# CBP does end run around warrants, simply buys license plate-reader data

Enlarge / A worker for repo firm Relentless Recovery in Cleveland, Ohio, backs a car equipped with automated license plate recognition cameras out of the garage before going out to scan for cars that need to be repossessed on April 30, 2018.

## reader comments

161 with 86 posters participating

## Share this story

US Customs and Border Protection can track everyone's cars all over the country thanks to massive troves of automated license plate scanner data, a new report reveals—and CBP didn't need to get a single warrant to do it. Instead, the agency did just what hundreds of other businesses and investigators do: straight-up purchase access to commercial databases.

CBP has been buying access to commercial automated license plate-reader (ALPR) databases since 2017, TechCrunch reports, and the agency says bluntly that there's no real way for any American to avoid having their movements tracked.

"CBP cannot provide timely notice of license plate reads obtained from various sources outside of its control," the agency wrote in its most recent privacy assessment (PDF). "The only way to opt out of such surveillance is to avoid the impacted area, which may pose significant hardships and be generally unrealistic."

When reached by TechCrunch for comment, CBP spokesperson Matthew Dyman told the site, “How would you be able to opt out of a license plate reader? Can I opt out of speed cameras here in DC?”

A different spokesperson told Vice Motherboard that the agency uses commercial ALPR databases for tasks such as “locating and apprehending the subjects of criminal investigations, illicit activity, or aliens who illegally entered the United States.”

Previous reporting by Vice led the site to conclude that CBP is likely contracting with a company called Vigilant Solutions, but the agency would neither confirm nor deny Vice’s questions, and the company did not return Vice’s requests for comment.

## Get a warrant

Thanks to the US Constitution and decades of case law, there are rules about what data law enforcement agencies can collect directly. For example, the Supreme Court in 2018 ruled that police and other investigators need a search warrant in order to obtain an individual’s mobile phone location data.

The warrant process also allows courts to push back on overbroad requests for information from law enforcement. A judge pushed back on the Department of Justice’s 2017 attempt to get records of more than 1.3 million IP addresses that visited a website organizing a protest against President Donald Trump, for example.

Massive, privately owned databases, however, so far seem to provide a convenient end run around the warrant process. CBP already buys cell phone location data, even though it would not legally be able to hoover it up on a wide scale directly. Police also purchase hacked and breached data from third-party vendors that they can then use to track and identify individuals in ways that otherwise might have required a

warrant.

Although hundreds of jurisdictions nationwide use automated plate-scanning technology, fewer than 20 states have laws of any kind on their books governing the collection, use, and storage of ALPR data. Even fewer of those laws specify what private entities can collect ALPR data and what can be done with that information. The software also seems to become more granular almost by the day.

Theoretically, CBP only has authority to operate within 100 miles of the US border. The data it purchases, however, may allow it to track any given license plate basically anywhere in the country.

## Public-private muddy waters

CBP writes in the privacy assessment that the ALPR data to which it has access comes from "both public and private sources," including but not limited to "private businesses (e.g., parking garages), local governments (e.g., toll booth cameras), law enforcement agencies, and financial institutions."

The technology itself continues to spread—not just to businesses and private investigators, but also to individual consumers. A company called Rekor began marketing ALPR technology, adapted for home-surveillance use, to consumers in January of this year. In April, Ars reported on a leaked survey that showed Amazon floating the idea of ALPR integration into Ring security cameras to some of its customers.

Ring now boasts more than 1,400 active partnerships with local law enforcement agencies all over the country. Police in those towns, cities, and counties are able to request footage from homeowners who use Ring surveillance products. The addition of plate-scanning software to something as widespread as Ring

doorbell cameras would then give thousands of police departments potential access to that kind of data as well—regardless of what laws states have on the books about law enforcement use of ALPR.

https://arstechnica.com/?p=1692626