AUTOMATED LICENSE PLATE READERS??

NO

NO

NO

I **oppose** the acquisition or use of license plate readers (ALPR).

Yadi
Pasadena resident
Pasadena City Council Meeting
Meeting: August 1, 2022
4. UASI Funds - ALPR

08/1/2022
Item 4

COMMITMENT • INTEGRITY • LEADERSHIP

View full PDF report

View Selected Abbreviations

Automated License Plate Readers

To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects

Report Number: 2019-118

Automated License Plate Readers

To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects

February 2020

Audit Highlights . . .

Our audit of the use of automated license plate readers (ALPR) at four local law enforcement agencies highlighted the following:

Local law enforcement agencies did not always follow practices that adequately consider the individual's privacy in handling and retaining the ALPR images and associated data.

All four agencies have accumulated a large number of images in their ALPR systems, yet most of the images do not relate to their criminal investigations—99.9 percent of the 320 million images Los Angeles stores are for vehicles that were not on a hot list when the image was made.

- None of the agencies have an ALPR usage and privacy policy that implements all the legally mandated—since 2016—requirements.
- Three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data, and the remaining agency has not developed a policy at all.
- Two of the agencies add and store names, addresses, dates of birth, and criminal charges to their systems—some of these data may be categorized as criminal justice information and may originate from a system maintained and protected by the Department of Justice.
- Three agencies use a cloud storage vendor to hold their many images and associated data, yet the agencies lack contract guarantees that the cloud vendor will appropriately protect the data.
- Three agencies share their images with hundreds of entities across the U.S. but could not provide evidence that they had determined whether those entities have a right or a need to access the images.

Agencies may be retaining the images longer than necessary and thus increasing the risk to individuals' privacy.

The agencies have few safeguards for creating ALPR user accounts and have not audited the use of their systems.

Report: https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf

Note: Three responding agencies that use ALPR systems did not indicate a retention period for their information: Bakersfield PD, Fountain Valley PD and Pasadena PD

AMERICANBARASSOCIATION

August 23, 2021
By David Horrigan

Data Privacy vs. Crime Prevention: The Automated License Plate Recognition Debate

If your child were the victim of a kidnapping, an automated license plate recognition (ALPR) reader might be a lifesaver—figuratively and literally.

On the other hand, if you were a victim of domestic abuse, ALPR technology in the wrong hands could put you in danger, and the tragic history of World War II taught us what can happen when totalitarian governments have an unlimited ability to collect data on their citizens.

But just what is automated license plate recognition technology, and do you really have a reasonable expectation of privacy in a number emblazoned on the front of your Ford or the back of your Buick?

Police departments, privacy advocates, and the courts have entered the ALPR debate. Is the technology a godsend for safety or an Orwellian data privacy nightmare? Perhaps it's both.

Robot Readers

What are automated license plate recognition readers?

According to the International Association of Chiefs of Police (IACP), ALPR technology consists typically of high-speed, high-resolution cameras with infrared filters that capture images of vehicle license plates. The images are transferred to processing applications performing optical character recognition (OCR) and then compared against law enforcement databases of license plates of interest, sometimes called "hot lists."

ALPR readers can be deployed in stationary positions, including highway overpasses or streetlight poles, or in mobile units, such as police cars.

Not surprisingly, ALPR developers join many law enforcement advocates in hailing the technology as an important means of protecting the public.

The ALPR company, Leonardo, cities stories of how license plate readers can come to the rescue—including in the return of a one-year-old kidnapping victim to his mother—and the company maintains ALPR technology can make places from college campuses to hotels safer.

Many privacy advocates have a different view.

Orwellian Tech Nightmare?

The digital civil liberties group, the Electronic Frontier Foundation (EFF), paints a picture of a technological Orwellian nightmare brought to us by automated license plate recognition readers.

"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," EFF

argues in its statement on the issue.

To those who would counter that there's no reasonable expectation of privacy in a license plate number—something that is displayed openly in public for the world to see—EFF notes the compulsory nature of license plates. In essence, the EFF Big Brother argument is that the government forces you to have a license plate, and then the government tracks your every move with that license plate.

What about that one-year-old kidnapping victim?

EFF notes that law enforcement uses ALPR technology to track millions of ordinary people—and the overwhelming majority of them are not even suspected of committing any crime.

The American Civil Liberties Union (ACLU) shares EFF's concerns.

"Enormous databases of innocent motorists' location information are growing rapidly. This information is often retained for years, or even indefinitely, with few or no restrictions to protect privacy rights," the ACLU argues in its position statement on ALPR.

