/News

The Private Companies Quietly Building a Police State

10/02/2025 UPDATES

By Campaign Zero

From Palantir's data fusion to Clearview's face scraping and Flock's license-plate dragnets, a handful of private vendors now underpin everyday policing—and ICE's deportation machine. Sold as "public safety," these tools supercharge surveillance, stitch together vast personal data, and evade democratic

oversight. Here's what they are, who profits, and how we can shrink police reliance on them.

Overview

Donald Trump entered the White House last January with a promise to carry out the largest mass deportation in United States history. While Trump hasn't made history with the numbers, his administration's policies have led to a dramatic surge in ICE arrests, fueled in part by private technology companies that have made them possible.

Powerful tools that collect and aggregate data, enable facial recognition, and increase surveillance have become a bedrock of American policing over the past two decades. In collaboration with private technology companies, law enforcement agencies at all levels have experimented with how to implement these tools and created a large consumer market for them. Against this backdrop, it is essential to understand the role of the tech industry in both increasing the reach of

local law enforcement and enabling mass deportations by the Trump administration.

The Trump administration has made a public show of its deportation efforts, but the technologies that make it possible have received less attention. ICE is, for example, one of the largest customers for Clearview AI, a facial recognition company that has scraped more than 30 billion faces from internet sources. Data brokers, including one owned jointly by several airline companies, are actively selling data to ICE and other federal agencies. Perhaps most noteworthy is a new $30 million contract between ICE and Palantir to build a platform integrating data from myriad sources to provide "near real-time visibility" of migrants in the country.

Palantir is a defense contractor that builds data integration tools for law enforcement and government agencies–what one former employee describes as "really extravagant plumbing with data." While the company brands itself as a neutral "data infrastructure" provider, Palantir is in reality a largely unchecked force in the expansion of mass surveillance. For example, the company is in conversation with the Trump administration to build and manage systems for the Social Security Administration and the IRS, a move challenged by civil rights groups. Palantir's "plumbing" could lay the foundation for which law enforcement agencies leverage massive troves of private information never intended for police use. Such systems have been used on a smaller scale for years in local police agencies, enabling mass surveillance and, in many cases, exacerbating racist policing.

The surveillance technologies currently used by ICE empower the agency in ways that are both unprecedented and massively expand its reach. But they are also in use far beyond this one agency. Electronic Frontier Foundation, a digital privacy organization, has mapped a wide

range of intrusive technology systems – from surveillance cameras to complex systems like Palantir's – used by local police agencies throughout the country. **Hundreds of companies, many of which began as military and defense contractors, now market their tools to, and develop them in concert with, law enforcement agencies across the United States.**

The significant role of private companies in police technology makes transparency and accountability increasingly difficult: proprietary algorithms are shielded by legal protections, contracts are negotiated outside of public view, and oversight bodies struggle to access or understand these systems. Lawmakers, meanwhile, struggle to keep pace with rapidly evolving technology. The privatization of policing infrastructure allows surveillance tools to proliferate without public scrutiny and operate beyond the reach of democratic governance and oversight.

There are, however, paths forward to prevent the spread of these technologies, safeguard civil liberties, and significantly curtail the growing surveillance power of American police. Campaign Zero's #CancelShotSpotter campaign, for example, has worked to push cities throughout the country to end their contracts with SoundThinking (previously known as ShotSpotter) which makes gunshot detection technology that is both ineffective and poses its own public safety risks. Grassroots coalitions have begun to challenge Palantir; investigative journalists have uncovered deep flaws in these tools; and organizations like EFF have contributed to meaningful lawsuits to curtail surveillance.

This post provides an overview of some of the most impactful and concerning police surveillance technology currently deployed, including the most dangerous companies building these tools for law

enforcement. Many of these systems are already in place, but as they continue to grow in scale, it is imperative that the public is informed to pressure the government to prioritize and demand our rights and safety over corporate interests to surveil and punish.

Deep dive on Critical Police Surveillance Technologies

Category #1: Big Data

Police departments have always collected and tracked data on citizens ensnared by the criminal legal system. But over the past 20 years these databases have evolved into a novel surveillance tool. Police databases are unfathomably large, and store basic personal information about any and all people, even those who have had no prior contact with law enforcement. Although much of this information may appear harmless to some, the reach and scope of police data massively expands police power to track and surveil U.S. residents, and threatens basic privacy rights and civil liberties.

One of the most troubling recent developments in police data is that it **captures information about *all people***. This "dragnet" approach to data collection is designed to give law enforcement maximum access to the entire population, transforming all personal information into potential evidence. Increasingly, law enforcement agencies are opting to purchase this data rather than collect it themselves, exploiting a loophole in Fourth Amendment legal protections. The data broker industry was built to sell personal information to advertisers, but now any police department can purchase access to a database like LexisNexis' Accurint, which contains cell phone numbers, banking history, property records, location history, utility bills, and much more.

