

The mass surveillance infrastructure of Trump's assault on immigrants and protesters

Kevin Reed
2 February 2026

Several recent media reports have revealed the Department of Homeland Security (DHS) has assembled a complex surveillance apparatus that merges biometric identification, mass data collection and predictive policing tools to target both immigrants and citizens alike. This sprawling system is being used to track and locate individuals for apprehension, detention and violence by lawless gangs of Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP) agents.

Awareness of this infrastructure has grown following the public assassinations in Minneapolis of anti-Trump activists Renée Good, who was murdered at point blank range by ICE officer Jonathan Ross on January 7, and Alex Pretti, who was beaten and murdered execution-style by CBP thugs who have yet to be named, on January 24.

In flagrant violation of core constitutional rights, including the First, Fourth and Fourteenth Amendments, this surveillance infrastructure represents the consolidation of a domestic spying regime aimed at suppressing opposition to the government's anti-immigrant crackdown and its broader policies of war and social counterrevolution.

Reports in the *New York Times* and *Washington Post* describe how ICE, CBP and other DHS components have deployed facial recognition apps, license plate databases, cell phone location tracking, AI-driven "target maps," social media monitoring and drones against both undocumented workers and citizens participating in protests.

These technologies are integrated through platforms built by companies like Palantir under multimillion-dollar contracts to compile dossiers that fuse immigration records, travel data, Social Security files, commercial data brokers' feeds and social media activity into a single, continuously updated system.

This network directly is being used to attack rights to free speech, protest, association and the press, by identifying, tracking and blacklisting those who oppose the government, including legal observers and bystanders filming ICE operations. It also violates constitutional protections against unreasonable searches and seizures, through warrantless facial scans, mass cell phone location tracking, dragnet license plate collection and data mining via fusion centers and private brokers.

Finally, the clandestine surveillance apparatus contradicts due process and equal protection guarantees of immigrants and protesters who are being placed under automated suspicion, often misidentified and subjected to raids, detention and even lethal violence without legal recourse.

DHS officials have acknowledged that facial recognition and other tools are routinely used in the streets without consent and civil rights organizations have warned that there is no effective government framework limiting these practices. As one ACLU attorney put it, the combination of these technologies is giving the state "unprecedented capabilities." Such capabilities are a component part of the police-state

apparatus being erected by the Trump administration across the country.

On January 28, the WSWS published a perspective entitled, "Was Alex Pretti the subject of a targeted assassination?" which argues that the killing of the beloved Minneapolis ICU nurse and legal observer by federal agents "was a targeted assassination carried out by the Trump administration's paramilitary forces in order to terrorize Minneapolis citizens opposing and recording its criminal activities."

CNN and other outlets confirmed that roughly a week before his murder, Pretti had intervened when he saw ICE agents chasing a family, blowing a whistle and shouting at the agents, who then tackled him, broke his rib and later described him as "known to federal agents."

The WSWS perspective notes that cellphone video from January 24 shows Pretti intervening to protect a woman knocked to the ground, being tackled, disarmed and held face-down while one agent removed his holstered firearm, after which another agent pushed this colleague aside and fired four shots into Pretti's back, followed by six more shots into his motionless body.

The article concludes: "Emerging evidence strongly indicates that the murder of ICU nurse Alex Pretti by federal agents on January 24 in Minneapolis was a targeted assassination."

Critically, the WSWS explained that Pretti and fellow observer Renée Good were already being tracked by ICE and CBP through centralized systems that collect license plates, IDs, photographs and video of "agitators," with Palantir and similar vendors compiling lists of protesters and those filming immigration operations.

A DHS memo obtained by CNN ordered agents to gather such data for a "centralized surveillance database," making it overwhelmingly probable that Pretti's earlier confrontation, his identity, his vehicle details and his role as a documenter of ICE abuses were recorded and flagged well before the fatal shooting.

This context—combined with the bystander video evidence and the prior assault by ICE agents—makes the likelihood of a targeted political assassination on US soil not only plausible but compelling. The use of body-camera footage—partially withheld from the public—to reconstruct events further underscores how every interaction with these agencies is now mediated by a digital infrastructure that can be selectively used to justify or conceal state violence.

