Cade Metz. "The Pentagon's Favorite Tech Guy Is This Hawaiian Shirt-Wearing Founder." *The New York Times*, March 2, 2026, www.nytimes.com/2026/03/02/technology/pentagon-anduril-palmer-luckey.html.

166 Schwenk, "Big Tech Oversees Itself."

167 Forbes. "Real Time Billionaires." Accessed June 21, 2026.

168 U.S. Department of State. "Jacob Helberg." www.state.gov/biographies/jacob-helberg.

Revolving Door Project, "DOGE Agent: Gregory Barbaccia." Accessed June 9, 2026. therevolvingdoorproject.org/gregory-barbaccia-doge-agent.

"Barton Gellman." *Wellfound,* Accessed June 9, 2026. https://wellfound.com/p/jim-o-neill-1.

"Michael Kratsios." *The White House,* Accessed June 9, 2026.

https://trumpwhitehouse.archives.gov/people/michael-kratsios/.

Forbes. "Real Time Billionaires." Accessed June 21, 2026.

169 Jeff Rumage. "Inside Elon Musk's Government Contracts." With Ellen Glover. *Built In,* January 15, 2026. https://builtin.com/articles/elon-musk-government-contracts.

170 Forbes. "Real Time Billionaires." Accessed June 21, 2026.

171 US Federal Election Commission data, including contributions to Republican National Committee during presidential election cycle.

172 US Federal Election Commission data.

173 US Federal Election Commission data, donation to America PAC.

174 Arjun Kharpal. "Departed Creator of Facebook's Virtual Reality Headset Reportedly Donated $100,000 to Trump Inauguration." *CNBC*, April 20, 2017. www.cnbc.com/2017/04/20/palmer-luckey-oculus-facebook-donated-trump-inauguration.html.

175 US Federal Election Commission data.

176 US Federal Election Commission data, including contributions to Republican National Committee during presidential election cycle.

177 David Wright and Alex Leeds-Matthews. "Elon Musk Spent More Than $290 Million on the 2024 Election, Year-End FEC Filings Show." *CNN*, February 1, 2025. https://edition.cnn.com/2025/02/01/politics/elon-musk-2024-election-spending-millions.

178 US Federal Election Commission data, including contributions to the Republican National Committee during the presidential election cycle.

179 US Federal Election Commission data, including contributions to the Republican National Committee during the presidential election cycle.

180 Stephen Semler. "Trump's Budget: Starving Everything Except the Military." *Jacobin*, May 12, 2025. https://jacobin.com/2025/05/trump-2026-budget-cuts-military.

181 Center for Constitutional Rights, "ICE Recruits Journalists."

182 Aizeki. "Multiplying State Violence."

183 Brendan McQuade. *Pacifying the Homeland: Intelligence Fusion and Mass Supervision*. University of California Press, 2019.

184 "New Brief: Analysis Shows That ICE Has Deputized More Than 13,000 Local Law Enforcement Officers, and Promised Billions in Funding to Local Agencies Through Expanded 287(g) Program," Fwd.US Blog, February 16, 2026. https://www.fwd.us/news/new-brief-analysis-shows-that-ice-has-deputized-more-than-13000-local-law-enforcement-officers-and-promised-billions-in-funding-to-local-agencies-through-expanded-287g-program/.

US Immigration and Customs Enforcement. "ICE Awards Florida's State and Local Law Enforcement With 287(g) Funds to Defend the Homeland." September 26, 2025.

https://www.ice.gov/news/releases/ice-awards-floridas-state-and-local-law-enforcement-287g-funds-defend-homeland.

Meg Anderson. "ICE is Giving Local Police Big Money to Help with Immigration Enforcement," *OPB,* May 5, 2026. https://www.opb.org/article/2026/05/05/ice-is-paying-incentives-to-local-police-to-help-reach-trump-s-deportation-goals/.

185 "Secure Communities: A Fact Sheet." *American Immigration Council*, November 29, 2011. https://www.americanimmigrationcouncil.org/fact-sheet/secure-communities-fact-sheet/. American Immigration Council, "What's in the Secure America Act?," 10 June 2026, https://www.americanimmigrationcouncil.org/fact-sheet/whats-in-the-secure-america-act.

Krisna Avila and Lena Graber. "ICE Detainers Are Illegal: So What Does That Really Mean?" *Immigrant Legal Resource Center*, April 9, 2020. https://www.ilrc.org/ice-detainers-%20are-illegal-so-what-does-really-mean.

186 "New Brief: Analysis shows that ICE has Deputized," 2026

187 See: H.R. 1. 119th Congress (2025-2026)

188 Bill Chappell. "How ICE Grew to be the Highest-Funded US Law Enforcement Agency." *NPR*, January 21, 2026. www.npr.org/2026/01/21/nx-s1-5674887/ice-budget-funding-congress-trump.

189 Johana Bhuiyan. "Trump's Tax Bill Funds $6bn Expansion of US-Mexico Border Surveillance, Report Finds." *The Guardian*, July 15, 2025. www.theguardian.com/us-news/2025/jul/15/trump-tax-bill-border-immigration. Ximena Bustillo and Sam Gringlas, "ICE is now funded through end of Trump's term, raising worries about oversight," *NPR*, 10 June 2026, www.npr.org/2026/06/09/nx-s1-5851664/house-reconciliation-vote-immigration-enforcement-ice-border-patrol.

190 Michela Tindera. "Companies Reap $22 bn From Trump's Immigration Crackdown." *Financial Times,* January 29, 2026. www.ft.com/content/c74170d3-237d-459c-8642-bfd71530897d?emailId=30b85317-d0eb-4467-81c9-b7d27d458c2e&segmentId=69ce8bbf-afc9-7c01-fb70-6e4448aa1f37

Usaspending.gov search for CBP contracts in FY2025 and FY2026.

191 René Marsh and Audrey Ash. "DHS Says Its New Deportation Planes are Almost Ready for Takeoff. Critics doubt the Plan Will Work." *CNN,* May 16, 2026.

https://www.cnn.com/2026/05/16/politics/deportation-planes-dhs-fleet-airline.

192 Alex Woodward. "How ICE Turned Into Trump's Personal Police." *Independent*, March 27, 2026. https://www.independent.co.uk/news/world/americas/us-politics/trump-ice-tsa-airports-national-guard-b2948536.html.

193 Andrea Fuller, Albert Sun, and Eileen Sullivan. "ICE Hired Thousands While the Rest of the Immigration System Shrank." *New York Times*, February 11, 2026. https://www.nytimes.com/2026/02/11/us/ice-agents-hiring-immigration-system.html.

194 US Office of Personnel Management. "2026 Special Rates for Certain Law Enforcement Personnel." Last Modified 2026. https://www.opm.gov/policy-data-oversight/pay-leave/2026-special-rates-for-certain-law-enforcement-personnel/.

195 Nicole Ogrysko. "For DHS Workforce, 2025 Marked a Year of Major Change." *Federal News Network*, December 19, 2025. https://federalnewsnetwork.com/hiring-retention/2025/12/for-dhs-workforce-2025-marked-a-year-of-major-change/.

196 Margot Mendelson, Shanya Strom, and Michael Wishnie. *Collateral Damage: An Examination of ICE's Fugitive Operations Program.* Migration Policy Institute, February 2009. https://www.migrationpolicy.org/sites/default/files/publications/NFOP_Feb09.pdf.

197 Sen. Adam Schiff, "Armed for Violence." February 2026. www.schiff.senate.gov/wp-content/uploads/2026/02/ARMED-FOR-VIOLENCE-REPORT2.18.26.pdf.

198 Schiff, "Armed for Violence."

199 Center for Democracy & Technology and Lawyers' Committee for Civil Rights Under Law. "Immigration, DOGE, and Data Privacy: Explainer." May 9, 2025, PDF file, https://cdt.org/wp-content/uploads/2025/05/CDT-and-LCCHR-May-9-2025-Immigration-DOGE-and-Data-Privacy-Explainer.pdf. See also Kashmir Hill. "Social Security Data Shared with DHS to Target Immigrants/" *WIRED*, April 16, 2024. https://www.wired.com/story/social-security-data-shared-with-dhs-target-immigrants/.

200 Charlie Savage. "IRS Agrees to Share Tax-Return Data with Immigration Authorities, Aiding Deportations." *The New York Times*, April 8, 2025. https://www.nytimes.com/2025/04/08/us/politics/irs-ice-tax-data-deal.html.

201 Amna Nawaz and Matt Loffman. "Whistleblower Responds after DOJ Confirms DOGE Mishandled Social Security Data." *PBS Newshour*, January 27, 2026. https://www.pbs.org/newshour/show/whistleblower-responds-after-doj-confirms-doge-mishandled-social-security-data.

202 Nawaz and Loffman, "Whistleblower Responds."

203 Isaac Chotiner. "How 'DOGE' Russell Vought and Elon Musk Remade Office of Management and Budget." *The American Prospect*, February 5, 2026. https://prospect.org/2026/02/05/doge-russell-vought-elon-musk-office-management-budget/.

