JANUARY 2021

LEADING A SUCCESSFUL CAMPAIGN AGAINST AUTOMATED LICENSE PLATE READERS

Automated license plate readers (ALPR) are a form of surveillance technology that threaten the privacy and safety of our communities. ICE can use information collected by license plate readers to track, target, and deport immigrants. This resource provides an overview of this surveillance technology, how you can investigate its use in your communities, and how to campaign against it.

WHAT ARE AUTOMATED LICENSE PLATE READERS?

Automated License Plate Reader (ALPR) technology refers to high-speed cameras that take pictures of passing cars. ALPR cameras capture multiple images of license plates passing by the camera, along with the time, date, and location of the plate. These cameras can be in fixed or mobile locations, like public street poles or police cars. The images and location data are uploaded to a database or cloud system. This data often includes images of the vehicles and location information, but entities can and have also stored other information such as names, addresses, dates of birth and even criminal information to their ALPR databases. People with access to the database can run searches to learn when and where a vehicle has been seen by an ALPR camera.

Vigilant Solutions, LLC is the primary company selling its ALPR technology and software **(known as LEARN)** to a variety of governmental and private entities that include law enforcement agencies, toll and parking lots as well as other sources. Vigilant's technology allows these entities to "share" access to vehicle information collected locally with other agencies nationwide. Vigilant claims to have over 5 billion ALPR data stored in its database, with over 150 million entries added monthly.

HOW IS ALPR INFORMATION USED FOR IMMIGRATION ENFORCEMENT?

In January 2018, ICE contracted with a company called Thomson Reuters to gain access to ALPR information from Vigilant's LEARN database. Thomson Reuters provides the platform **(known as CLEAR)** to access Vigilant's ALPR data as well as training and technical support for the platform's use. ICE's contract, which was set to expire in September 2020, allows its ICE officers to search ALPR information collected by local agencies that have agreed to share their information with ICE. As of the time of this writing, we are unsure whether ICE extended this contract. Vigilant's database pulls from various sources, including state and local law enforcement agencies across the country and from commercial sources located in forty-seven states (minus Hawaii, Maine, and Vermont), the District of Columbia, and Puerto Rico.

In addition to the agencies that share ALPR information formally, ICE also contacts local law enforcement officers informally to ask them to share ALPR information results directly to ICE, circumventing ICE's internal rules on how it is supposed to use and track searches.

When local law enforcement agencies and other entities make ALPR information accessible to ICE, ICE uses the information to find and arrest immigrants for deportation purposes. ICE can search for information on a targeted person or even their family members or friends in order to locate and arrest the person.

WHY IS ALPR A PROBLEM?

ALPR technology is disproportionally used on communities where persons of color, immigrants, and low-income persons reside. These populations have a higher chance of having their information stored in an ALPR database and ultimately tracked. For example, the New York Police Department has used ALPR technology to surveil Muslim communities by recording license plates of everyone parked near mosques. Similarly, the Oakland Police Department has disproportionally deployed ALPR-mounted cars in communities of color.

Moreover, ALPR technology raises civil rights and civil liberties concerns. Location information can track our daily movements and reveal information that we otherwise want to keep private. A Virginia state court found that ALPR technology violated a state privacy law because the technology can identify a vehicle's owner when the license plate location information was coupled with data from databases containing other information like criminal and DMV records. ALPR technology also raises concerns under the Fourth Amendment of the U.S. Constitution because long-term location tracking can violate individual privacy. This is because ALPR technology has the ability to map out our car's movements over time by collecting numerous data at different locations throughout time.

HOW CAN YOU CAMPAIGN AGAINST THE USE OF ALPR TECHNOLOGY?

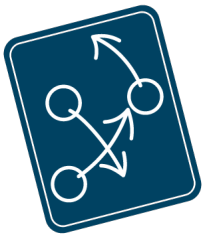
SEEK TRANSPARENCY: LEARN HOW ALPR IS USED IN YOUR JURISDICTION

Before starting a campaign, you should understand if and how your locality uses ALPR technology. Seeking transparency can happen by asking questions of elected officials, public employees, police departments, or sheriff departments through public or one-on-one meetings or by other formal means. All states and the federal government have open records act laws that allow you to request information from federal, state, and local government entities. You can submit an open records request to your local government to obtain useful information about ALPR, including the number of cameras, policies, costs, data being stored, and information on whether the information is shared with other agencies, like ICE.

CREATE PARTNERSHIPS

When campaigning against the use of ALPR, consider building partnerships with other organizations or individuals interested in issues of immigration, police practices, privacy, and criminal justice reform. Because ALPR affects all of our privacy, immigrant rights organizers often partner with other activists to learn from one another and co-lead campaigns.

CONSIDER STRATEGY: ABOLISHING ALPR TECHNOLOGY AND RESTRICTING ITS USE



Before launching a campaign, you should assess your goals and the different tactics that you can take. Many advocates have engaged in efforts to prevent local agencies from using the technology altogether. This is especially helpful in areas where a locality has not yet installed ALPR or a contract for ALPR technology is up for renewal.

Advocates have also considered passing state or local ordinances and pushing for the adoption of policies that restrict and regulate the use of ALPR and other surveillance technology. Policies can include requirements that driver information be destroyed after a certain date, limit sharing of data with external agencies or individuals, prohibit the use of data for immigration purposes, and mandate public reporting of data and policies surrounding the use of ALPR.

CHOOSING YOUR TARGETS

In creating a campaign, you should first assess the various entities involved and which ones you might want to target to achieve your goals. A primary audience are the individuals in your community who decide whether to purchase ALPR technology and the policies governing its use. These can include the county boards of supervisors, city councils, and members of the sheriff's office or police department. Also consider federal and state law enforcement agencies, including ICE, sheriffs, police, and fusion centers, as being a target of your requests for information as part of open records requests. Other targets for your advocacy include the companies selling or providing access to ALPR technology, like Vigilant and Thomson Reuters; you can describe what you've learned about these companies publicly.

EXPOSE THE USE OF ALPR THROUGH MEDIA

As you plan your campaign, consider reaching out to local and major media outlets. Journalists have written about the findings from open records requests. You can also use the press to publicize protests and campaign events.