The surveillance toolkit fielded by DHS and its partners is extensive and expanding. Among the known tools are the following:

- **Mobile facial recognition (NEC's Mobile Fortify and similar apps):**
 - *Purpose:* Instantly match face scans against "trusted source photos" including passport, driver's license, immigration and watch list databases.
 - *Use:* ICE and CBP agents point phone cameras at people in the street, at

traffic stops and at protests to verify identity and immigration status; numerous citizens in Minneapolis report being scanned without consent near demonstrations against ICE.

- **Iris?scanning and other biometrics:**

- *Purpose:* Rapid biometric confirmation at close range, often integrated with mobile devices.

- *Use:* Deployed in field operations, detention centers and border zones to enroll migrants in databases that can track them indefinitely and flag them whenever they interact with state institutions, from airports to local police.

- **Automated license?plate readers (ALPRs):**

- *Purpose:* Capture and store images of vehicle plates, locations and times, building a historical map of movements.

- *Use:* ICE purchases mobile readers from Motorola Solutions and taps into commercial systems like Thomson Reuters' 20?billion?record database, as well as local police networks and Flock Safety cameras, to track where the owners of targeted vehicles live, work, attend meetings and protest.

- **Cell?phone location tracking (Stingrays and bulk data):**

- *Purpose:* Use cell?site simulators that mimic towers, and commercial location data, to identify and follow mobile devices in real time.

- *Use:* Agents can either search for a specific device or sweep entire areas around protests and immigrant neighborhoods, mapping networks and identifying who attends demonstrations or visits targeted homes.

- **Digital forensics and device exploitation (Cellebrite, Paragon, others):**

- *Purpose:* Break into locked phones and computers, bypass encryption, extract and recover deleted files, messages and app data.

- *Use:* Once ICE or CBP seize a device—during raids or arrests, at checkpoints—specialized teams use these tools to download years of communications, contacts and media, feeding this data into central systems for further analysis and cross?matching.

- **AI?driven ImmigrationOS and Palantir targeting platforms:**

- *Purpose:* Integrate multiple data streams—immigration records, travel histories, commercial databases, social media, license plates and biometrics—into a single map?based interface that assigns “confidence scores” to addresses and individuals.

- *Use:* A Palantir app shows agents a map dotted with “potential deportation targets,” providing dossiers that include names, photos, Alien Registration Numbers and calculated likelihood of presence at given locations, effectively automating where to raid and whom to prioritize.

- **Social?media monitoring and data?broker contracts:**

- *Purpose:* Monitor platforms such as X, TikTok, Instagram, Facebook, YouTube and Reddit around the clock, scraping posts and metadata to identify organizers, slogans, locations and networks.

- *Use:* ICE has assembled teams that track protest hashtags, livestreams and viral clips of raids, linking online speech to physical identities via facial recognition, IP tracing and data purchased from private brokers.

- **Drones and aerial surveillance (including MQ?9 Predator):**

- *Purpose:* Provide persistent overhead monitoring of wide areas, using high?resolution cameras and, in some cases, signals?intelligence payloads.

- *Use:* Small drones have been deployed over immigration protests, while CBP flew a military?grade MQ?9 Predator over anti?ICE demonstrations in Los Angeles, demonstrating the fusion of foreign?war technology with domestic repression.

- **Fusion centers and nationwide data sharing:**

- *Purpose:* Aggregate data from federal, state and local police, as well as private sources, under DHS coordination.

- *Use:* Fusion centers act as clearinghouses for Suspicious Activity Reports, gang databases and immigration “intelligence,” allowing ICE, CBP, FBI and local departments to share watch lists and surveillance data outside traditional warrant procedures.

- **Body?worn cameras and “evidence” management systems:**

- *Purpose:* Record encounters and feed video into analytic tools, including face recognition and pattern detection.

- *Use:* Though DHS scaled back plans for universal ICE body?cams, some agents involved in the Pretti killing wore them, and the selective release or suppression of this footage is part of how the state shapes the narrative of its own crimes.

Each tool, taken alone, undermines basic rights. In combination, these technologies are an integrated apparatus of population control directed especially against immigrants and political opponents of Trump’s presidential dictatorship drive.

Civil rights lawyers and privacy advocates have sounded the alarm over this expansion. The ACLU has warned that what is at stake is not isolated abuses but a structural capacity for continuous monitoring of entire communities. The US Commission on Civil Rights has previously documented, for example, how facial recognition programs raise grave concerns around accuracy, discrimination, lack of oversight and barriers to challenging misuse, particularly for poor and minority populations.

