STREET LEVEL SURVEILLANCE

AUTOMATED LICENSE PLATE READERS

Automated license plate readers (ALPRs) are high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police squad cars. ALPRs automatically capture all license plate numbers that come into view, along with the location, date, and time. The data, which includes photographs of the vehicle and sometimes its driver and passengers, is then uploaded to a central server.

Vendors say that the information collected can be used by police to find out where a plate has been in the past to determine whether a vehicle was at the scene of a crime, to identify travel patterns, and even to discover vehicles that may be associated with each other. Law enforcement agencies can choose to share their information with thousands of other agencies.

Taken in the aggregate, ALPR data can paint an intimate portrait of a driver's life and even chill First Amendment protected activity. ALPR technology can be used to target drivers who visit sensitive places such as health centers, immigration clinics, gun shops, union halls, protests, or centers of religious worship.

Drivers have no control over whether their vehicle displays a license plate because the government requires all car, truck, and motorcycle drivers to display license plates in public view. So it's particularly disturbing that automatic license plate readers are used to track and record the movements of millions of ordinary people, even though the overwhelming majority are not connected to a crime.

How ALPR Systems Work

Stationary or Fixed ALPR cameras

PHOTO BY MIKE KATZ-LACABE (CC BY)

Stationary or fixed automated license plate readers

These are installed in a fixed location, such as a traffic light, a telephone pole, the entrance of a facility, or a freeway exit ramp. These cameras generally capture only vehicles in motion that pass within view.

If multiple stationary ALPR cameras are installed along a single thoroughfare, the data can reveal what direction and what speed a car is traveling. With enough cameras, police can track a vehicle in real-time. If the data is stored over time, they can reveal every time a particular plate has passed a given location, allowing the government to infer that the driver likely lives or works close by. Smaller municipalities often install ALPR cameras at the entrances and exits to the town, creating a virtual gated community no one can visit without being documented. Police will sometimes disguise ALPRs as mundane objects, such as traffic cones or cacti.

ALPR cameras are often used in conjunction with automated red-light and speed enforcement systems, and also as a means of assessing tolls on roads and bridges.

Mobile ALPR cameras

PHOTO BY MIKE KATZ-LACABE (CC BY)

Mobile automated license plate reader

Mobile ALPRs are often attached to police patrol cars, allowing law enforcement officers to capture data from license plates as they drive around the city throughout their shifts. In most cases, these cameras are turned on at the beginning of a shift and not turned off again until the end of the shift.

In addition to capturing images of passing vehicles, mobile ALPR cameras are effective at capturing license plates of parked cars. For example, a patrol car may drive around a public parking lot capturing hundreds of vehicles' plates in minutes.

Police can also use ALPRs for "gridding." This involves an ALPR-equipped vehicle systematically driving up and down every block of neighborhood to capture intelligence on residents.

Also, private vendors like Vigilant Solutions capture plate data with mobile ALPRs and then sell that data to police agencies and others.

ALPR Trailers

PHOTO BY MIKE KATZ-LACABE (CC BY)

A Walnut Creek Police Department ALPR trailer

ALPRs are also available as trailers that police can tow to particular areas and leave for extended periods of time. These collect data in a similar fashion as fixed ALPRs, without police having to permanently install the cameras. The Drug Enforcement Administration has purchased these systems in the past, disguised as speed enforcement trailers, in order to track vehicles in areas along the U.S.-Mexico border. Trailers, or vehicles equipped with ALPR, have also been parked by police near gun shows and political rallies.

ALPR Databases

Most of this ALPR data is stored in databases for extended periods of time—often as long as five years. The databases may be maintained by the police departments, but often they are maintained by private companies such as Vigilant Solutions or Flock Safety. Law enforcement agencies without their own ALPR systems can access data collected by other law enforcement agencies through regional sharing systems and networks operated by these private companies. Several companies operate independent, non-law enforcement ALPR databases, contracting with drivers to put cameras on private vehicles to

also purchase access to this commercial data on a subscription basis.

Hotlists

Law enforcement agencies will often pre-load a list of license plates that the ALPR system is actively looking for—such as stolen vehicles and vehicles associated with outstanding warrants. Police officers can also create their own hotlists. If the ALPR camera scans a plate on the list, the system sends an alert to the officer in the squad car (if it's a mobile reader) or the agency (if it's a fixed reader). Some hotlists include low-level misdemeanors and traffic offenses. Some agencies use these hotlists to generate revenue by stopping citation scofflaws.