Steven Groves. ""Russell Vought Confirmation and Budget Issues." *AP News*, April 2025. https://apnews.com/article/trump-russell-vought-confirmation-budget-project-2025-7d1c476694176876256e95cecbd49231.

204 Makena Kelly and Victoria Elliot. "DOGE Isn't Dead. Here's What Its Operatives Are Doing Now." *Wired*, December 2, 2025. https://www.wired.com/story/what-is-doge-doing-now/.

205 Kevin Collier, "At Least 11 Lawsuits are Taking on DOGE Over Data Access and Privacy Laws." *NBC News,* February 19, 2025. https://www.nbcnews.com/tech/security/doge-lawsuits-11-cases-musk-group-focus-data-privacy-rcna191695.

Kelly and Elliott, "DOGE Isn't Dead."

206 Koshgarian, "Trump's Budget Has Endless Funds for War."

Geoff Hing. "How Encounters With Police Can Lead to Arrests—Even in Sanctuary Cities." The Marshall Project, September 5, 2025. https://www.themarshallproject.org/2025/09/05/florida-ice-arizona-police-colorado

207 Stephen Semler. "Trump's Budget: Starving Everything Except the Military." *Jacobin*, May 12, 2025. https://jacobin.com/2025/05/trump-2026-budget-cuts-military.

208 Empower LLC, with data from USAspending.gov and Crunchbase

209 "Companies Reap $22 bn From Trump's Immigration Crackdown." *Financial Times,* January 29, 2026. www.ft.com/content/c74170d3-237d-459c-8642-bfd71530897d?emailId=30b85317-d0eb-4467-81c9-b7d27d458c2e&segmentId=69ce8bbf-afc9-7c01-fb70-6e4448aa1f37

Empower LLC, with data from Usaspending.gov for CBP contracts in FY2025 and FY2026

210 Caroline Haskins. "All the Ways Big Tech Fuels ICE and CBP." *WIRED*, March 3, 2026. www.wired.com/story/how-big-tech-is-powering-trumps-immigration-crackdown.

211 Federal contracting data from USAspending.gov.

212 Empower LLC research found that Palantir, Skydio, and Databricks have received equity from In-Q-Tel, which has a formal DHS partnership (see: www.iqt.org/portfolio); Scale AI received funding from DHS Silicon

Valley Innovation Program (see: www.dhs.gov/science-and-technology/svip-portfolio); and Anduril and Shield AI have received contract award money from the SBIR program (see: www.sbir.gov/awards).

213 US Department of Homeland Security. "Office of Public-Private Partnerships." *Science and Technology Directorate,* June 5, 2026. https://www.dhs.gov/science-and-technology/office-public-private-partnerships.

214 Technologies include face authentication by iProov; presence analytics from CrowdVision and Kiana Analytics; and Small Unmanned Aircraft Systems (drones) from Shield AI, Echodyne, and others. See: DHS. "SVIP Portfolio and Performers." www.dhs.gov/science-and-technology/svip-portfolio.

215 US Small Business Administration. "DHS SBIR, Portfolio." Accessed June 10, 2026. www.sbir.gov/portfolio.

Paul Szoldra. "CIA Investment Vehicle in-Q-Tel Board Members Under Scrutiny." *Business Insider,* August 13, 2016. www.businessinsider.com/cia-vc-firm-conflict-of-interest-2016-8.

216 US Small Business Administration. "Portfolio Data: Anduril Industries Inc." Accessed June 10, 2026. www.sbir.gov/portfolio/1546735.

217 In-Q-Tel, 2025 Form 990.

218 In-Q-Tel, Portfolio, www.iqt.org/portfolio.

219 Contract award data from USAspending.gov. See: https://www.usaspending.gov/search?hash=22c260998e0900bc0d86f952fc369ade.

220 US Department of War. "Contracts for March 13, 2026." www.war.gov/News/Contracts/Contract/Article/4434754/contracts-for-march-13-2026.

221 Michael Steinberger. "From CIA Cash to Local Police: How Palantir Got its Start." *Yahoo Finance*, November 23, 2025. https://finance.yahoo.com/news/cia-cash-local-police-palantir-163513772.html.

222 (awarded to Idea Mind LLC and Intellisense Systems)

223 (awarded to Synthetik, Analytical AI, Toyon Research Corporation, and Intellisense Systems)

224 Jason Wilson. "Hacked Data Shines Light on Homeland Security's AI Surveillance Ambitions." *The Guardian,* March 15, 2026. www.theguardian.com/us-news/2026/mar/15/hacked-data-homeland-security. (awarded to Cassius LLC).

225 The text of the Advancing American AI Act at Section (b) of Sec. 7224 states: "Not later than 180 days after the date of enactment of this Act— (1) the Secretary of Homeland Security….shall issue policies and procedures for the Department related to—(A) the acquisition and use of artificial intelligence; and (B) considerations for the risks and impacts related to artificial intelligence-enabled systems, including associated data of machine learning systems, to ensure that full consideration is given to— (i) the privacy, civil rights, and civil liberties impacts of artificial intelligence-enabled systems; and (ii) security against misuse, degradation, or rending inoperable of artificial intelligence-enabled systems…" Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7224(a), 7224(d)(1)(B), and 7225 (codified at 40 U.S.C. 11301 note), https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf.

226 See: www.itdashboard.gov/agency-analysis.

227 US Department of the Treasury. "FY 2027 Budget Request Overview Book, PDF, FY2027, 3–9, https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2027/FY2027_Budget_Request_Overview_Book.pdf

228 Mijente and Just Futures Law. "Automating Deportation." June 2024. https://mijente.net/wp-content/uploads/2024/06/Automating-Deportation.pdf.

229 US Department of Homeland Security. "AI Use Case Inventory Library."

US Government Accountability Office. "Artificial Intelligence: Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity." February 2024. https://www.gao.gov/assets/d24106246.pdf, 6.

230 US Department of Homeland Security. "Department of Homeland Security Artificial Intelligence Roadmap." March 15, 2024. https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificial-intelligence-ciov3-signed-508.pdf, 5.

231 US Department of Homeland Security. "AI Use Case Inventory Library."

232 US Department of Homeland Security: Office of the Inspector General. "DHS Has Taken Steps to Develop and Govern Artificial Intelligence, But More Action is Needed to Ensure Appropriate Use." January 30, 2025. https://www.oig.dhs.gov/sites/default/files/assets/2025-02/OIG-25-10-Jan25.pdf?utm_source=chatgpt.com, 18.

233 *Pangea Legal Services et al v USCIS et al,* (1:24-cv-02809), District Of Columbia District Court, Filed: 10/03/2024; See: https://www.documentcloud.org/documents/28134750-2025-hqli-00002-6th-interim-response-records-sept-2025/#document/p73

234 Over 140 civil liberty groups raised concerns about the DHS AI inventory. Sign-on letter from organizations available here; https://www.justfutureslaw.org/aitech. See also Rachel Levinson-Waldman. "A Start for Transparency with Room to Grow." *Brennan Center*, January 22, 2025. https://www.brennancenter.org/our-work/analysis-opinion/start-ai-transparency-dhs-room-grow. See also: American Immigration Council. "Mission Creep: AI Surveillance at DHS Crosses Dangerous Line into Tracking Americans?" *American Immigration Council Blog*, Accessed June 5, 2026. https://www.americanimmigrationcouncil.org/blog/ice-ai-surveillance-tracking-americans.

235 Mijente and Just Futures Law, "Automating Deportation."

236 US Department of Homeland Security, "DHS Has Taken Steps to Develop and Govern," 14.

See also US Department of Homeland Security: Office of the Chief Information Officer. "DHS Playbook for Public Sector Generative Artificial Intelligence Deployment." January 2025. https://www.dhs.gov/sites/default/files/2025-01/25_0106_ocio_dhs-playbook-for-public-sector-generative-artificial-intelligence-deployment-508-signed.pdf.

237 Anthony Kimery. "Lawmakers Press DHS, ICE Over Palantir Surveillance Tools." *Biometric Update*, April 20, 2026. https://www.biometricupdate.com/202604/lawmakers-press-dhs-ice-over-palantir-surveillance-tools. See also Representatives Garamendi, Goldman, Velazquez, and Senator Wyden. "Reps. Garamendi, Goldman, Velazquez, & Sen. Wyden Demand Answers on ICE Use of Palantir-developed Technologies to Fuel Mass Surveillance." April 17, 2026.https://garamendi.house.gov/media/press-releases/reps-garamendi-goldman-velazquez-sen-wyden-demand-answers-ice-use-palantir.

238 US Government Accountability Office. "Artificial Intelligence: OMB Action Needed to Address Privacy-Related Gaps in Federal Guidance." March 26, 2026. https://www.gao.gov/products/gao-26-107681.

239 Lindsey Wilkinson. "ICE Work with AI Agents Is Minimal, CIO Says." *Fedscoop*, May 19, 2026. https://fedscoop.com/ice-agentic-ai-strategy-palantir-fbi/.

