Lawsuit Accuses Digital Recognition Network of Secretly Collecting Billions of License Plates

Lawsuit Accuses Digital Recognition Network of Secretly Collecting Billions of License Plates

by **Derrick Broze**, *The Last American Vagabond*
June 8, 2021

A recently filed lawsuit accuses Digital Recognition Network of covertly collecting vehicle data on millions of Americans and selling it for a profit.

On May 26, several vehicle owners sued the company Digital Recognition Network (DRN) for using its fleet of unmarked surveillance vehicles to collect data on Americans. The plaintiffs claim that DRN has driven its vehicles around United States and covertly gathered data on unsuspecting Americans while reaping profits.

Courthouse News reports that DRN has *"amassed more than 20 billion license plate scans – equal to 70 scans for every vehicle in the nation."* The Class Action Complaint and Demand for Jury Trial was filed by plaintiff Guillermo Mata in response to DRN's use of automatic license plate reader (ALPRs) systems. ALPRs are used to gather license plate, time, date and location of a vehicle. They can also be used to create a detailed map of where an individual travels and what they are doing with their time. The devices can be attached to light poles or toll booths, as well as on top of or inside vehicles.

The lawsuit alleges, ***"Defendant DRN created a nationwide surveillance program that tracks vehicle's movements and, in turn, individuals' locations."*** The plaintiffs also claim that DRN ***"stores all of the amassed information in a proprietary database and makes it available to anyone willing to pay for access to it."***

The claim states that DRN's *"privately-owned surveillance network"* is its fleet of *"unmarked vehicles that patrol America's roadways, equipped with high-speed cameras that allow them to capture photos of license plates, together with the time and location data of the photographed vehicles."*

After collecting the data DRN applies its proprietary algorithm to scan the data and make predictions about where the vehicle is traveling and where the vehicle may be located a future time. The plaintiffs argue that because DRN's cameras are attached to moving vehicles they are difficult to see and *"nearly unavoidable"*. Further, the individuals being scanned by the cameras are not subjects of any law enforcement investigations, nor are they part of state or federal watchlists. DRN has also failed to reasonably notify the public they are under constant surveillance by the network of vehicles outfitted with this technology.

DRN openly advertises their ability to collect "vehicle stories" that contain location and time data that can reveal private information that individuals may not wish to be public. The complaint states that, *"DRN can reveal whether an individual has recently visited an abortion clinic, a cancer treatment clinic, a religious center, or an LGBT community center, thus giving insight into one's health and medical history, religious beliefs, and sexual orientation."*

Digital Recognition Network uses the Reaper HD camera to gather this data from unsuspecting drivers. The Reaper is manufactured and sold by Motorola who describes it as a *"complete, fixed solution"* which allows users to *"receive* *real-time alerts, conduct comprehensive searches and leverage advanced analytics to uncover new insights and operate more efficiently."*

The plaintiffs filed the lawsuit in the hopes that the court will find that DRN's surveillance program is in violation of current California law. In 2016, California passed a law regulating and limiting the use of ALPRs. When passing the law California legislators acknowledged the breadth of privacy concerns associated with the technology. These concerns include:

- The collection of a license plate number, location, and time stamp over multiple time points can identify not only a person's exact whereabouts but also their pattern of movement.
- Unlike other types of personal information that are covered by existing law, civilians are not always aware when their ALPR data is being collected.
- One does not even need to be driving to be subject to ALPR technology: A car parked on the side of the road can be scanned by an ALPR system.

The Fight Against ALPRs

The concerns associated with Automatic License Plate Readers are not new. In 2014, I first reported on the dangers associated with ALPRs. At that time the Electronic Frontier Foundation (EFF) and the American Civil liberties Union (ACLU) of Southern California filed a lawsuit against the Los Angeles Police Department and the Los Angeles Sheriff Department claiming that the agencies were using ALPRs to gather information on drivers. The two watchdog agencies argued that the two departments were illegally keeping quiet on how the information is used.

In 2015, I reported on the Federal Bureau of Investigations (FBI) investing in this controversial technology despite the known privacy concerns. That same year it was also revealed that the National Highway Traffic Safety Administration (NHTSA) had granted hundreds of thousands of dollars to local and state law enforcement agencies for the purchase of ALPRs systems.

I have also reported on the potential for abuse of ALPRs, specifically the potential for law enforcement departments and officers to create lists of "vehicles of interest" and alert other ALPR users when the vehicle is spotted. Officers can search individual plates numbers in the ALPR system to track during their shift. There is no prerequisite of reasonable suspicion or a warrant needed to be added to such a list, creating a situation that is ripe for abuse. For example, in 2009 the BBC reported on the case of John Catt, a regular attendee of anti-war protests in his home town, Brighton. His vehicle was tagged by police at one of the events and he was added to a "hotlist". Catt said while on a trip to London he was pulled over by anti-terror police. He was threatened with arrest if he did not cooperate and answer the questions of the police.

More recently, the Biden administration has continued the push for militarizing the border with ALPRs. On February 25, more than 40 privacy, immigrants' rights, and civil liberties organizations called on the Biden administration to abandon a bill which would extend the Trump administration's border policy, particularly creation of a "virtual" or biometric wall. These organizations – including Mijente, Rio Grande Valley Equal Voice Network, Electronic Privacy Information Center (EPIC), Fight for the Future, and Restore the Fourth – wrote a letter to the Biden admin scolding the recently minted president for continuing the militarization of the border.

The letter, titled *A Virtual Wall Is Trump's Wall by Another Name*, warned that *"the rapid expansion of license plate recognition technology used by Customs and Border Protection and other federal agencies is a major privacy and policing* *concern."* The American Civil Liberties Union and other civil liberties organizations have been warning about the rise in use of automatic license plate readers (ALPRs), high definition cameras capable of seeing not only a vehicle's license plate, but the people in the vehicle.

While most Americans are likely unaware of this invasive technology, they are being monitored by ALPRs every single day. Not only do Americans face surveillance from ALPRs in the hands of law enforcement, but now they must contend with constant surveillance from a private company they have likely never heard of.

Connect with Derrick Broze at The Last American Vagabond