What Kinds of Data an ALPR Collects

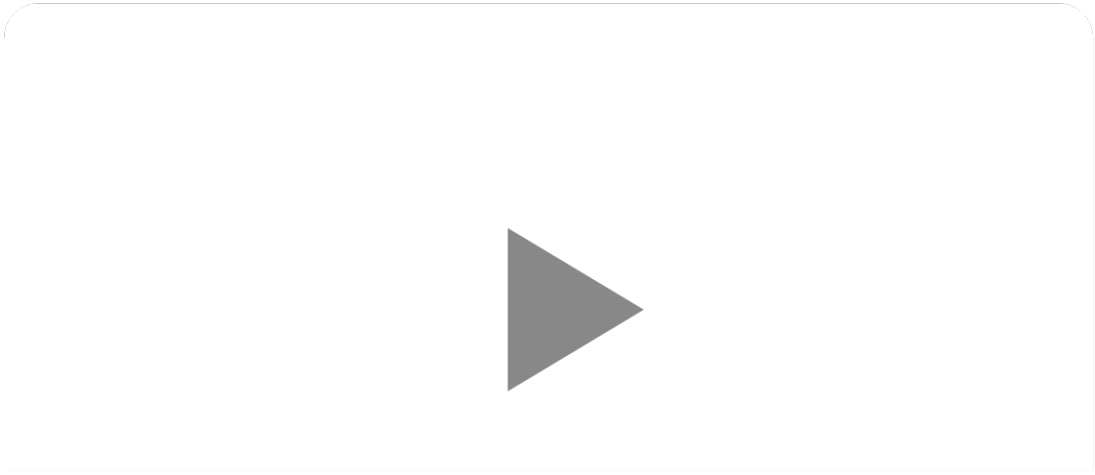
ALPRs collect license plate numbers and location data along with the exact date and time the license plate was encountered. Some systems are able to capture make and model of the vehicle. They can collect thousands of plates per minute. One vendor brags that its dataset includes more than 6.5 billion scans and grows at a rate of 120-million data points each month.

When combined, ALPR data can reveal the direction and speed a person traveled through triangulation. In aggregate over time, the data can reveal a vehicle's historical travel. With algorithms applied to the data, the systems can reveal regular travel patterns and predict where a driver may be in the future. The data also reveal all visitors to a particular location.

The data generally does not include the driver's name. However, law enforcement officers can use other databases to connect individual names with their license plate numbers.

In addition to capturing license plate data, the photographs can reveal images of the vehicle, the vehicle's drivers and passengers, as well as its immediate surroundings—and even people getting in and out of a vehicle. Some products create "vehicle fingerprints" that also include information such as the vehicle's color, make, model, physical damage, and bumper stickers.

How Law Enforcement Uses ALPR Technology



A time-lapse visualization of the data collected by Oakland Police Department vehicles mounted with license plate readers.

ALPR data is gathered indiscriminately, collecting information on millions of ordinary people. By plotting vehicle times and locations and tracing past movements, police can use stored data to paint a very specific portrait of drivers' lives, determining past patterns of behavior and possibly even predicting future ones—in spite of the fact that the vast majority of people whose license plate data is collected and stored have not even been accused of a crime. Without ALPR technology, law enforcement officers must collect license plates by hand. This creates practical limitations on the amount of data that can be collected and means officers must make choices about which vehicles they are going to track. ALPR technology removes those limitations and allows officers to track everyone, allowing for faster and broader collection of license plates with far reduced staffing requirements.

A report by EFF in 2021 found that according to data from 63 law enforcement agencies in California, only 0.05% of the data collected by ALPRs was relevant to a public safety interest at the time the data was captured.

Law enforcement has two general purposes for using license plate readers.

Real-time investigations

By adding a license plate to a "hot list," officers can use ALPR to automatically identify or track particular vehicles in real time. Licenses plates are often added to hot lists because the vehicle is stolen or associated with an outstanding warrant. Officers may also add a plate number to the list if the vehicle has been seen at the scene of a crime, the owner is a suspect in a crime, or the vehicle is believed to be associated with a gang. Hot lists often include low-level offenses, too.

Historical investigations

Since ALPRs typically collect information on everyone—not just hot-listed vehicles—officers can use a plate, a partial plate, or a physical address to search and analyze historical data. For example, an officer may enter the location of a convenience store to identify vehicles seen nearby at the time of a robbery. The officer can then look up those plate numbers to find other locations that plate has been captured.

Training materials, policies and laws in some jurisdictions instruct officers that a hot-list alert on its own may not be enough to warrant a stop. Officers are instructed to visually confirm that a plate number is a match. Failure to manually confirm, combined with machine error, has caused wrongful stops.

Law enforcement claims that ALPR data has been used to, for example, recover stolen cars or find abducted children. However, police have also used ALPR data for mass enforcement of less serious offenses, such as searching for uninsured or tracking down individuals with overdue court fees.

to as long as several years, although some entities—including private companies—may retain the data indefinitely.

Who Sells ALPR Technology

Vigilant Solutions (a subsidiary of Motorola Solutions) and Flock Safety are two of the most common ALPR vendors in the United States. Other vendors include Rekor, Elsag, Axon, Perceptics, and Jenoptik.

Vigilant Solutions, through its sister company Digital Recognition Network, offers access to data it has privately collected through partnerships with repossession companies, who passively collect ALPR through their own vehicles. Flock Safety similarly has arranged partnerships with a large number of homeowners associations that provide data to law enforcement. Both companies offer law enforcement the ability to share data with each other across the country.

Threats Posed by ALPR

ALPR is a powerful surveillance technology that can be used to invade the privacy of individuals as well as to violate the rights of entire communities.

