

COVID19 POLICING PROJECT

We are continuing to track enforcement of public health and quarantine orders through police stops, harassment, tickets, fines, and arrests — and increased risk of exposure to COVID-19 through protest policing tactics. Please let us know what's happening in your community through the [reporting form](#) at covid19policing.com or by emailing covid19policing@gmail.com!

Also, check out this recent [article](#) emphasizing that protests have not increased COVID-19 infection rates — the problem isn't protests, it's policing!

Surveillance, Tech Companies, and COVID-19 Policing

State surveillance, coupled with policing, is broadly expanding under the pretext of managing the COVID-19 public health crisis, with technology playing a key role. While the Department of Homeland Security and CBP recently deployed drones to spy on protesters in [15 cities](#), capturing over 270 hours of surveillance footage, ***the NYPD is reportedly in negotiations with the tech company Draganfly about its “[pandemic drone](#),” which can detect temperatures, heart rates, and respiratory rates from an aerial distance of 190 feet.*** None of the symptoms tracked by the pandemic drone are definitive signs of coronavirus, while the level of intrusion into individual bodily integrity posed by such surveillance is deeply concerning. This convergence of police surveillance technology with COVID-related biometric tracking is an alarming outgrowth of the state's carceral approach to public health.

Data-sharing is a major site of expansion for state surveillance under the pandemic. Our last [update](#) details how public health departments in many states have shared confidential patient information with law enforcement, endangering the safety and health of communities bearing the brunt of the pandemic. Police unions recently won a [court decision](#) in Erie County, Pennsylvania ***mandating health departments to give arresting officers information about arrestees' COVID-19 status*** — reasoning that if a person is being arrested and is positive for COVID-19, they likely have broken quarantine rules (which would not be the case if the person was arrested in their home, or is arrested on their way to or from seeking medical care, for instance).

Advocates are resisting information sharing about COVID-19 status with law enforcement, and have pushed legislators in New York to introduce legislation that would ban police and

immigration enforcement from accessing the vast troves of personal information collected through contact tracing.

While surveillance and [data-sharing](#) technology have always been central to policing tactics, recent developments in machine learning and digital spying have enabled law enforcement to integrate different systems of criminalization in unprecedented ways. What's less known is the role that private tech companies currently play in brokering COVID-19 personal health data between various federal agencies, health departments, and law enforcement.

Government collaboration with Big Tech is accelerating COVID-19 criminalization

Tech corporations are eager to profit from the growing pandemic as a lucrative new market under [surveillance capitalism](#). From contact tracing apps to quarantine monitoring devices, many companies are now in the business of developing [carceral technology](#) products to assist police in enforcing COVID-19 public health orders and help business owners monitor workers for “compliance.” Wearable ankle monitors — what Media Justice refers to as “[digital prisons](#)” — are the main tech tool used to detain people under house arrest. ***Some [cities](#) have resorted to using ankle monitors to track the GPS location of people under court-ordered quarantine.*** The same companies that specialize in house-arrest monitors are now marketing similar devices to government agencies for the purpose of [quarantine enforcement](#).

As federal, state, and local governments ramp up their contact tracing systems, they are working closely with private tech companies to capture and share personal health data for surveillance. ***The Department of Health and Human Services (HHS) announced a new program, ‘[Protect Now](#),’ which consolidates data from COVID-19 patient records, contacts, and hospital stays onto a single platform managed by Palantir Technologies. This data is then shared among government agencies without consent, accountability, or transparency.*** HHS received \$500 million from the CARES Act for surveillance and paid Palantir over \$24 million. Personal health data is becoming an ever more valuable commodity to tech companies hoping to land big government contracts during the pandemic.

Palantir, along with Amazon and Google, are well established players in the surveillance economy. These companies have had a direct hand in tracking and detaining Black, Indigenous, and migrant communities. According to a [report](#) by Mijente, ICE hired Palantir to create an “Integrated Case Management” system to collect massive volumes of personally identifiable information that it shared across data systems at all levels of government. Palantir’s [software](#) helped ICE to arrest and deport undocumented families. LAPD also hired Palantir to analyze data from its “Chronic Offender Bulletins,” which targeted communities of color for surveillance under LAPD’S “[predictive policing](#)” program.

What's being done about it:

[Just Futures Law](#), [MediaJustice](#), [Mijente](#), and the [Immigrant Defense Project](#) announced they have filed Freedom of Information Act (FOIA) and public record requests to demand [information](#) from the Trump administration about the personal health data being collected and shared through secretive contracts with tech companies engaged in COVID-19 surveillance.

[Follow](#) their work for updates on exposing and dismantling COVID-19 data-sharing agreements between government and big tech.

Recommendations:

- **Cancel contracts with tech companies** who collect and share people's personal health data for COVID-19 surveillance.
- **Prevent and dismantle the integration of data systems** between federal agencies, health departments, and law enforcement.
- **Support legislation to ban public health departments from sharing data with law enforcement agencies and private tech contractors.** Proposed bills that ban health departments from sharing data with police and immigration enforcement should also include tech data-brokers.