Another evolution in police data that has supercharged police surveillance, is the **integration of databases** through platforms like Palantir Gotham and Axon Fusus. Keeping data isolated – referred to as siloed data – is a critical safeguard for privacy, ensuring that personal information related to disparate services like welfare benefits and mental health is used for its originally intended purpose. By cross-referencing an ever-growing list of databases, law enforcement agencies can create and track complex digital profiles for any individual without their knowledge or consent. When one researcher raised concerns over these sprawling systems to an employee of LA County's Chief of Information Office, he dismissed privacy concerns as obsolete: "consent is anachronistic."

Finally, data-driven policing has given rise to **changes in how law enforcement operates**. For starters, this shift has made police increasingly focused on collecting as much data as possible. Some departments use a point system to identify "chronic offenders," and because every "police contact" adds one point, officers are encouraged to constantly stop and question targeted individuals. Implicit and explicit biases mean that data collection is never data neutral, so even as some claim that a focus on data can mitigate racial disparities, research has found that it actually *increases* racial bias in policing. Lastly, data-driven policing has fueled faith in "predictive policing," which police departments continually try to implement even as it has been found to be ineffective and harmful time and again.

Category #2: Facial Recognition/Biometric Tracking

Biometric surveillance relies on collecting, coding, and searching our biological or physical characteristics. This form of surveillance typically uses an algorithm to search for and match data from things like fingerprints, DNA, iris scans, faces, and tattoos. Many understand this

type of forensic data as foolproof investigative information, as portrayed in popular movies and shows about crime. But blind faith in these technologies has led to dragnet collection of our physical features, undermining privacy and civil liberties in the process.

The most alarming development in biometric tracking is that **law enforcement is increasingly expanding its collection of these data across the entire population**. Researchers successfully developed iris recognition technology that can capture and scan a person's eye from nearly 40 feet away, *including in the reflection of a car's side mirror*. Some police departments have begun pressuring people into providing DNA samples at routine traffic stops, an attempt to expand their databases in concert with private companies that store and possibly integrate that data into other systems. Recently, ICE agents have also begun taking photographs of people using an app on their phones that searches Homeland Security databases.

Another key issue is **how police departments use biometric data**. Iris scans and DNA are very reliable for one-to-one matching (e.g., comparing two iris scans), but far less reliable in one-to-many matching (e.g., comparing an iris scan to thousands of scans in a database). Tattoo matching technology is unproven to be effective, and is highly reliant on interpretation, but was nevertheless a key factor in determining whom ICE deported to El Salvador earlier this year. Finally, much of this biometric data is increasingly collected and stored by private companies, raising essential privacy and oversight concerns.

Facial recognition technology is one of the most well-known and alarming forms of modern surveillance. Clearview AI, for example, has scraped 30 billion faces from social media and other sources, and works with law enforcement agencies at all levels, from NYPD to ICE. Its founders have routinely expressed racist beliefs and dystopian visions

of government surveillance, but their technology continues to spread with virtually no oversight. ICE and Clearview are currently finalizing a "sole-source" contract with no oversight mechanisms, which would make Clearview AI the sole provider of facial scans for the federal agency.

Category #3: Video Surveillance Infrastructure

Video surveillance is perhaps the longest standing and most easily recognizable form of modern surveillance technology. It is precisely that familiarity with surveillance cameras, though, that obscures just how ubiquitous and expansive they have become and the level of intrusion into daily life that they impose. Surveillance cameras do not just capture video, but can be equipped with added surveillance technology and create massive networks that significantly expand the reach of the police. In addition, the increasing use of private surveillance cameras often provides law enforcement with easy access to live or recorded footage not intended for that purpose.

Surveillance cameras can be found in nearly all public urban spaces today, and importantly **they are often networked together and fed into central monitoring systems**. Numerous cities have networks of hundreds of surveillance cameras that police can monitor in real time from central hubs. Many departments also add drone and helicopter surveillance cameras into these networks – especially to monitor large events like protests–and mount 360° cameras on the tops of their vehicles. The proliferation of body-worn cameras, which have struck an uneasy balance between increasing surveillance and accountability of police, adds yet another way in which law enforcement can constantly record community members in public.

Importantly, **cameras have also evolved rapidly in terms of the data they can collect**. One of the most well-known examples is Automated License Plate Readers (ALPRs), which record license plate numbers and enable real-time tracking of vehicles. Recently, journalists uncovered that CBP has been accessing Flock Safety's nation-wide network of over 80,000 ALPRs in violation of state law in certain places, like Illinois. Surveillance cameras also enable the expanded use of facial recognition technology, can use advanced technology like thermal imaging, and can even sort images based on factors like gender, clothing, and more. In one demonstration by BriefCam, they show how the software enables rapid review of video based on specific characteristics of individuals, vehicles, and more.