Rules and Regulations for Readers

Citing a 2012 project in which ACLU affiliates across the nation sent public records act requests to approximately 600 local and state police departments as well as state and federal agencies, the organization says the practice is more widespread than you might think.

In addition, the ACLU says the results of its project are deeply disturbing.

"The documents paint a startling picture of a technology deployed with too few rules that is becoming a tool for mass routine location tracking and surveillance," the ACLU argues.

ALPR is also becoming big business. A recent estimate by Market Study Report indicates the global market for ALPR was $794.1 million in 2019 and that it will increase to over $1.2 billion in 2025.

Not surprisingly, the data privacy debate over automated license plate recognition has reached the courts, and last fall, the Virginia Supreme Court weighed in on this legal technology dilemma.

In Neal v. Fairfax Cty. Police Dep't, 849 S.E. 2d 123 (2020), Virginia's high court reversed a lower court and held a local police department's use of ALPR technology did not violate Virginia's Government Data Collection and Dissemination Act (the "Data Act").

In Neal, Harrison Neal filed a Freedom of Information Act request with Virginia's Fairfax County Police Department, seeking the department's ALPR data for his vehicle. The police returned two sheets of paper, each with a photo of his vehicle and his license plate, each with the time and date the photo was taken.

Neal filed suit, seeking injunctive relief to prevent the police department from collecting and storing ALPR data without any suspicion of criminal activity—the so-called "passive use" of ALPR, where the readers are collecting data from each passing vehicle.

In the proceeding that became known as "Neal I," the trial court granted summary judgment to the police, holding the department's use of ALPR technology did not violate Virginia's Data Act because the data collected did not constitute "personal information" under the act.

However, the Virginia Supreme Court reversed. Although the high court conceded that "a license plate number stored in the ALPR database would not be personal information because it does not describe, locate, or index anything about an individual," the court said that didn't end the data privacy inquiry because the pictures and data associated with each license plate number did constitute "personal information" under the Data Act.

On remand, the lower court held the ALPR record-keeping process—the technology combined with other law enforcement databases—did constitute an information system under the Data Act, and the police department appealed.

In considering the case on its return visit to the Virginia Supreme Court, the high court noted—almost refreshingly—the limits of its inquiry and that our courts are not here to make public policy.

"In resolving this case, our task is not to reach the right public policy balance by weighing competing demands for efficiency and security against considerations of privacy. Our duty is more modest: we must determine from the text and structure of the Data Act where the legislature has drawn the line," Justice Stephen McCullough wrote for the court.

In reversing the lower court again, the Virginia Supreme Court noted the additional fact-finding by the lower court on remand and held the ALPR system did not violate the Data Act because the ALPR system itself—without the use of other law enforcement databases—was not an "information system" under the act because it did not contain the "name, personal number, or other identifying particulars of a data subject."

Why the ALPR Debate Matters

Justice McCullough did an excellent job of articulating why this debate matters when he wrote in Neal: "Modern technology enables governments to acquire information on the population on an unprecedented scale. National, state, and local governments can use that information for a variety of administrative purposes and to help apprehend dangerous criminals. But knowledge is power, and power can be abused."

Even the police chiefs' organization cautions that access to ALPR databases should be limited to authorized law enforcement personnel who have met minimum training, certification, and background checks, and that there should be stringent data audits.

Attorney Gail Gottehrer, who has served as a member of Connecticut's Task Force to Study Fully Autonomous Vehicles and on the New York State Bar Association's Transportation Committee, sees the important role humans play in the data privacy aspects of automated technologies.

"ALPR technologies, like many emerging technologies, are tools. Whether they help achieve public safety goals or threaten privacy rights depends on who uses them and the ways in which they are used. On their own, ALPR technologies may not reveal much about a specific individual, but when government or private entities combine ALPR data with other data in their possession, the result may be a disturbingly comprehensive profile of that person," Gottehrer said.

However, Gottehrer notes there are ways to reduce the danger of such disturbingly comprehensive profiles.

"Ways to maximize the benefits of ALPR technologies and minimize the privacy risks associated with them include limiting the types of entities that can collect and use ALPR data and the purposes for which they can use the data—as well as delineating when (or if) the data can be shared, and the period of time for which the data can be kept, after which it (and all copies and backups) must be destroyed," Gottehrer added

As Gottehrer notes, with any technology, its success or failure depends on how it's used. There's a reason we say "People, process, and technology," and not "Technology and those other two extraneous, superfluous elements."

https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/automobile-litigation/data-privacy-vs-crime-prevention/