240 Schwenk, "Big Tech Oversees Itself."

241 US Department of Homeland Security: Office of the Chief Information Officer. "Department of Homeland Strategy for Artificial Intelligence (AI) Strategy for OMB M-25-21." September 26, 2025. https://www.dhs.gov/sites/default/files/2025-09/25_0926_cio_dhs_ai_strategy_for_omb_m-25-21_508.pdf, 7.

242 US Department of Homeland Security. "Office of Biometric Identity Management." Accessed June 6, 2026. https://www.dhs.gov/obim.

243 Erik German. "Meet the CIA-Backed Venture Fund Behind Palantir, Anduril, and a Spy Tool That Might be on Your Phone." *Fortune*, July 29, 2025. https://fortune.com/2025/07/29/in-q-tel-cia-venture-capital-palantir-anduril/.

244 USAspending.gov search for awards to Palantir.

245 USAspending.gov search for awards to Palantir.

246 IDIQ Contract W519TC25D0039, www.usaspending.gov/award/CONT_IDV_W519TC25D0039_9700. See also: Samantha Subin, "Palantir lands $10 billion Army software and data contract," *CNBC,* 1 August 2025, www.cnbc.com/2025/08/01/palantir-lands-10-billion-army-software-and-data-contract.html.

247 See: Contract no. 70CTD022FR0000170.

248 Blanket Purchase Agreement 70RTAC26A00000001, www.usaspending.gov/award/CONT_IDV_70RTAC26A00000001_7001.

249 Makena Kelly. "DHS Opens a Billion-Dollar Tab with Palantir." *Wired,* February 19, 2026. archive.ph/2026.02.19-170751/https://www.wired.com/story/department-homeland-security-ice-billion-dollar-agreement-palantir/#selection-689.0-689.44.

Makena Kelly. "Palantir Defends Work with ICE to Staff Following Killing of Alex Pretti." *Wired*, January 26, 2026. https://www.wired.com/story/palantir-ice-dhs-alex-pretti-killing-workers-slack-minneapolis/.

250 Miles Jamison. "Palantir Lands ICE Contract for ImmigrationOS Support." *Executive Gov,* October 15, 2025. www.executivegov.com/articles/palantir-ice-contract-immigrationos.

251 See: 1.5.1 ICE LSJ ICM Palantir-signed-REDACTED 1.8.26, govtribe.com, Limited Source Justification.

252 This graphic is based on research by Empower LLC, showing the increase in awards granted to the following companies: Peraton, LexisNexis, Cellebrite, Msab Group, Pen-Link, Thomson Reuters, RELX, Clearview AI, BI² Technologies, Palantir Technologies and Anduril Industries.

253 Just Futures Law et al v. US Citizenship and Immigration Services et al (1:26-cv-01045), District Of Columbia District Court, Filed: 03/27/2026, https://www.justfutureslaw.org/legal-filings/foiatps-p43te. See also Renderos v. Clearview AI, Inc., 3:21-cv-04572, (N.D. Cal.), https://www.justfutureslaw.org/legal-filings/clearview (pleadings available here);

254 Business and Human Rights Centre. "Accusations and Actions: A Decade Tracking Tech Company Responses to Human Rights." January 15, 2024. https://www.business-humanrights.org/en/from-us/briefings/accusations-actions-a-decade-of-tech-company-responses-to-allegations-of-human-rights-abuse/.

255 Sarah Lamdan. "Data Cartels: The Companies that Control and Monopolize Our Information." *Stanford University Press,* 2022.

256 Justin Sherman. "Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy,

Personal Safety, and National Security." *Testimony Prepared for US Committee for Energy and Congress*, April 19, 2023. https://www.congress.gov/118/meeting/house/115788/witnesses/HMTG-118-IF02-Bio-ShermanJ-20230419.pdf; Also available at https://www.justinwsherman.com.

257 DHS also mines its own hundreds of millions of data points collected through immigration applications, immigration casework, immigration enforcement encounters, consular processing, surveillance, and travel. See, for example, Privacy Impact Assessment for Palantir's Investigative Case Management System, www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf. See also: www.dhs.gov/science-and-technology/DA-TC and www.dhs.gov/information-sharing.

258 Somos Un Pueblos Unido, Just Futures Law, and Mijente. "Subjected to Surveillance: ICE Access to New Mexico Residents' Personal Data." 2024. https://files.constantcontact.com/b6dfe469001/3326abb4-4580-48be-89dd-1e006a202e09.pdf.

Matt Bracken. "Dem Governors Unwittingly Share DMV Data With ICE, Lawmakers Warn." *Fedscoop*, November 12, 2025. https://fedscoop.com/ice-database-drivers-license-registration-facial-recognition/.

259 Jason Koelber and Joseph Cox. "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows." *404 Media*, May 27, 2025. www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows.

260 Industry reports estimate data brokerage market at approximately $300 billion or more. See Apoorva Priyadarshi and Garvit Vyas. "Market Research Futures." April 15, 2026. https://www.marketresearchfuture.com/reports/data-broker-market-11676.

261 Just Futures Law and Mijente. "The Data Broker to Deportation Pipeline: How Thomson Reuters & LexisNexis Share Utility & Commercial Data with ICE." 2021. https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/62df020189b0681d1b9398a8/1658782211567/Commercial+and+Utility+Data+Report.pdf.

262 American Friends Service Committee. "Equifax Inc." www.investigate.info/company/equifax.

263 LexisNexis Risk Solutions. "LexisNexis Linking and LexID Technology Overview for Government." https://risk.lexisnexis.com/-/media/files/government/lexidforgovernmentbr%20002%20pdf.pdf.

LexisNexis. "LexisNexis Public Records." https://www.lexisnexis.com/pdf/LexisNexis_Public-Records-Competitor-Comparison.pdf.

264 LexisNexis Risk Solutions, "Lexis Nexis Linking."

LexisNexis, "LexisNexis Public Records."

265 Sam Biddle. "ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months." *The Intercept*, June 9, 2022. https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances.

266 USASpending.gov. "Definitive Contract 70CMSD21C00000001, Awarding Agency: Department of Homeland Security (DHS), Recipient: LexisNexis Risk Solutions Inc." Accessed June 10, 2026. www.usaspending.gov/award/CONT_AWD_70CMSD21C00000001_7012_-NONE-_-NONE-.

267 USASpending.gov. "Delivery Order 70CMSD23C00000004, Awarding Agency: Department of Homeland Security (DHS), Recipient: LexisNexis Special Services Inc." Accessed June 10, 2026. www.usaspending.gov/award/CONT_AWD_70CMSD23C00000004_7012_-NONE-_-NONE-.

268 USASpending.gov. "Delivery Order 70B04C23F00000043, Awarding Agency: Department of Homeland Security (DHS), Recipient: LexisNexis Special Services Inc." Accessed June 10, 2026.

www.usaspending.gov/award/CONT_AWD_70B04C23F00000043_7014_GS00F178DA_4732.

269 USASpending.gov. "Delivery Order 70CMSD21C00000002, Awarding Agency: Department of Homeland Security (DHS), Recipient: Thomson Reuters Special Services LLC." Accessed June 10, 2026.

www.usaspending.gov/award/CONT_AWD_70CMSD21C00000002_7012_-NONE-_-NONE-.

Solicitation documents specify that Tasks 2/2A are for license plate reader technology, training, and maintenance. See: https://sam.gov/workspace/contract/opp/bfb956783d5d44a6b2a307b5e11f8f95/view.

270 Lily Hay Newman, "Internal Docs Show How ICE Gets Surveillance Help from Local Cops." *Wired*, March 13, 2019. www.wired.com/story/ice-license-plate-surveillance-vigilant-solutions.

271 USASpending.gov. "Definitive Contract 70CMSD25C00000008, Awarding Agency: Department of Homeland Security (DHS), Recipient: Thomson Reuters Special Services LLC." Accessed June 10, 2026.

www.usaspending.gov/award/CONT_AWD_70CMSD25C00000008_7012_-NONE-_-NONE-.

272 USASpending.gov. "Purchase Order 70CMSD23P00000138, Awarding Agency: Department of Homeland Security (DHS), Recipient: Thomson Reuters Special Services LLC." Accessed June 10, 2026.

www.usaspending.gov/award/CONT_AWD_70CMSD23P00000138_7012_-NONE-_-NONE-.

273 Shereena Qazi. "Thomson Reuters Faces Questions on Rights Abuses for Aiding Deportation." *TRT World*, June 14, 2021. www.trtworld.com/article/13117201.

Edward Ongweso Jr. "Shareholders Push Thomson Reuters to End Intimate Ties with ICE." *VICE*, May 26, 2020. www.vice.com/en/article/shareholders-push-thomson-reuters-to-end-intimate-ties-with-ice.

274 Johana Bhuiyan. "US Immigration Agency Explores Data Loophole to Obtain Information on Deportation Targets." *The Guardian,* April 20, 2022. www.theguardian.com/us-news/2022/apr/19/us-immigration-agency-data-loophole-information-deportation-targets.