Finally, the widespread adoption of **private surveillance cameras has massively expanded the reach of police surveillance**. Private technologies like Amazon Ring and its accompanying Neighbors app have turned regular homeowners into active participants in the surveillance network. These apps allow users to share footage of "suspicious activity" with neighbors and even with police. Some companies actively promote such integration, as in the case of Motorola's CityProtect system.

Category #4: Digital Street Surveillance

Much of the surveillance that police engage in is entirely invisible. Digital street surveillance has evolved extensively in recent years, driven by an increase in technological capabilities and the proliferation of mobile devices. Law enforcement agencies now have unprecedented access to detailed location data and mobile communications, enabling large-scale monitoring of individuals in public and private spaces. While these tools are often justified as being necessary for solving crimes or protecting public safety, they raise significant concerns about privacy

and constitutional protections, particularly as many of these practices occur without proper judicial oversight.

Three prominent methods currently in use are IMSI capture, geofencing, and real-time location tracking. **IMSI (International Mobile Subscriber Identity)** capture involves devices like the "Stingray" (made by L3Harris) or "dirtboxes," (made by Digital Receiver Technology) which mimic cell towers to trick phones into connecting them. This in turn allows law enforcement to extract SIM card IDs and other data. Once connected, these devices can pinpoint a phone's location and, if the signal is downgraded to 2G, potentially intercept call metadata, texts, and unencrypted communications. Despite this invasiveness, such surveillance is often conducted without a warrant.

Geofencing, unlike IMSI capture, is a legal method that involves obtaining a reverse-location warrant from companies like Google, which holds data on over a billion devices. This technique allows police to collect location data for all devices within a defined area during a specific timeframe, with the goal of identifying suspects. **Real-time location tracking**, meanwhile, leverages data gathered by commercial apps for advertising and sold by brokers such as Fog Data Science and LexisNexis. Such third-party data brokering enables law enforcement to purchase surveillance data often without court approval.

These technologies represent real expansion of dragnet surveillance, in which large groups of people are monitored regardless of suspicion. The use of IMSI capture and data broker purchases often circumvent warrant requirements, while geofencing collects data on innocent individuals en masse. Such practices undermine Fourth Amendment protections against unreasonable searches and seizures and pose serious risks to civil liberties, particularly in contexts like protests or political dissent.

Who You Need to Know in Police Surveillance Technology

Palantir

Who are they?

A U.S.-based technology company that develops data analytics and AI software primarily for national defense.

What technologies do they sell?

- Data Analytics & Fusion Centers (Palantir Gotham, Gotham Europa)
- Predictive Policing tools (crime data analysis and patrol coordination)

Why worry?

Palantir, co-founded by Peter Thiel and initially funded by the CIA, brings military-grade surveillance and predictive policing tools into local law enforcement. Agencies like ICE, NYPD, LAPD, and New Orleans Police use its Gotham system—marketed as *"Your software is the weapons system."* This transfer of military tech to domestic policing raises major civil liberties concerns.

Important Links:

- Palantir Gotham: Europa marketing video
- Primer on Palantir
- LAPD's use of Palantir
- Privacy concerns around Palantir

Clearview AI

Who are they?

A U.S. company that scraped 30 billion+ facial images without consent for its AI-powered facial recognition database.

What technologies do they sell?

- Facial Recognition (AI matching faces to “faceprints”)
- Data Scraping (collecting photos from across the internet)

Why worry?

Clearview has been used by hundreds of U.S. police departments, logging over 1 million searches by 2023. Its massive database, built without consent, effectively places everyone into a perpetual police line-up. Accuracy is unverified, transparency is lacking, and founder Hoan Ton-That has openly embraced dystopian visions of surveillance.

Important Links:

- The Far-Right Agenda Behind Clearview
- Clearview use by U.S. police
- Weak Guardrails on facial recognition
- Settlement in Illinois lawsuit against Clearview
- Clearview and International Law

Axon

Who are they?

A U.S.-based company selling tasers, cameras, and digital evidence tools to law enforcement, military, and security firms.

What technologies do they sell?

- Tasers
- Body-worn cameras
- Evidence.com (cloud-based evidence management)
- Draft One (AI-assisted police reports)
- Axon Fusus (surveillance integration of cameras & tech)

Why worry?

Axon is nearly a monopoly in tasers and police cameras. Its tools enable widespread surveillance of civilians and give the company huge influence over how policing is done. Its corporate interests conflict with democratic accountability.

Important Links:

- John Oliver talks about Axon
- EFF's exposé on Draft One

Geolitica (formerly PredPol)

Who are they?

Sold predictive policing software until 2023, when it was acquired by SoundThinking (ShotSpotter).