A former CBP adviser now at the Center for American Progress notes that DHS has access to a “vast amount of trade, travel, immigration, and screening information,” and explicitly warns that “everyone should be alarmed at the possibility of this data being weaponized for inappropriate reasons.” Others have called for shutting down all DHS fusion centers and ending information?sharing pipelines and predictive?policing programs such as those devised by Palantir because they violate Fourth Amendment protections and enable dragnet targeting of immigrants and working class communities.

The warnings point to the fact that ICE and CBP are not rogue actors but spearheads of a bipartisan assault on democratic rights by the Trump administration using vulnerable sections of the population such as immigrant workers for testing purposes. Their “highly targeted” operations, as DHS officials euphemistically describe them, are in fact mass sweeps backed by data systems deliberately insulated from public scrutiny and judicial review.

For more than two decades, the *World Socialist Web Site* has warned that the “war on terror” launched after September 11, 2001, provided the pretext for building a comprehensive surveillance and repressive apparatus that would be turned inward against the working class. The Snowden revelations in 2013 exposed the National Security Agency’s (NSA) bulk collection of Americans’ phone records and its PRISM program to harvest emails, photos and other content from major internet companies, revealing that the intelligence agencies were systematically lying about domestic spying and working directly with the telecom and tech monopolies.

In January 2014, then-President Obama announced that the NSA’s bulk data collection operation was being ended and, in June 2015, the USA Freedom Act was signed into law formally claiming that mass surveillance was being halted. However, as Edward Snowden himself pointed out, these programs continued in more sophisticated forms.

In 2020, a federal appeals court ruled that the NSA’s telephone metadata dragnet was illegal and likely unconstitutional, confirming that the state had violated both statutory limits and constitutional protections on a vast scale. Yet rather than dismantle this machinery, successive administrations—including Obama, Trump and Biden—adapted it, shifting from overt NSA programs to a more fragmented system of policing, immigration and “homeland security” surveillance that relies heavily on private contractors, data brokers and fusion centers.

The present DHS technology stack—Palantir’s real?time tracking platforms, AI?driven targeting, ubiquitous biometric collection and corporate data?broker feeds—represents the continuation, not the abandonment, of the system exposed by Snowden. It has been repurposed to criminalize immigrants and dissenters.

The integration of Social Security records with immigration databases discussed in internal DHS communications shows that the same logic of total information awareness is now being applied to every aspect of social life, from work to travel. Moreover, the recent attempt by Trump's Attorney General Pam Bondi to blackmail the state of Minnesota into handing over its databases of Medicaid and SNAP benefit recipient data and voter registration data is particularly ominous.

The WSWS has consistently argued that mass surveillance is not an aberration but a necessary instrument of a ruling class preparing for deepening war abroad and class conflict at home. The targeted killing of figures like Alex Pretti, selected through these systems because they dared to oppose the regime, is the outcome of this trajectory.

The exposure of DHS's surveillance infrastructure—including the role of tech corporations, data brokers and a vast network of "fusion" partnerships—demonstrates that democratic rights cannot be defended within the framework of capitalism. A state that protects the wealth of a tiny oligarchy amid staggering inequality, domestic militarization and imperialist war will inevitably treat immigrants, protesters and workers as enemies to be monitored, controlled, suppressed and killed.

The working class, which produces everything in society and operates the very technologies being used by the state, is the only social force capable of dismantling this machinery. The ICE and CBP repressive apparatus and the entire system of immigration raids, detention and deportation must be abolished and the full legalization and equal rights of all immigrants guaranteed. DHS fusion centers, predictive policing and data broker contracts, facial recognition and mass biometric collection by the state must be shut down.

The tech giants and surveillance contractors like Palantir and critical infrastructure must be seized and placed under the democratic control of the working class to address social needs, not the profits and repressive requirements of the capitalist oligarchy. The struggle against surveillance and police state measures must also be linked to the fight against war, austerity and authoritarian rule. Only the conscious, independent mobilization of the working class in the struggle for socialism can halt the descent into dictatorship and secure a future for workers and young people free of police repression and based on genuine democratic rights for all.



To contact the WSWS and the
Socialist Equality Party visit:

wsws.org/contact