275 "Justification For Other Than Full and Open Competition," add-on to contract 70CMSD21C00000001 for Law Enforcement Investigative Database Subscription (LEIDS), https://sam.gov/workspace/contract/opp/de2276d6af534f2897a46197682bc6e8/view.

276 USASpending.gov. "Purchase Order 70CMSD23P00000133,

Awarding Agency: Department of Homeland Security (DHS), Recipient: Equifax Inc." Accessed June 10, 2026. www.usaspending.gov/award/CONT_AWD_70CMSD23P00000133_7012_-NONE-_-NONE-.

277 USASpending.gov. "Blanket Purchase Agreement Call 70CMSD-25FC0000033, Awarding Agency: Department of Homeland Security (DHS), Recipient: Verato, Inc." Accessed June 10, 2026.

www.usaspending.gov/award/CONT_AWD_70CMSD25F-C0000033_7012_70CMSD25A00000001_7012.

278 Includes the following companies: LexisNexis, Equifax, RELX, Thomson Reuters, Appriss.

279 US Department of Homeland Security. "Repository for Analytics in a Virtualized Environment (RAVEn)." May 13, 2020. https://www.dhs.gov/sites/default/files/2025-06/25_0618_priv_pia-ice-055-raven-appendix-update.pdf

280 American Friends Service Committee. "Booz Allen Hamilton Holding Corp." www.investigate.info/company/booz-allen-hamilton.

281 Community Justice Exchange. "Falcon." Accessed June 10, 2026. https://abolishdatacrim.org/en/bestiary/falcon#:~:text=FALCON%20is%20Homeland%20Security%20Investigations,reporting%20and%20connects%20multiple%20datasets.

282 Caroline Haskins. "Amazon, Google, Microsoft, and Other Tech Companies are in a 'Frenzy' to Help ICE Build its Own Data-Mining Tool for Targeting Unauthorized Workers." *Business Insider,* September 1, 2021. www.businessinsider.com/amazon-google-microsoft-ice-raven-data-mining-tool-undocumented-workers-2021-8?utm_source=yahoo.com&utm_medium=referral.

283 Haskins, "Amazon, Google, Microsoft."; See: USASpending.gov. "Delivery Order 70CTD022FR0000002, Awarding Agency: Department of Homeland Security (DHS), Recipient: Booz Allen Hamilton Inc." Accessed June 11, 2026. https://www.usaspending.gov/award/CONT_AWD_70CTD-022FR0000002_7012_GS35F386DA_4732.

284 American Friends Service Committee, "Booz Allen Hamilton Holding Corp."

285 US Department of Homeland Security. "Privacy Impact Assessment for the Office of Biometric Identity Management." Accessed June 6, 2026. https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1.

286 Mijente, Just Futures Law, and Immigrant Defense Project, "HART Attack: How DHS's Massive Biometrics Database Will Supercharge Surveillance and Threaten Rights." May 2022. www.immigrantdefenseproject.org/wp-content/uploads/HART-Attack.pdf.

287 Rebeca Heilweil. "DOGE Has Arrived at the Heart of Homeland Security's Biometrics Operations." *Techscoop,* May 6, 2025. https://fedscoop.com/doge-arrives-at-homeland-security-biometrics-operations.

288 US Government Accountability Office. "DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System." June 2021. www.gao.gov/assets/d21386.pdf.

U.S. Government Accountability Office. "DHS Needs to Address Significant Shortcomings in Program Management and Privacy." September 2023. www.gao.gov/assets/gao-23-105959.pdf.

289 Rebecca Heilweil. "Homeland Security Centralizes Control Over the Government's Largest Biometrics Database." *FedScoop,* August 14, 2025. https://fedscoop.com/homeland-security-centralizes-control-over-the-governments-largest-biometrics-database.

290 Derek B. Johnson. "DHS Privacy Probe Will Focus on Biometric Tracking by ICE, OBIM." *Cyberscoop*, February 6, 2026. https://cyberscoop.com/dhs-ig-audit-ice-obim-biometric-data-privacy-facial-recognition.

291 USASpending.gov. "Delivery Order 70RDAD23FR0000023, Awarding Agency: Department of Homeland Security (DHS), Recipient: Peraton Technology Services Inc." Accessed June 10, 2026. www.usaspending.gov/award/CONT_AWD_70RDAD23FR0000023_7001_70RTAC21D00000006_7001.

292 Veritas Capital. "Veritas Capital Completes Acquisition of Perspecta." May 6, 2021. veritascapital.com/veritas-capital-completes-acquisition-of-perspecta.

293 Blackstone. "The Life Cycle of Private Equity." March 2021. https://pws.blackstone.com/emea/wp-content/uploads/sites/20/blackstone-secure/Life-Cycle-of-Private-Equity-EMEA.pdf?v=1638976450.

294 Peraton. "Peraton is the New Name of Former Harris Corporation Government Services Business." July 28, 2017. www.peraton.com/news/peraton-is-the-new-name-of-former-harris-corporation-government-services-business.

295 US Department of Homeland Security. "Fiscal Year 2027 Congressional Justification." www.dhs.gov/sites/default/files/2026-04/26_0403_ocfo_fy27-buget-management-directorate.pdf.

296 Rebecca Heilweil. "Homeland Security Centralizes Control Over the Government's Largest Biometrics Database." *FedScoop*, August 14, 2025. https://fedscoop.com/homeland-security-centralizes-control-over-the-governments-largest-biometrics-database.

297 Kate McQuarrie. "Trump Team Financials: Antoine McCord." *Propublica.* https://projects.propublica.org/trump-team-financial-disclosures/appointees/mccord-antoine

298 Rebeca Heilweil. "DOGE Has Arrived at The Heart of Homeland Security's Biometrics Operations." *FedScoop,* May 6, 2025. fedscoop.com/doge-arrives-at-homeland-security-biometrics-operations.

299 Rebeca Heilweil. "The White House is Reviewing the Nation's Biometrics Operation." *FedScoop,* May 20, 2025. https://fedscoop.com/white-house-is-reviewing-the-nations-biometrics-operation/.

300 Anthony Kimery. "Internal Struggle Over US Federal Biometric Data Management Intensifies." *Biometric Update*, June 14, 2025. www.biometricupdate.com/202506/internal-struggle-over-us-federal-biometric-data-management-intensifies.

301 Just Futures Law. "Reining in AI Surveillance." Accessed June 11, 2026. https://www.justfutureslaw.org/aitech.

302 USASpending.gov. "Delivery Order 70CMSD25FR0000089, Awarding Agency: Department of Homeland Security (DHS), Recipient: Carahsoft Technology Corp." Accessed June 11, 2026. https://www.usaspending.gov/award/CONT_AWD_70CMSD25FR0000089_7012_47QSWA18D008F_4732.

303 DHS, Privacy Impact Assessment for ICE Investigative Case Management, 16 June 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf

304 USASpending.gov. "Indefinite Delivery Contract HSCETC14C00002, Awarding Agency: Department of Homeland Security (DHS), Recipient: Palantir USG Inc." Accessed June 11, 2026.

www.usaspending.gov/award/CONT_IDV_HSCETC14C00002_7012.

305 USASpending.gov. "Delivery Order 70CTD022FR0000170, Awarding Agency: Department of Homeland Security (DHS), Recipient: Palantir Technologies Inc." Accessed June 11, 2026. www.usaspending.gov/award/CONT_AWD_70CTD022FR0000170_7012_GS35F0086U_4730.

306 USASpending.gov, "Delivery Order 70CTD022FR0000170."

307 Immigration Policy Tracking Project. "Palantir Granted $30 Million to Build 'ImmigrationOS' Surveillance Platform for ICE." April 18, 2025. immpolicytracking.org/policies/reported-palantir-awarded-30-million-to-build-immigrationos-surveillance-platform-for-ice.

308 Steven Hubbard. "ICE to Use ImmigrationOS by Palantir, a New AI System, to Track Immigrants' Movements." *American Immigration Council,* August 21, 2025. www.americanimmigrationcouncil.org/blog/ice-immigrationos-palantir-ai-track-immigrants.

309 Bobby Allyn. "Former Palantir Workers Condemn Company's Work with Trump Administration." *NPR*, May 5, 2025. www.npr.org/2025/05/05/nx-s1-5387514/palantir-workers-letter-trump.

310 Rosemarie Cho. "ICE Just Ordered $30 Million Worth of New Technology from Palantir to Track Immigrants." *Business Insider,* April 17, 2025. https://www.businessinsider.com/ice-palantir-new-technology-30-million-visa-overstays-self-deportation-2025-4.

311 Erman Akilli. "Palantir's All-Seeing Eye: Domestic Surveillance and

the Price of Security." *SETA,* June 10, 2025, www.setav.org/en/palantirs-all-seeing-eye-domestic-surveillance-and-the-price-of-security.

USASpending.gov. "Delivery Order 70CTD022FR0000002."

