ALPRS & LAW ENFORCEMENT

AYYAN ZUBAIR

JULY 5, 2019
Automated License Plate Readers & Law Enforcement

Background

Automated License Plate Readers (ALPRs) are high speed cameras mounted to street lights and patrol cars that track the license plates of every car that passes its line of vision.¹ Often, these cameras also capture photographs of the vehicle and its passengers.² ALPRs notify operators when they capture a plate on an agency’s watch list, prompting an almost-immediate—and error prone—law enforcement response.³ Police departments and private companies store and share this data—timestamped driving records of millions of people—for months and even years.⁴

ALPR’s Disproportionate Impact

When ALPRs get it wrong, communities of color, immigrants, and other minority groups pay the price. In Oakland, drivers in a predominately African-American or Latinx area are more likely to be tracked by an ALPR than those in a high-density white neighborhood.⁵ In New York City, the NYPD routinely outfitted unmarked police cars with ALPRs to record the plates of everyone parked near a mosque.⁶ And newly-released documents reveal that ICE creates watch lists using ALRP data to track undocumented immigrants.⁷

Disturbingly, ALPRs have at least a 10% error rate.⁸ These errors enable law enforcement profiling and, in some cases, even result in individuals being stopped at

---

¹ A recent Electronic Frontier Foundation study found that government agencies used ALPRs to scan over 2.5 billion license plates between 2016 and 2017. 99.5% of these plates were not under criminal suspicion at the time they were scanned. See DAVE MASS & BERYL LIPTON, EFF and MuckRock Release Records and Data from 200 Law Enforcement Agencies’ Automated License Plate Reader Programs, EFF, Nov. 15, 2018, https://www.eff.org/deeplinks/2018/11/eff-and-muckrock-release-records-and-data-200-law-enforcement-agencies-automated.
² AMERICAN CIVIL LIBERTIES UNION, You are Being Tracked: How License Plate Readers are Being Used to Track Americans’ Movements, 2013, https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf at 4-6.
³ See id.
⁴ See id.
gunpoint by police. Rather than acknowledging the risks of this technology, most agencies—including the NYPD—systematically block any attempt at oversight.  

**ALPR’s Security Issues**

This technology has been a prime target for hacking in the past. ALPRs store data on millions of cars, and a breach could potentially compromise millions of drivers’ histories—where they prayed, where they shopped, and where they slept. In June 2019, CBP revealed that a cyberattack on a government contractor compromised almost 100,000 license plate photos taken at the U.S. border. Disturbingly, CBP’s contractor, Perceptics, purportedly photographs over 200 million vehicles annually. In 2015, Boston’s entire ALPR system laid exposed on the Internet, and many ALPR cameras continue to remain vulnerable to hackers.

**ALPRs & NYPD**

In 2015, the NYPD signed a multi-year contract with Vigilant Solutions to access the company’s nationwide database of over 2 billion license plates. Vigilant’s technology added one million data points per day to the NYPD’s vast Domain Awareness System. Vigilant’s “stakeout” feature allows the NYPD to virtually surveil everything from political rallies, to abortion clinics, to Sunday church services. Its artificial intelligence tool purportedly enables the NYPD to “learn” a person’s daily routine with eerily precise accuracy. Disturbingly, the NYPD relies on Vigilante’s “associate analysis” to determine “possible associates” of criminal activity based on the company’s Orwellian surveillance algorithms. Considering the NYPD’s past history of discrimination against New Yorkers of color and immigrants, it is virtually certain that these communities will continue to bear the brunt of this dystopian technology.

---

10. See KTVU, supra note 5.
12. Id.
15. See id.
16. The Domain Awareness System collects the license plate data scanned by the approximately 500 license plate readers operated by the NYPD and combines it with footage from cameras and other surveillance devices around the city. The NYPD holds on to the license plate data for at least five years regardless of whether a car triggers any suspicion. See MARIKO HIROSE, *Documents Uncover NYPD’s Vast License Plate Reader Database*, ACLU, Jan. 25, 2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database?redirect=blog/speak-freely/documents-uncover-nypds-vast-license-plate-reader-database.
17. See id.
18. See id.
19. See id.
Legislative Action

Lawmakers across the country are creating safeguards to prevent ALPR misuse. In 2015, California passed S.B. 34, requiring agencies that utilize ALPRs to protect data, maintain access logs, and implement a usage and privacy policy. This law also prohibits public agencies from selling, sharing, or transferring ALPR data to private entities. The same year, Minnesota placed strict limits on license plate readers, including limits on who can be tracked using ALPRs and how the data may be shared. Minnesota also bars law enforcement from capturing images of a vehicle’s occupants, which has become increasing common in New York and other jurisdictions.

In New York City, Council Member Vanessa L. Gibson introduced “The Public Oversight of Surveillance Technology” (POST) Act in 2018, requiring the NYPD to create a privacy and use policy for surveillance tools. The Act would not prohibit ALPRs, but it would require the NYPD to establish basic safeguards for ALPRs and other surveillance systems.

In June 2019, New York State Senator Andrew Gounardes introduced S6428, creating a statewide task force on the role of artificial intelligence in New York State Government. If enacted, S6428’s 15-member task force would review how state agencies use artificial intelligence tools, such as ALPRs, to make decisions about policing, education, state hiring, and other areas of government operations.

Conclusion

Left unregulated, ALPRs hold the power to drastically curtail our right to privacy. This Orwellian technology lets the government know what you did last summer—where you went, who you were with, even what you were wearing. As government agencies repeatedly fail to keep such sensitive information safe, these troves of data will be constantly at-risk of third-party intrusion. As such, federal, state, and local legislatures must consider policies to prevent privacy rights from becoming nothing more than a legal fiction.

21 See id.
23 See id.