

US government using license plates to track movements of millions

Eric London
18 July 2013

A report issued by the American Civil Liberties Union (ACLU) on Wednesday [<http://www.aclu.org/alpr>] details an immense operation through which nearly 1 billion license plate records of hundreds of millions of drivers are tracked and huge databases are amassed, providing the American government with access to the history and recent whereabouts of the majority of the US population.

For years, a network of federal security agencies, local police departments and private companies have been using automatic license plate readers on police cruisers, in parking lots, at traffic intersections—even through smartphone apps—to photograph cars and their drivers and to record license plate numbers with the matching time, date and location.

“More and more cameras, longer retention periods, and widespread sharing allow law enforcement agents to assemble the individual puzzle pieces of where we have been over time into a single, high-resolution image of our lives,” the report says.

“The systems can also plot all vehicles at a particular location, such as the location where a crime—or a political protest—took place” through a procedure called “geofencing,” whereby “law enforcement or private companies can construct a virtual fence around a designated geographical area, to identify each vehicle entering that space.”

The use of this technology for such authoritarian procedures gives the lie to the claims of the government and security apparatus that the purpose of the license-tracking program is to stop crime.

In Maryland, for example, where license plate trackers stored over 85 million license plate reads in 2012 alone, only 0.2 percent of those license plates were matched to any suspected unlawful activity. Of the 0.2 percent, 97 percent of those were for violation

of state registration or smog check programs.

However, the data on the whereabouts of all 85 million plates in Maryland is stored in a state fusion center, the Maryland Coordination and Analysis Center (MCAC), which is then shared with a regional database called the National Capital Region License Plate Reader Project (NCR). According to the NCR, “any law enforcement agency” can take license plate data and “retain it indefinitely.”

Regional databases similar to the NCR exist across the country to help circumvent individual state limitations on the length of time for which license plate and travel data can be held. Though not referenced in the ACLU report, the aggregated license plate data from all state and regional databases are likely compiled and stored indefinitely by the National Security Agency alongside the DNA and ID photograph records and Internet and phone communications of the vast majority of people in the US.

The depth of the involvement of the national security apparatus is evidenced by the “billions of dollars in grants” that the Department of Homeland Security (DHS) has provided through the DHS Security Grant Program and the Infrastructure Protection Program. Remarkably, license plate tracker manufacturers claim that the DHS is outdone by the Justice Department, which is the “lead Federal funding agency” for the license-tracking program.

License plate readers are also increasingly used to militarize the US-Mexico and US-Canada borders.

According to DHS reports, license plate readers are also used by the Customs and Border Protection agency to scan “nearly 100 percent of land border traffic.” In addition, Immigration and Customs Enforcement has admitted to routinely using license plate readers, as has

the Drug Enforcement Agency.

In collaboration with the national security apparatus, local police departments are being mobilized to build massive databases at the grassroots level.

In 2011, the license plate tracking program was used by 75 percent of police agencies, with an additional 10 percent stating they planned to increase use of license plate readers in the near future.

And the program is not limited to use in the US. Two license plate reader manufacturers, ELSAG and PIPS Technology, claim they have sold readers to thousands of agencies abroad as well as to police agencies in all 50 states.

In addition to use by local and federal security agencies, the ACLU reports that private companies have created “numerous privately owned databases containing the location information of vast numbers of Americans” by “scan[ning] thousands of plates each day and stor[ing] information indefinitely, creating huge databases of Americans’ movements.”

The ACLU writes that “MVTrac, one of the biggest companies in this industry, claims to have photographs and location data on ‘a large majority’ of registered vehicles in the United States, while the Digital Recognition Network (DRN) boasts of ‘a national network of more than 550 affiliates’ ” that are “located in every major metropolitan area of the United States.”

“DRN affiliates,” the ACLU report continues, “feed location data on up to 50 million vehicles each month...into DRN’s national database. This database now contains over 700 million datapoints on where American drivers have been.”

Data collected from law enforcement, at parking lots, and by other private access control monitoring systems have been aggregated into the National Vehicle Location Service (NVLS), run by Vigilant Solutions, a partner of DRN. According to Vigilant Solutions, the NVLS “is the largest [license plate] data sharing initiative in the United States.”

The amassing of such an immense database is a blatant violation of the Fourth Amendment of the US Constitution, which states:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...”

In its 2012 ruling in *United States v. Jones*, a five-justice majority of the Supreme Court agreed that a

police department’s warrantless, month-long monitoring of the defendant’s whereabouts through a GPS monitoring device constituted an unconstitutional search because “[f]or such offenses, society’s [reasonable] expectation [of privacy] has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car, for a very long period.”

But local law enforcement agencies use plate readers without limitation and in blatant violation of the US constitution. The ACLU report describes the practice of the Pittsburg Police Department in California as “typical.” Pittsburg police claim that “[r]easonable suspicion or probable cause is not required,” for use of license plate readers, which can be operated during “any routine patrol operation.”

In setting up these vast databases, the US government has mobilized the private sector and local law enforcement to set up a police-state mechanism whereby it is possible to track the whereabouts of a majority of people in close to real time and to monitor political dissidents by tracking attendance at meetings and rallies.



To contact the WSWS and the
Socialist Equality Party visit:

wsws.org/contact