312 Joseph Cox. "'ELITE': The Palantir App ICE Uses to Find Neighborhoods to Raid." *404 Media*, January 15, 2026. www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid.

313 Cox, "ELITE."

314 Cox, "ELITE."

315 Joseph Cox. "Here is the User Guide for ELITE, the Tool Palantir Made for ICE." *404 Media*, January 30, 2026, https://www.404media.co/here-is-the-user-guide-for-elite-the-tool-palantir-made-for-ice/.

316 Katya Schwenk. "ICE Will Use AI to Surveil Social Media." *Jacobin,* October 26, 2025. jacobin.com/2025/10/ice-zignal-surveillance-social-media.

317 Katya Schwenk. "ICE Just Spent Millions on a Social Media Surveillance AI Program." *Truthout*, October 25, 2025. truthout.org/articles/ice-just-spent-millions-on-a-social-media-surveillance-ai-program.

318 USASpending.gov. "Delivery Order 70CMSD25FR0000110, Awarding Agency: Department of Homeland Security (DHS), Recipient: Thundercat Technology, LLC." Accessed June 11, 2026. https://www.usaspending.gov/award/CONT_AWD_70CMSD25FR0000110_7012_NNG15SC92B_8000.

319 Joseph Cox. "The 200+ Sites an ICE Surveillance Contractor is Monitoring." *404 Media,* March 12, 2025. www.404media.co/the-200-sites-an-ice-surveillance-contractor-is-monitoring.

320 Joseph Cox. "Homeland Security Uses AI Tool to Analyze Social Media of US Citizens and Refugees." *VICE*, May 17, 2023. www.vice.com/en/article/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees.

321 It is possible that CBP holds a contract for Babel Street services through a third party that is not searchable using publicly accessible sources.

322 US Department of Homeland Security. "AI Use Case Inventory Library."

323 Electronic Privacy Information Center. "EPIC v. ICE (Location and Social Media Surveillance)." Case No. 22-762 (2022). https://epic.org/documents/epic-v-ice-location-and-social-media-surveillance.

324 USASpending.gov. "Delivery Order 70Z02325F91220001, Awarding Agency: Department of Homeland Security (DHS), Recipient: Panamerica Computers, Inc." Accessed June 11, 2026. www.usaspending.gov/award/CONT_AWD_70Z02325F91220001_7008_NNG15SD02B_8000.

325 USASpending.gov. "Delivery Order 70B06C25F00000048, Awarding Agency: Department of Homeland Security (DHS), Recipient: Thundercat Technology, LLC." Accessed June 11, 2026. https://www.usaspending.gov/award/CONT_AWD_70B06C25F00000048_7014_NNG15SC92B_8000.

326 "Fivecast." www.fivecast.com.

327 Joseph Cox. "The A.I. Surveillance Tool DHS Uses to Detect 'Sentiment and Emotion'." *404 Media,* August 24, 2023. www.404media.co/ai-surveillance-tool-dhs-cbp-sentiment-emotion-fivecast.

328 US Department of Homeland Security. "AI Use Case Inventory Library."

329 OSINT Combine. "NexusXplore." www.osintcombine.com/nexusxplore.

330 USASpending.gov. "Delivery Order 70CMSD25FR0000155, Awarding Agency: Department of Homeland Security (DHS), Recipient: Alvarez LLC." Accessed June 11, 2026. https://www.usaspending.gov/award/CONT_AWD_70CMSD25FR0000155_7012_NNG15SD19B_8000.

331 Joseph Cox. "Revealed: US Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data." *Vice,* September 21, 2022. www.vice.com/en/article/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data.

332 Cox. "Revealed: US Military Bought Mass Monitoring Tool."

333 USASpending.gov, "Delivery Order 70CMSD25FR0000155."

334 See USASpending.gov. "Purchase Order 70B03C25P00000508, Awarding Agency: Department of Homeland Security (DHS), Recipient: Pen-Link Ltd." Accessed June 11, 2026. https://www.usaspending.gov/award/CONT_AWD_70B03C25P00000508_7014_-NONE-_-NONE-.

See also USASpending.gov. "Purchase Order 70CMSD25P00000138, Awarding Agency: Department of Homeland Security (DHS), Recipient: Pen-Link Ltd." Accessed June 11, 2026.

https://www.usaspending.gov/award/CONT_AWD_70CMSD25P00000138_7012_-NONE-_-NONE-.

335 Surveillance Watch. "Tangles." March 20, 2026. www.surveillance-watch.io/entities/tangles.

336 Thomas Brewster. "ICE Acaba de Gastar Millones en Tecnología de Vigilancia Prohibida por Facebook." *Forbes,* September 18, 2025. https://forbes.com.mx/ice-acaba-de-gastar-millones-en-tecnologia-de-vigilancia-prohibida-por-facebook/.

337 US Securities and Exchange Commission. "Pen-Link's PLX Privacy Impact Assessment." March 6, 2025. www.sec.gov/files/pia-penlink.pdf.

338 Penlink, "Penlink Taps Former Acting DEA Administrator, Derek Maltz, to Lead Global Business Growth and Strategy." June 25, 2025, www.penlink.com/blog/penlink-taps-former-acting-dea-administrator-derek-maltz-to-lead-global-business-growth-and-strategy.

339 On file with authors. This excerpt is from documents retrieved through Pangea Legal Services et al v USCIS et al, (1:24-cv-02809), District Of Columbia District Court, Filed: 10/03/2024; https://www.justfutureslaw.org/legal-filings/dhsaifoia; (on file with authors).

340 US Commission on Civil Rights. "The Civil Rights Implications of the Federal Use of Facial Recognition Technology." September 2024. https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf. See also Clare Garvie, Alvaro Bedoya, Jonathan Frankle. "The Perpetual Line-Up." *Georgetown Law, Center on Privacy and Tech,* October 18, 2016. https://www.perpetuallineup.org/.

341 2025 DHS AI Use Case Inventory, DHS-2729, DHS-2412, DHS-2413, DHS-2414, DHS-2415, DHS-2416, DHS-2570, DHS-2619, DHS-2669, DHS-2731, DHS-398, DHS-2457, DHS-2458

DHS-2459, DHS-2577, DHS-362, DHS-2417, DHS-35. DHS-401. DHS-251, DHS-407, DHS-2759, www.dhs.gov/publication/ai-use-case-inventory-library.

342 Anthony Kimery. "Smart Glasses and the New DHS Surveillance Budget." *Biometric Update*, April 21, 2026. www.biometricupdate.com/202604/smart-glasses-and-the-new-dhs-surveillance-budget. See also Benjamin S. Weiss. "DHS startles Congress with Request for Millions to Develop ICE 'Smart Glasses." *Courthouse News Services,* April 21, 2026. https://www.courthousenews.com/dhs-startles-congress-with-request-for-millions-to-develop-ice-smart-glasses/.

343 Electronic Privacy Information Center. "GAO Reports More Negatives Than Positives to Police Use of Facial Recognition, Highlights Need for Comprehensive Data Privacy Law." April 29, 2024, https://epic.org/gao-reports-more-negatives-than-positives-to-police-use-of-facial-recognition-highlights-need-for-comprehensive-data-privacy-law/.

344 Derek B. Johnson, "DHS Privacy Probe Will Focus on Biometric Tracking by ICE, OBIM." *Cyberscoop*, February 6, 2026. https://cyberscoop.com/dhs-ig-audit-ice-obim-biometric-data-privacy-facial-recognition/.

345 Mijente, Just Futures Law, and Immigrant Defense Project, "HART Attack." See also Anthony Kimery, "DHS's Biometric Power Shift Raises Oversight Concerns." *Biometric Update*, August 14, 2025. www.biometricupdate.com/202508/dhss-biometric-power-shift-raises-oversight-concerns.

346 Clearview AI. "Clearview 2.0." Accessed June 4, 2026. https://www.clearview.ai/clearview-2-0.

347 Kashmir Hill. "The Secretive Company That Might End Privacy as We Know It." *The New York Times*, January 18, 2020. www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

348 Rachel McColluch. "Potential £17 Million Fine for Facial Recognition Company Clearview AI." *Acuity Law*, January 25, 2022. https://acuityl-aw.com/fine-for-facial-recognition-company-clearview-ai.

349 USASpending.gov. "Purchase Order 70CMSD25P00000111, Awarding Agency: Department of Homeland Security (DHS), Recipient: Clearview AI, Inc." Accessed June 11, 2026.

www.usaspending.gov/award/CONT_AWD_70CMSD25P00000111_7012_-NONE-_-NONE-.

350 Lindsey Wilkinson. "CBP to Strengthen 'Tactical Targeting,' 'Counter-Network Analysis' with Clearview AI." *FedScoop*, February 11, 2026. https://fedscoop.com/dhs-cbp-contract-biometric-facial-recognition-ai.