What technologies do they sell?

- Predictive Policing algorithms (now rebranded as ResourceRouter)

Why worry?

Geolitica's predictive policing tools were found to be both ineffective and racially biased, disproportionately targeting low-income communities of color. Though Geolitica shut down in 2023, its software lives on under SoundThinking.

Important Links:

- The Markup on predictive policing failures
- SoundThinking's acquisition of Geolitica
- Racial bias in predictive policing

Flock Safety

Who are they?

A U.S.-based company selling automated license plate recognition (ALPR) and vehicle tracking systems.

What technologies do they sell?

- Drones (Flock Aerodomes)
- License Plate Recognition (vehicle fingerprinting cameras)

Why worry?

Flock enables mass, warrantless surveillance, often targeting immigrants, communities of color, and even women seeking reproductive care. Their massive ALPR network captures sensitive data with little oversight.

Important Links:

- EFF on Flock ALPR
- Controversy over Flock's "Nova" tool
- Flock cameras used to track abortion seekers

LexisNexis

Who are they?

A U.S. data analytics company creating databases from public and third-party sources.

What technologies do they sell?

- Data Brokering
- Accurint (law enforcement data integration platform)

Why worry?

LexisNexis acts like a "virtual fusion center," creating massive digital profiles often over 260 pages long. Its databases are sold to hundreds of police agencies, bypassing traditional legal protections. ICE has used its data millions of times.

Important Links:

- How LexisNexis works
- Legal Challenge to LexisNexis
- LexisNexis & ICE

DJI

Who are they?

A Chinese company and the world's leading drone manufacturer.

What technologies do they sell?

- Drones with cameras, thermal sensors, and surveillance features

Why worry?

DJI drones are widely used by law enforcement without clear regulations or warrants, enabling stealth surveillance. Recent U.S. executive orders aim to reduce reliance on foreign-made drones, targeting DJI specifically.

Important Links:

- DJI and modern warfare
- Congress moves to ban Chinese drones

Motorola Solutions

Who are they?

A U.S. legacy company providing communications and surveillance tools since the 1920s.

What technologies do they sell?

- Radios for law enforcement
- Body-worn cameras
- ALPR contracts (with 60+ departments)
- CityProtect (private camera registry for police access)
- Command Center Software Suite (AI-integrated mapping & data)

Why worry?

Motorola has quietly become a key surveillance vendor, integrating private data and cameras with law enforcement systems. Its ecosystem creates massive surveillance reach with little transparency.

Important Links:

- Command Center Suite
- Command Central Community
- EFF report on Motorola

L3Harris Technologies

Who are they?

The 6th largest U.S. defense contractor, formed by a 2019 merger of L3 Technologies and Harris Corporation.

What technologies do they sell?

- IMSI Catchers (“Stingrays”) for cell phone tracking
- Drones and surveillance balloons

Why worry?

Best known for the Stingray, which captures phone data en masse, L3Harris plays a major role in militarizing domestic policing. Though local sales stopped, federal agencies (especially ICE) still use their tools.

Important Links:

- Milwaukee PD hides Stingray use
- Overview of L3Harris
- L3Harris seeks to buy Israeli spyware firm
- FOIA on Stingray costs

Digital Receiver Technology (DRT)

Who are they?

Specialize in covert phone interception for military, intelligence, and police.

What technologies do they sell?

- Cell-Site Simulators (“DRTboxes”)

Why worry?

DRTboxes function like Stingrays, mimicking cell towers to intercept calls and data—often without warrants. They enable dragnet surveillance across wide areas.

Important Links:

- Texas Guard used DRTboxes on planes
- Chicago & LA's decade of dirt box use

Fog Data Science

Who are they?

A U.S. company founded by ex-DHS officials, specializing in smartphone location tracking.

What technologies do they sell?

- Data brokering (location data from mobile apps)

Why worry?

Fog sells real-time and historical phone location data to police, letting agencies bypass warrants. This reflects the broader dangers of the unregulated data broker industry.

Important Links:

- EFF overview of Fog
- Police use Fog Reveal to track abortion seekers

Find more in: UPDATES

Additional tags: ACCOUNTABILITY BODY-WORN CAMERAS FEDERAL SHRINK THE RELIANCE AND POWER OF THE POLICE UNITED STATES

SHARE TWEET EMAIL

Up Next

VIEW ALL NEWS

09/26/2025

07/24/2025

Campaign Zero and Win NYC Host Back-to-School Bash for Over 600 Children and Families

Summer Series at Cuyahoga: Transformation in Action

06/27/2025

04/04/2025

Michael Brown's Legacy Lives Through Them

Supporting Youth with Transformative Programming

Help us end police violence in America.

Your Email Address

JOIN US

We Will Win.

community@campaignzero.org