Law enforcement agencies have abused this technology. Police officers in New York drove down a street and electronically recorded the license plate numbers of everyone parked near a mosque. Police in Birmingham targeted a Muslim community while misleading the public about the project. ALPR data EFF obtained from the Oakland Police Department showed that police disproportionately deploy ALPR-mounted vehicles in low-income communities and communities of color.

Moreover, many individual officers have abused law enforcement databases, including license plate information and records held by motor vehicle departments. In 1998, a Washington, D.C. police officer "pleaded guilty to extortion after looking up the plates of vehicles near a gay bar and blackmailing the vehicle owners." More recently, an officer in Kechi, Kansas was arrested on suspicion of accessing a Flock Safety ALPR database to stalk his estranged wife.

In addition to deliberate misuse, ALPRs sometimes misread plates, leading to dire consequences. In 2009, San Francisco police pulled over Denise Green, an African-American city worker, handcuffed her at gunpoint, forced her to her knees, and searched both her and her vehicle—all because her car was misidentified as stolen due to a license plate reader error. Her experience led the U.S. Ninth Circuit Court of Appeals to rule that technology alone can't be the basis of such a stop, but that judgment does not apply everywhere, leaving people vulnerable to similar law enforcement errors. More recently, in Aurora, Colorado a group of Black youths were traumatized by police after an ALPR system incorrectly identified their vehicle as stolen.

Aggregate data stored for lengthy periods of time (or indefinitely) becomes more invasive and revealing, and it is susceptible to both misuse and data breach. Even Customs & Border Protection, arguably the largest and best funded law enforcement agency in the U.S., saw its ALPR vendor, Perceptics, hacked and data published online. Sensible retention limits, specific policies about who inside an agency is allowed to access data, and audit and control processes could help minimize these issues. One of the

does not match a hot list.

Automated license plate readers can also be used to target immigrant communities and people seeking or providing reproductive health services.

EFF's Work on ALPR

EFF has been investigating and combating the privacy threats of ALPR technology through public records requests, litigation, and legislative advocacy since 2012.

ALPR Litigation

EFF and the ACLU of Southern California sued the Los Angeles County Sheriff's Department and the Los Angeles Police Department after the agencies refused to hand over ALPR data. The agencies claimed the records were exempt from the California Public Records Act because they were investigative records. This argument amounts to claiming that all Los Angelenos are under investigation, a point that both a lawyer for the LAPD and a California Supreme Court Justice agreed sounded "Orwellian" during oral arguments. In 2017, the California Supreme Court ruled in EFF and ACLU's favor and ordered the case back to the Superior court.

EFF and the ACLU also sued the Marin County Sheriff's Office in 2021 on behalf of local activists in *Lagleva v. Marin County Sheriff*. The sheriff had been sharing data collected through ALPRs with out-of-state agencies, including Immigration & Customs Enforcement, in violation of laws regulating ALPR use and prohibiting the sharing of criminal justice data for immigration enforcement. As part of a settlement, the sheriff agreed to cease sharing data outside of California.

Outside of California, EFF has filed briefs in a lawsuit over the excessive storage collection of ALPR data in the state of Virginia, as well as briefs in cases in Massachusetts and Nevada.

ALPR Accountability and Transparency

In 2015, the California legislature passed S.B. 34, a bill that requires ALPR users to protect data, maintain access logs, hold public meetings before starting an ALPR program, implement a usage and privacy policy, and maintain access logs. The law also prohibits public agencies from selling, sharing, or transferring ALPR data except to other public agencies.

EFF has coordinated volunteers to collect ALPR policies across the state of California and to expose agencies failing to comply with the law. EFF has also independently filed public records requests with dozens of agencies to shine light on their use of ALPR data through our Data Driven and Data Driven 2 projects.

In 2019, EFF successfully advocated for the California Legislature to order an audit of several law enforcement agencies' compliance with S.B. 34. As a result, the California State Auditor issued a scathing report substantiating many of EFF's concerns that agencies weren't following the law, failing to enact adequate policies, and sharing data far too broadly.

EFF Legal Cases

ACLU of Southern California and EFF v. LAPD and LASD

Neal v. Fairfax County Police Department

Lagleva v. Marin County Sheriff

United States v. Yang

Commonwealth v. McCarthy

People v. Gonzales

Suggested Additional Reading

You Are Being Tracked (ACLU)

License Plate Readers for Law Enforcement Opportunities and Obstacles (RAND Corporation)

Automated License Plate Readers Threaten Our Privacy (EFF/ACLU)

The Four Flavors of Automated License Plate Reader Technology (EFF)

Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use (Brennan Center)

Things to Know Before Your Neighborhood Installs an Automated License Plate Reader (EFF)

Automated License Plate Readers Threaten Abortion Access. Here's How Policymakers Can Mitigate the Risk (EFF)

Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns Using Automated License Plate Readers (EFF)

Data Driven 2: California Dragnet—New Data Set Shows Scale of Vehicle Surveillance in the Golden State (EFF)

How to Pump the Brakes on Your Police Department's Use of Flock's Mass Surveillance License Plate Readers (ACLU)

Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects (California State Auditor)

Most recently updated October 1, 2023

TECHNOLOGIES