351 DHS 2413, 2414, 2415, 2416 (CBP); DHS 345 (CBP), DHS 398 DHS 2731 (CBP), Mobile Fortify) AI Inventory; https://www.dhs.gov/publication/ai-use-case-inventory-library

352 Just Futures Law. "Mobile Fortify: The Facial Recognition App ICE Uses to Surveil Us." Accessed June 11, 2026. https://static1.square-space.com/static/62c3198c117dd661bd99eb3a/t/69ab27c1fc25b87d-270c834c/1772824513281/Mobile%2BFortify%2BWhat%2BWe%2B-Know%2B%282%29.pdf.

353 "ICE Pilots Mobile Fortify App, Expanding Facial Recognition Surveillance into U.S. Communities," *ID Tech,* June 27, 2025. https://idtechwire.com/ice-pilots-mobile-fortify-app-expanding-facial-recognition-surveillance-into-u-s-communities/.

354 US Department of Homeland Security, Privacy Office. "Mobile Fortify, Privacy Threshold Analysis." February 2025. https://www.document-cloud.org/documents/26209262-mobile-fortify-pta/.

355 Anthony Kimery. "ICE Facial Recognition App Mobile Fortify Powered by NEC." *Biometric Update,* January 29, 2026. www.biometricupdate.com/202601/ice-facial-recognition-app-mobile-fortify-powered-by-nec.

356 Joseph Cox. "ICE and CBP Agents Are Scanning Peoples' Faces on the Street to Verify Citizenship." *404 Media*, October 29, 2025. https://www.404media.co/ice-and-cbp-agents-are-scanning-peoples-faces-on-the-street-to-verify-citizenship/.

357 Sanya Mansoor. "How ICE is Using Facial Recognition in Minnesota." *The Guardian*, January 27, 2026. www.theguardian.com/technology/2026/jan/27/ice-facial-recognition-minnesota.

358 NEC. "Use Cases." Accessed June 11, 2026. www.necam.com/en_US/necnss/resources/case/index.html.

For OBIM contract, see USASpending.gov. "Definitive Contract 70RDA124C00000002, Awarding Agency: Department of Homeland Security (DHS), Recipient: NEC National Security Systems, Inc." Accessed June 11, 2026. www.usaspending.gov/award/CONT_AWD_70RDA124C00000002_7001_-NONE-_-NONE-.

See also Mijente, Just Futures Law, and Immigrant Defense Project, "HART Attack."

359 USASpending.gov. "Definitive Contract 70CTD025C00000001, Awarding Agency: Department of Homeland Security (DHS), Recipient: BI² Technologies, LLC." Accessed June 11, 2026. https://www.usaspending.gov/award/CONT_AWD_70CTD025C00000001_7012_-NONE-_-NONE-.

360 Anthony Kimery. "ICE's Biometric Surveillance Reach Expands with BI² Iris Scanning Tech." *Biometric Update,* August 7, 2025. www.biometricupdate.com/202508/ices-biometric-surveillance-reach-expands-with-bi2-iris-scanning-tech.

361 Nick Schwellenbach and Russ Choma. "Clients of a Trump-Connected Lobbying Firm Keep Landing No-Bid ICE Contracts." *Mother Jones,* December 2025. www.motherjones.com/politics/2025/09/trump-ice-contracts-ballard-partners-lobbying-bi2-technologies-palantir-biometrics.

362 See: Lobbying Disclosure Report for Ballard Partners for 2025, https://disclosurespreview.house.gov/ld/ldxmlrelease/2025/Q2/301746615.xml

363 Schwellenbach and Choma, "Clients of a Trump-Connected Lobbying Firm."

See USASpending.gov. "Indefinite Delivery/ Indefinite Quantity Contract 70CMSD25D00000001, Awarding Agency: Department of Homeland Security (DHS), Recipient: SNA International LLC." Accessed June 11, 2026. www.usaspending.gov/award/CONT_IDV_70CMSD25D00000001_7012.

364 Saira Hussain. "ICE's Rapid DNA Testing on Migrants at the Border Is Yet Another Iteration of Family Separation." *Electronic Frontier Foundation,* August 2, 2019. www.eff.org/deeplinks/2019/08/ices-rapid-dna-testing-migrants-border-yet-another-iteration-family-separation.

365 Dell Cameron. "DHS Has Been Collecting US Citizens' DNA for Years." *Wired*, September 23, 2025. www.wired.com/story/dhs-has-been-collecting-us-citizens-dna-for-years.

366 Johana Bhuiyan. "US Immigration Authorities Collecting DNA Information of Children in Criminal Database." *The Guardian*, May 31, 2025. www.theguardian.com/us-news/2025/may/31/cbp-dna-collection-children-immigrants.

367 Cameron, "DHS Has Been Collecting US Citizens' DNA."

368 National Urban Security Technology Laboratory. "Automated License Plate Readers: Market Survey Report." *US Department of Homeland Security, Science and Technology,* June 2025.

https://www.dhs.gov/sites/default/files/2025-06/25_0606_st_lprmsr.pdf.

369 Jason Koelber and Joseph Cox. "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows." *404 Media*, May 27, 2025. www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows.

370 See at USASpending.gov Contracts No. 70B03C25P00000454, 70B03C25F00000529; Contract No. 70CMSD25FR0000049; Contract No. 70CMSD25FR0000087; Contracts No. 70B06C25F00000316, 70B03C25F00000498, 70B02C25F00001335.

371 Investigate. "Micro Systemation AB." *American Friends Service Committee,* July 12, 2024. https://investigate.afsc.org/company/micro-systemation#:~:text=The%20collaboration%20brings%20together%20Berla's,technology%20from%202011%20to%202016.

372 Investigate, "Micro Systemation AB."

373 Sam Biddle. "Your Car Is Spying on You, and a CBP Contract Shows the Risks." *The Intercept,* May 23, 2021. https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/.

374 See at USASpending.gov Contract No. 70B02C25F00001335, Contract No. 70B03C25F00000498, Contract No. 70B06C25F00000316.

375 Crunchbase search for Flock Safety financial information.

376 Bedrock. "Geoff Lewis." Accessed June 11, 2026. bedrockcap.com/geoff-lewis.

377 Palantir. "PCL Team." Accessed June 11, 2026. www.palantir.com/pcl/team.

378 US Customs and Border Protection. "Border Search of Electronic Devices at Ports of Entry." Accessed June 11, 2026. https://www.cbp.gov/travel/cbp-search-authority/border-search-electronic-devices.

379 Aram Rostom. "FBI to Investigate Minneapolis Activists After Far-Right Claim About Signal Chats." *The Guardian*, January 27, 2026. https://www.theguardian.com/us-news/2026/jan/27/minneapolis-fbi-signal-investigation-kash-patel.

380 Max Nesterak. "Why is ICE seizing people's phones and documents?" *Minnesota Reformer*, February 12, 2026. https://minnesotareformer.com/2026/02/12/why-is-ice-seizing-peoples-phones-and-documents/.

381 Usaspending.gov search for Cellebrite and Magnet Forensics for FY2025.

382 See Delivery Order 70CMSD25FR0000087, www.usaspending.gov/award/CONT_AWD_70CMSD25FR0000087_7012_NNG15SD74B_8000.

383 Delivery Order 70CMSD25FR0000049, www.usaspending.gov/award/CONT_AWD_70CMSD25FR0000049_7012_NNG15SC82B_8000.

384 USASpending.gov search for "Cellebrite" by Awarding Agency: US Immigration and Customs Enforcement,

385 Usaspending.gov data for Cellebrite awards.

386 Investigate. "Cellebrite DI Ltd." *American Friends Service Committee.* April 1, 2025. https://investigate.afsc.org/company/cellebrite.

387 Lindsey Wilkinson. "DHS Units to Re-Up Contract With Controversial Mobile Device Data Extractor." *FedScoop*, May 11, 2026. https://fedscoop.com/dhs-cellebrite-privacy-drones-data-mobile-devices-ice.

388 Jacob Shamsian, "A Cybersecurity Executive Was Pardoned by Donald Trump. His Crime Was a Mystery." *Yahoo! News,* January 1, 2025. www.yahoo.com/news/cybersecurity-executive-pardoned-donald-trump-091501946.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMFqArXWqcLPuLvEVxbAVSzw96pYzeGrFlDvENcVLb2hPpZb9o6F1SbuqxoCnMbRQnJTqLnTD1lTVHrc8bGngUAk3waMrH2OFvlHA_06zWT6tQmVW3hJ7M3phH4zb7dH2O0AQKbATSlu62upBhoIAv6EKaBvZK-9_rJhShtA7kxo&guccounter=2.

389 Thomas Brewster. "Trump Pardoned Him. Now He's Selling His Cyber Business For $200 Million." *Forbes,* June 5, 2025. www.forbes.com/sites/thomasbrewster/2025/06/05/trump-pardoned-corellium-founder-now-selling-cyber-business-to-cellebrite.

390 Lorenzo Franceschi-Bicchierai. "A Leak Details Apple's Secret Dirt on a Trusted Security Startup." *Wired,* November 21, 2022. www.wired.com/story/corellium-nso-group-darkmatter-apple-lawsuit/#:~:text=According%20to%20the%20leaked%20document,journalists%2C%20and%20human%20rights%20defenders.

