PALANTIR & THE POLICE STATE

How one tech company is helping build the machinery of mass surveillance and deportation

Use this zine to start a conversation

"Seeing Stone" to Surveillance Empire

Palantir takes its name from Tolkien's palantír, a seeing stone that lets the powerful spy on anyone and twist what they see.

In the real world, Palantir builds AI "seeing stones" for governments, militaries, and police. Its software ingests oceans of personal data (social media, financialrecords, biometrics, location data) and turns them into dossiers and "risk scores" on real people.

Billionaire co-founder Peter Thiel and CEO Alex Karp have used these tools to win billions in U.S. government contracts.

Palantir as ICE's Nerve Center

For over a decade, Palantir has been the digital backbone of ICE. Its systems (FALCON, Investigative Case Management, ImmigrationOS, and now tools like ELITE) pull in data from passports, Social Security, tax records, license-plate readers, even health agencies. These platforms help ICE map neighborhoods, track "self-deportation," prioritize who to arrest, and coordinate raids and deportations on a massive scale. When ICE agents surround day labor corners or show up at people's homes, they're often acting on Palantir-built lists.

Toward a Super-Database on Everyone

Under Trump, Palantir's role expanded from immigration to a potential "super-database" on virtually everyone in the United States. An executive order pushed agencies to pool data from Homeland Security, Defense, Health and Human Services, Social Security, IRS, and more. Palantir was tapped to make it all searchable and actionable.

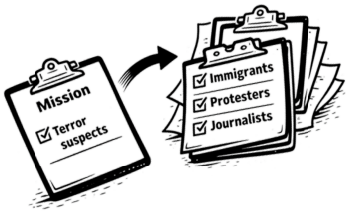
With that kind of integrated system, the same tools used to hunt immigrants can be turned on political opponents, journalists, or anyone who angers those in power.

Algorithms as Secret Law

IPalantir claims it "just provides the tools." But in AI systems, design is policy.

Choosing which data to include, what triggers an alert, and how risk is scored quietly decides who gets targeted and who is ignored. Past algorithms used in criminal justice have falsely labeled Black people "high-risk" at far higher rates than white people, feeding judges biased "neutral" scores. ImmigrationOS and similar tools risk automating that same injustice: quietly labeling people as threats, with no transparency and almost no way to appeal.

Mission Creep: From Hospitals to Workplaces



Once Palantir's systems are in place, they tend to spread. At JP Morgan, for example, Palantir tools encouraged constant surveillance of workers until investigators were even monitoring top executives.

Police in U.S. cities have quietly used Palantir to build lists of "persons of interest" and map over-policed neighborhoods, creating feedback loops that justify even more surveillance.

Power, Profits, and Contempt for Democracy

Palantir sits at the crossroads of tech oligarchs and authoritarian politics. Thiel has written that since women got the vote and social programs expanded, "capitalist democracy" is basically an oxymoron. He and fellow billionaires like Elon Musk have poured money and staff into Trump's administration, while Palantir's CEO boasts that their software exists to "scare enemies and on occasion kill them." As deportations ramp up, Palantir's ICE contracts keep growing —turning human suffering and weakened civil liberties into a lucrative business model.

What We Can Do

This story isn't just about tech. It's about who gets to live freely in a democracy. We can:

- **Demand** that cities, universities, companies refuse or cancel contracts with Palantir and other surveillance vendors.
- **Push** Congress and local officials to ban Palantir from immigration enforcement and block any national "super-database."
- **Support** immigrant-led groups, legal defense funds, and rapid-response networks that support ICE victims.

It's Blue Turn

JOIN OUR FIGHT FOR DEMOCRACY

Regular Meetings and Actions in SF Bay Area