FIGHT FOR THE FUTURE

ICE’s Surveillance Technology

ICE operations are supported by a web of public and private surveillance. Many of these systems predate the current administration, but ICE has moved quickly to acquire new tools using their massive new slush fund. Immigrants, protesters, and anyone unlucky enough to be racially profiled by ICE are getting caught up in this web. ICE’s use of surveillance systems is a direct threat to the civil rights of those being monitored and is being used to enable further abuses. Reforms in the wake of DHS agents killing legal observers must break this web of surveillance and not unintentionally provide the agency with new surveillance tools. Demands like more funding for body cameras would simply be a new input for the surveillance machine.

The Dangers of Trickle Up Surveillance

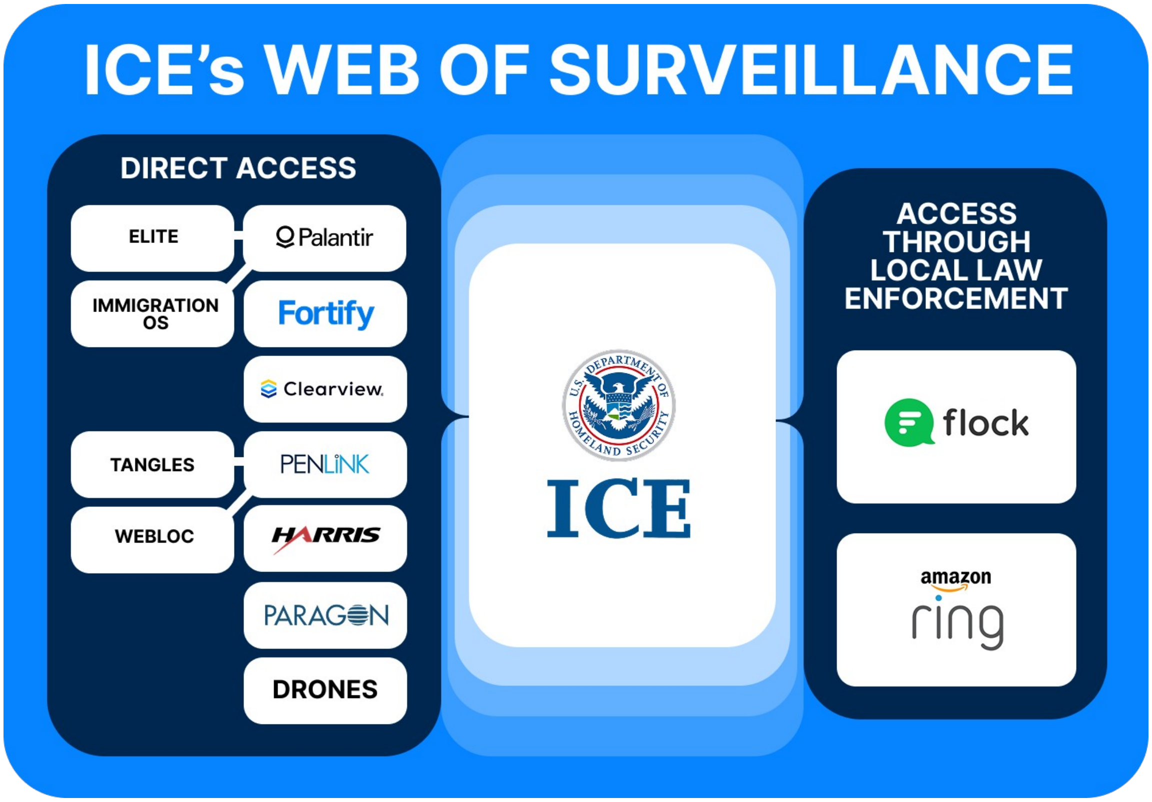
Private and local surveillance systems are funneling data to ICE through data sharing agreements. Footage from Flock cameras is often shared between local law enforcement agencies, with many conducting queries on behalf of ICE or even giving DHS agents credentials to directly access their databases. Soon, Ring doorbell camera data will be added to Flock’s massive network. ICE also uses state drivers’ license databases to power their internally developed Mobile Fortify facial recognition app. Commercial location data, used for targeted advertising, is purchased directly by the government or through apps like Webloc. Meta-database tools that ICE uses, like Palantir’s ELITE, combine data from a number of sources including HHS and U.S. Citizenship and Immigration Services. The data that ICE can access has the potential to feed into a massive surveillance operation.

Surveillance is Being Used to Threaten Protesters and Observers

Agents have repeatedly used these systems to intimidate and harass protesters and legal observers. Legal observers in Maine and Minneapolis have reported federal agents showing up at their homes to threaten and intimidate them. Several observers who were following ICE vehicles have reported being led back to their homes, after having their license plate or face scanned. Others have reported ICE showing up at their homes to deliver threats after recording an encounter. This use of surveillance systems is transparently intended to chill speech and discourage lawful attempts to document their actions. The chilling effect of these threats is amplified by the apparent impunity enjoyed by ICE agents who kill or injure observers.

More Surveillance Won’t Fix This

Alex Pretti’s murder was captured by multiple body cams. Body cameras did not deter CBP agents from killing him in broad daylight. This footage is in the hands of an organization which routinely ignores court orders and has been subject to no meaningful congressional oversight under Trump. A body cam mandate would solve nothing and would give the DHS even more material to feed into facial recognition to build their list of “domestic terrorists.”



Meta Surveillance Databases: Palantir provides two meta-database products to ICE. Enhanced Leads Identification & Targeting for Enforcement (ELITE) provides map-based dossiers of targets and is used to find areas to raid. ImmigrationOS provides near real-time tracking of immigrant movement.

Facial Recognition Technology: ICE uses several facial recognition systems. Mobile Fortify compares faces to federal databases, including TSA's massive facial recognition database. Clearview AI harvests photos from the internet to provide facial recognition services.

Data Broker Access: ICE uses Penlink's Webloc to access detailed cellphone location data both in real-time and retroactively. It can be used to identify all phones in an area or track individual phones.

Social Media Surveillance: ICE uses Penlink's Tangles to identify people and then do sentiment analysis based on their social media presence.

Cell Site Simulators: Known by the brand name Stingray, cell site simulators trick phones into connecting to them by spoofing a cell tower and can gain access to location data, voice calls, texts, and internet traffic.

Image and Video Collection: ICE uses a number of sources of images and video for it's surveillance databases: officer recordings, drones through CBP, and Flock and Ring through local police.

Spyware: ICE has a $2 million contract with Paragon, a company that makes country-level spyware products. It is not known at this time what this contract is for.