391 David Gee. "Cellebrite + Correlium: The Unmatched Partnership Explained." *Cellebrite*, December 2, 2025. cellebrite.com/en/blog/cellebrite-corellium-the-unmatched-partnership-explained.

392 Lorenzo Franceschi-Bicchierai. "ICE Unit Signs New $3M Contract for Phone-Hacking Tech." *TechCrunch,* September 18, 2025. https://techcrunch.com/2025/09/18/ice-unit-signs-new-3-million-contract-for-phone-hacking-tech/.

393 Franceschi-Bicchierai,"ICE Unit Signs New $3M Contract."

394 See USASpending.gov Contract No. 70CMSD25FR0000097 and Contract No. 70CMSD25P00000130.

395 See Purchase Order 70CTD024P00000012, www.usaspending.gov/award/CONT_AWD_70CTD024P00000012_7012_-NONE-_-NONE-.

396 Jude Joffe-Block. "ICE Acknowledges It Is Using Powerful Spyware." *NPR,* April 7, 2026.

https://www.npr.org/2026/04/07/nx-s1-5776799/ice-spyware-privacy.

397 Jude Joffe-Block. "What We Know About How the U.S. Government Uses Spyware (And What We Don't)." *NPR,* May 21, 2026. https://www.npr.org/2026/05/19/nx-s1-5826085/spyware-trump-dhs-paragon

398 Center for Constitutional Rights. "ICE and CBP Surveillance Tech FOIA." October 30, 2025. https://ccrjustice.org/home/what-we-do/our-cases/ice-and-cbp-surveillance-tech-foia.

Joseph Cox. "We Sued ICE to Get Its Spyware Contract. The Agency Is Redacting Essentially Everything." *404 Media,* June 1, 2026.

https://www.404media.co/we-sued-ice-to-get-its-spyware-contract-the-agency-is-redacting-essentially-everything/.

399 Thomas Brewster. "How ICE Is Using Fake Cell Towers to Spy on People's Phones." *Forbes,* September 9, 2025. www.forbes.com/sites/the-wiretap/2025/09/09/how-ice-is-using-fake-cell-towers-to-spy-on-peoples-phones.

400 Brewster. "How ICE is Using Fake Cell Towers."

401 Joseph Cox, "CBP Tapped into the Online Advertising Ecosystem to Track Peoples' Movements." *404 Media,* March 3, 2026. www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements.

402 Cox. "CBP Tapped."

403 Lena Cohen and Hudson Hungo. "The Government Uses Targeted Advertising to Track Your Location. Here's What We Need to Do." *Electronic Frontier Foundation,* March 5, 2026. www.eff.org/deeplinks/2026/03/targeted-advertising-gives-your-location-government-just-ask-cbp.

404 Sheera Frankel and Mike Isaac. "Homeland Security Wants Social Media Sites to Expose Anti-ICE Accounts." *The New York Times*. February 13, 2026. https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html?smid=nytcore-android-share

405 The case involves the use of a geofence warrant, which police use to demand information on all cellphones within a certain area and period of time. The outcome of the case, which revolves around Fourth Amendment questions, could have profound implications for location tracking. Chatrie v. United States." Oyez, www.oyez.org/cases/2025/25-112. Accessed May 17, 2026.

406 See: USAspending.gov, Contract No. 70CMSD24FR0000115.

407 Lorenzo Franceschi-Bicchierai. "ICE Bought Vehicles Equipped with Fake Cell Towers to Spy on Phones." *TechCrunch,* October 7, 2025. techcrunch.com/2025/10/07/ice-bought-vehicles-equipped-with-fake-cell-towers-to-spy-on-phones.

408 Sam Richards. "Powerful Mobile Phone Surveillance Tool Operates in Obscurity Across the Country." *The Intercept*. December 23, 2020. theintercept.com/2020/12/23/police-phone-surveillance-dragnet-cellhawk.

409 See: USAspending.gov, Contract No. 70CMSD25P00000064.

410 See: https://sam.gov/workspace/contract/opp/3ff22adcf3e34b09b7e1d811036ce1bd/view.

411 USAspending.gov contract search. See, for instance: Contract No. 70CDCR26FR0000003.

412 See: US DHS, ICE Request for Information Skip Tracing/Process Serving 2025, last access on June 12, 2026, at: https://share.mayfirst.org/s/HJGgEG6X5y4eGp6?dir=/&editing=false&openfile=true

413 Eva Dou. "ICE launches nationwide program for covert surveillance of immigrants." *The Washington Post*, January 30, 2026. www.washingtonpost.com/technology/2026/01/30/ice-capgemini-skip-tracing-contracts.

414 Sam Biddle. "10 Companies Have Already Made $1 Million As Ice Bounty Hunters. We Found Them." *The Intercept*, December 23, 2025. theintercept.com/2025/12/23/ice-bounty-hunters-track-immigrant-surveillance.

415 Jack Burgess. "French tech giant Capgemini to sell US subsidiary working for ICE." *BBC*. February 1, 2026. www.bbc.com/news/articles/cd9e4xw8vqqo.

416 See: USAspending.gov, IDIQ Contract 70CDCR26D00000015, www.usaspending.gov/award/CONT_IDV_70CDCR26D00000015_7012.

417 See: USAspending.gov, Contract No. 70CDCR26FR0000021.

418 Hannah Hollingsworth and John Hanna. "Trump administration using no-bid contracts, boosting big firms, to get more ICE detention." *PBS Newshour*, June 16, 2025. https://www.pbs.org/newshour/nation/trump-administration-using-no-bid-contracts-boosting-big-firms-to-get-more-ice-detention-beds.

419 Billal Rahman. "ICE Missing Trump Admin's Deportation Target." *Newsweek*, April 15, 2026. https://www.newsweek.com/ice-missing-trump-admin-deportation-target-11833477.

420 Based on search of database TRAC. "Alternatives to Detention." https://tracreports.org/immigration/detentionstats/atd_pop_table.html-https://tracreports.org/immigration/detentionstats/atd_pop_table.html.

421 BI Incorporated website. "Wrist-worn Electronic Monitoring: Embracing a New Era of Accountability." Last accessed on June 6, 2026. bi.com/wrist-worn-electronic-monitoring-devices

422 Adam Satariano. "The Tech Arsenal that Could Power Trump's Immigration Crackdown." *Boston Globe,* January 25, 2025. bostonglobe-prod.cdn.arcpublishing.com/2025/01/25/nation/tech-arsenal-that-could-power-trumps-immigration-crackdown.

423 Department of Homeland Security. "DHS Launches CBP Home App with Self-Deport Reporting Feature." March 10, 2025. www.dhs.gov/news/2025/03/10/dhs-launches-cbp-home-app-self-deport-reporting-feature.

424 Massachusetts Immigrant & Refugee Advocacy Coalition. "CBP

ONE app parole termination, IRS sharing data with DHS." April 10, 2025. https://miracoalition.org/news/policy-update-4-10-25-cbp-one-app-parole-termination-irs-sharing-tax-data-with-dhs/.

425 Congressional Budget Office. "Reconciliation Recommendations of the House Committee on Homeland Security," 9 May 2025, www.cbo.gov/publication/61384. Also see, Will Parrish. "The U.S. Border Patrol and An Israeli Military Contractor Are Putting A Native American Reservation Under 'Persistent Surveillance'." *The Intercept*, August 25, 2019. https://theintercept.com/2019/08/25/border-patrol-israel-elbit-surveillance.

426 Parrish. "The U.S. Border Patrol and An Israeli Military Contractor."

427 Parrish. "The U.S. Border Patrol and An Israeli Military Contractor."

428 DHS Office of Inspector General. "CBP Has Improved Southwest Border Technology, but Significant Challenges Remain." February 23, 2021. www.oig.dhs.gov/sites/default/files/assets/2021-02/OIG-21-21-Feb21.pdf.

429 Kenneth Niemeyer. "Palmer Luckey and Other Defense Tech Leaders see Trump's Victory as a Win for the Industry," *Business Insider,* November 10, 2024. www.businessinsider.com/palmer-luckey-anduril-trump-defense-tech-growth-2024-11; Anduril Industries financial information on Crunchbase; See also Chris Morris. "These are the Companies JD Vance has Invested in as a VC (and Beyond)," *Fast Company,* July 17, 2024. www.fastcompany.com/91157500/companies-jd-vance-invested-in-as-a-vc.

430 Sam Biddle. "Trump's Big Beautiful Gift to Anduril," *The Intercept*, July 9, 2025. https://theintercept.com/2025/07/09/trump-big-beautiful-bill-anduril.

431 Lindsey Wilkinson. "DHS Moves Forward on Autonomous Surveillance Towers at the Border," *FedScoop*, April 16, 2026. https://fedscoop.com/dhs-budget-border-wall-surveillance-shutdown.

432 General Dynamic Information Technology website. "GDIT Unveils New Autonomous Surveillance Towers to Strengthen Border Security," press release, March 11, 2026. www.gdit.com/about-gdit/press-releases/gdit-unveils-new-autonomous-surveillance-towers-to-strengthen-border.

