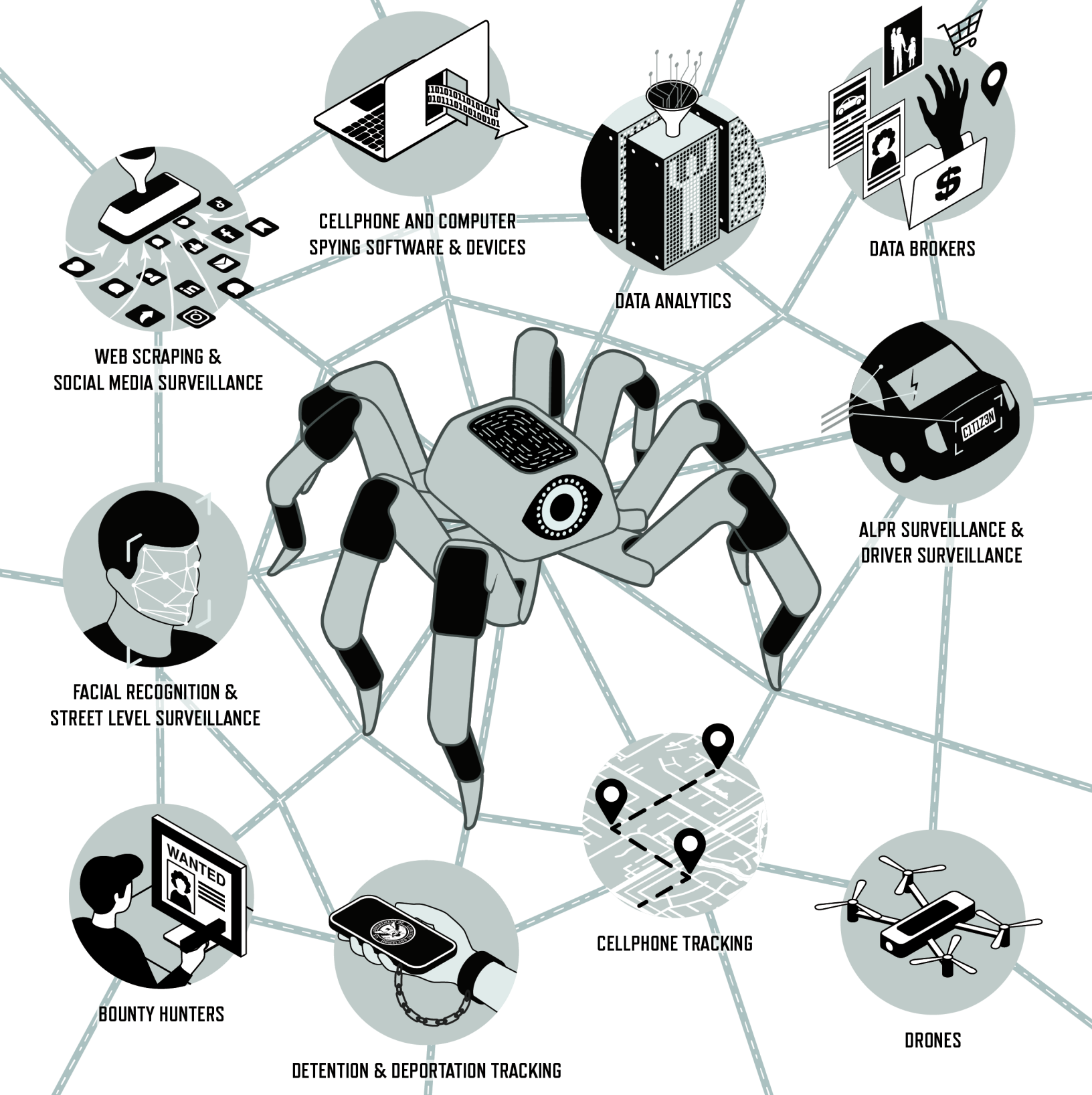
ICE's Top 10 Surveillance Technologies

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.

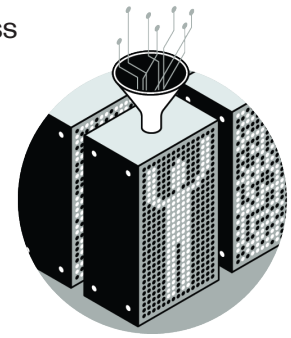


1. Data Brokers

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:

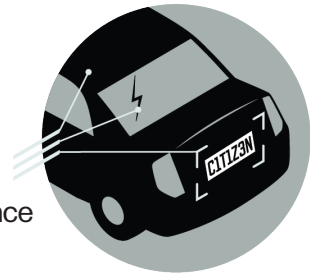
- ICE and CBP use surveillance products from **Babel Street,** a social media monitoring company that allows customers to search a name, email, or phone number and pull up associated social media posts, IP addresses, job history, and more. ICE reportedly uses **Babel's Locate X** product to monitor cell 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.

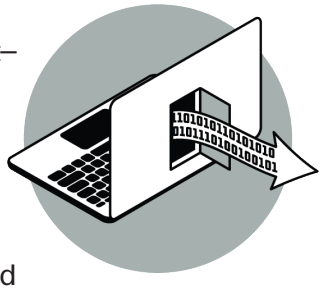
5. Nationwide Driver Surveillance



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.

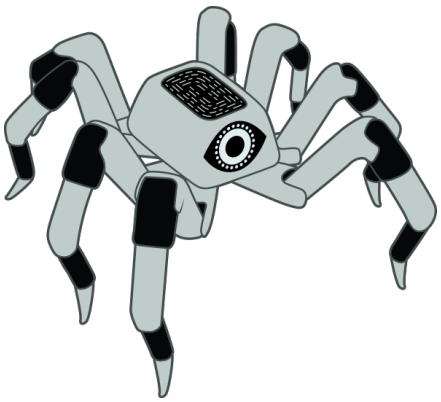
1 ICE officials have stated that they consider an identity "match" in Mobile Fortify to be a "'definitive" determination of a person's citizenship status and that an ICE officer may ignore a birth certificate or other evidence of US citizenship if the app states otherwise. In other words, even if you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