433 See: USAspending.gov, Contract No. 70B02C20D00000019, see also: Contract No. 70B02C24F00000395.; "Anduril Surveillance Towers," US Customs and Border Protection, 21 October 2021, www.cbp.gov/document/foia-record/anduril-surveillance-towers; See also Joseph Cox. "CBP Is Testing Palmer Luckey's AI-Powered Surveillance Towers in the Great Lakes." *404 Media,* November 29, 2023. www.404media.co/cbp-anduril-canada-great-lakes

434 See: USAspending.gov, Contract data from USAspending.gov.

435 Anduril website. "Anduril Announces $5B Series H Raise," May 13, 2026. www.anduril.com/news/anduril-announces-usd5b-series-h-raise.

436 Derek Staahl. "New AI Surveillance Towers at US-Mexico Border Raise Privacy Concerns," *AZFamily*, May 6, 2026. https://www.azfamily.com/2026/05/07/new-ai-surveillance-towers-us-mexico-border-raise-privacy-concerns.

437 Jason Koebler, Joseph Cox, and Jordan Pearson. "Customs and Border Protection Is Flying a Predator Drone Over Minneapolis," May 29, 2020. ,https://www.vice.com/en/article/customs-and-border-protection-predator-drone-minneapolis-george-floyd/

438 TIME staff. "U.S. Immigration Agency Using Drones Capable of Surveillance During L.A. Protests," *TIME*, June 12, 2025. https://time.com/7293743/drones-los-angeles-protests-law-enforcement/; See also Jon Collins, "Drone surveillance drove surveillance fears as ICE surged in Minnesota," *MPR News,* March 13, 2026, https://www.mprnews.org/story/2026/03/13/minnesota-drone-sightings-drove-surveillance-fears-as-ice-surged

439 Letter from Senators Markey, Wyden, et al to former DHS Secretary Kristi Noem on the use of drones over protests, dated July 31, 2025. https://www.markey.senate.gov/imo/media/doc/letter_to_dhs_on_aerial_surveillance.pdf (last accessed June 6, 2026).

440 Customs and Border Protection website. "CBP Small Drones Program," www.cbp.gov/frontline/cbp-small-drones-program. See also: Dell Cameron. "Border Patrol Bets on Small Drones to Expand US Surveillance Reach," *WIRED*, December 17, 2025. www.wired.com/story/border-patrol-bets-on-small-drones-to-expand-us-surveillance-reach.

441 Defense Contract Management Agency, https://bluelist.appsplatformportals.us.

442 See: USAspending.gov, Blanket Purchase Agreement 70B02C22A00000002, www.usaspending.gov/award/CONT_IDV_70B02C22A00000002_7014.

443 Cal Biesecker. "CBP Acquires Trusted Small UAS For Operational Evaluations," *Defense Daily*, October 20, 2022, www.defensedaily.com/cbp-acquires-trusted-small-uas-for-operational-evaluations/unmanned-systems.

444 Department of Homeland Security website. "Department of Homeland Security Launches New Office to Advance Drone and Counter-Drone Technologies," January 12, 2026. www.dhs.gov/news/2026/01/12/department-homeland-security-launches-new-office-advance-drone-and-counter-drone. See also: Department of Homeland Security website. "Counter-Unmanned Aircraft Systems (C-UAS)," www.dhs.gov/science-and-technology/counter-unmanned-aircraft-systems-c-uas.

445 Department of Homeland Security website. "Department of Homeland Security Launches New Office to Advance Drone and Counter-Drone Technologies," January 12, 2026. www.dhs.gov/news/2026/01/12/department-homeland-security-launches-new-office-advance-drone-and-counter-drone.

446 DHS website. "Department of Homeland Security Launches New Office."

447 See: USAspending.gov, Contract No. 70B03C25F00000193.

448 Eleanor Pringle. "Marc Andreessen says Half of His Time Goes to Helping Trump at Mar-a-Lago," *Fortune,* December 11, 2024. fortune.com/2024/12/11/marc-andreessen-half-time-florida-trump-business-policies.

449 See: USAspending.gov, Contract No. 70CMSD25FR0000122

450 Haye Kesteloo. "ICE's $85 Billion Surveillance Machine Includes Skydio Drones for Protest Monitoring and Roving No-Fly Zones for Everyone Else," *DroneXL,* February 2, 2026. dronexl.co/2026/02/02/ices-surveillance-skydio-drones.

451 Kesteloo. "ICE's $85 Billion Surveillance Machine."

452 Langston B. Lee. "New York Mayor Eric Adams Built a Drone Dystopia. Mamdani Shouldn't Let it Fly," *Tech Policy Press,* January 6, 2026. www.techpolicy.press/new-york-mayor-eric-adams-built-a-drone-dystopia-mamdani-shouldnt-let-it-fly.

453 Kesteloo. "ICE's $85 Billion Surveillance Machine."

454 Eva Dou. "ICE Amps Up its Surveillance Powers, Targeting Immigrants and Antifa." *The Washington Post*, October 17, 2025. www.washingtonpost.com/technology/2025/10/17/ice-surveillance-immigrants-antifa.

455 Jon Collins. "Drone Sightings Drove Surveillance Fears as ICE Surged in Minnesota." *MPR News*, March 13, 2026. www.mprnews.org/story/2026/03/13/minnesota-drone-sightings-drove-surveillance-fears-as-ice-surged.

456 Kesteloo. "ICE's $85 Billion Surveillance Machine."

457 Alma Campos. "Cook County Investigates ICE Purchasing of Data Software to Target Undocumented Immigrants." *South Side Weekly*, August 5, 2022. https://southsideweekly.com/cook-county-investigates-ice-purchasing-of-data-software-to-target-undocumented-immigrants/.

458 San Francisco Police Department website. "19B Surveillance Technology Policies," last accessed June 9 2026. https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies

459 Porland City Code. https://www.portland.gov/code/34/10

460 Rojas et al v. Clearview AI, Inc., et al., Alameda County Superior Court, Case No. RG21096898; see also https://www.justfutureslaw.org/legal-filings/clearview.

461 Michael Sandoval. "Defending Maine Communities from Federal

Surveillance and Intimidation." *Protect Democracy*, February 23, 2026. https://protectdemocracy.org/work/defending-maine-communities-from-federal-surveillance-and-intimidation/.

462 Sam Levin. "Video Shows ICE Violently Arresting Oregon Farm Workers and Using Facial Recognition." *The Guardian*, May 21, 2026. https://www.theguardian.com/us-news/2026/may/21/ice-immigration-oregon-facial-recognition.

463 Levin. "Video Shows ICE Violently Arresting."

464 Daisuke Wakabayashi and Scott Shane. "Google Will Not Renew Pentagon Contract That Upset Employees." *The New York Times*, June 1, 2018. https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

465 Billy Perrigo. "Google Workers Revolt over $1.2 Billion Dollar Contract with Israel." *Time*, January 19, 2026. https://time.com/6964364/exclusive-no-tech-for-apartheid-google-workers-protest-project-nimbus-1-2-billion-contract-with-israel/

466 Rosalie Chan. "Read the Internal Letter Sent by a Group of Amazon Employees Asking the Company to Take a Stand against ICE," *Business Insider*, July 11, 2019. https://www.businessinsider.com/amazon-employees-letter-protest-palantir-ice-camps-2019-7?op=1. See also: Sebastian Moss, "Microsoft Employees' Open Letter Protests Against JEDI Contract, says Azure Should Not be Used for "Waging War," *Data Center Dynamics*, October 15, 2018. https://www.datacenterdynamics.com/en/news/microsoft-employees-open-letter-protests-against-jedi-contract-says-azure-should-not-be-used-waging-war/

467 National Nurses United. "Nurses, Community Allies to Highlight Connection between ICE Violence and Palantir," February 4, 2026. https://www.nationalnursesunited.org/press/nurses-community-allies-to-highlight-connection-between-ice-violence-and-palantir.

468 Madi Smith, "Maine Nurses Demand Maine Health Cancel its Contract with Palantir Technologies," *Maine Public Health,* May 1, 2026, https://www.mainepublic.org/health/2026-05-01/maine-nurses-demand-maine-health-cancel-its-contract-with-palantir-technologies

469 See: National Nurses United. *Press Releases*. Multiple dates. https://www.nationalnursesunited.org/press

Smith. "Maine nurses demand."

470 Simon Jessup. "Alphabet Investors Push for Safeguards on Use of its Cloud AI," *Reuters,* June 8, 2026. https://www.reuters.com/sustainability/boards-policy-regulation/alphabet-investors-push-safeguards-use-its-cloud-ai-tech-2026-04-29/?utm_source=chatgpt.com.

471 Gabrielle Saulsbery. "Citizens Bank Customers Pull Money Over Lender's ICE Ties," *Banking Dive,* October 23, 2025, https://www.bankingdive.com/news/citizens-bank-customers-pull-money-over-lenders-ice-ties/819223/