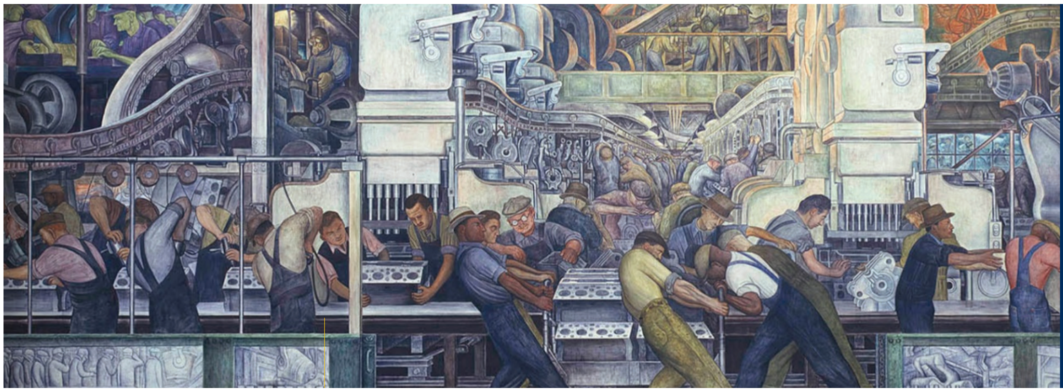


FORD SCHOOL OF PUBLIC POLICY
SCIENCE, TECHNOLOGY AND PUBLIC POLICY
UNIVERSITY OF MICHIGAN

Automated License Plate Readers: Legal and Policy Evaluation

JANUARY 2023

Noah Stein, Public Policy BA ‘23

EXECUTIVE SUMMARY

Automated License Plate Readers (ALPRs) are a surveillance technology that can alert law enforcement about vehicle locations in real time or provide information on past movements. In recent years, growing numbers of public and private entities have begun using ALPRs, moving some communities to implement policies aimed at limiting the potential damage posed by the technology. This memo analyzes legal and policy concerns related to the technology. It concludes by suggesting policy options that communities can advocate for including a ban or moratorium, and appropriate safeguards if the technology is used.

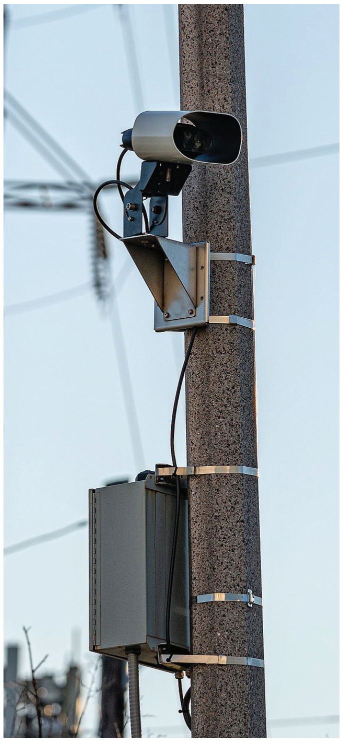
THE TECHNOLOGY

How it Works

ALPRs use a combination of high-speed cameras and computer software to log every license plate that passes by the camera. Every time a vehicle passes, the ALPR takes a photograph, records the time and location, then uploads these to a central database. ALPR software compares each plate with a “hot list” of vehicles, including those believed to be at a recent crime scene or stolen and even those involved with low-level offenses. The ALPR system may then automatically alert law enforcement if there are any matches. In addition to the real-time comparison, customers can store ALPR databases for indefinite periods and search them to plot a vehicle’s past movement and predict future locations.[1]

ALPR companies collect license plate data by placing cameras in a variety of locations. One method is to use stationary cameras on traffic lights, telephone poles, or entrances and exits to different neighborhoods or municipalities. In some instances, police departments have attempted to conceal the cameras by installing them in unusual places such as cactuses.[2] The cameras can also be semi-stationary and put on parked vans or tractor-trailers. Alternatively, ALPR users such as law enforcement, auto recovery companies, and bail bond agencies can place the cameras directly on cars, making them fully mobile. In the past, police have used license plate readers to target locations where people have a constitutional right to assemble, such as mosques and political rallies, or where they are engaging in legal activities, such as gun shows.[3]

Users can access ALPR data through subscription agreements with private companies and sharing between government agencies.[4] Many police departments use scans from other organizations to expand their databases and often share the information with federal agencies. For example, in 2020, the California State Auditor found that the Sacramento Police Department shared data with over one thousand agencies all over the United States.[5] An ACLU investigation from 2019 found that over 80 local police departments shared ALPR data with Immigration and Customs Enforcement (ICE), violating local sanctuary and privacy policies in some cases.[6] Customs and Border Protection has also received license plate information from law enforcement agencies all over the country.[7]



Major Vendors

The two leading purveyors of ALPRs are Motorola Solutions and Flock Safety. Motorola Solutions is a large, multinational company that does over $8 billion in revenue every year, with the US government as its leading client.[8] Among many other surveillance products, it offers a wide array of license plate scanning products and software.[9] Besides law enforcement, Motorola also markets and sells the technology to businesses, including auto recovery companies, banks, and insurance agencies.[10] Flock Safety, a growing start-up, attained over $300 million in venture capital in recent years, leading to a valuation of $3.5 billion.[11] Like Motorola, Flock sells its technology to both the public and private sectors.[12]

Current Usage

ALPRs are already in widespread use throughout the United States. A 2013 report sponsored by the Department of Justice showed that 77% of police departments serving populations of over 100 thousand used ALPR technology, with other studies showing that their use has rapidly increased over the intervening years.[13] Motorola and Flock have collectively claimed to serve over 3000 communities across the US. Motorola states that they have an active database containing over 44 billion license plate records with over 600k daily hot list alerts.[14] These sizable numbers show the extensive use and growing adoption of the technology.

Private sector entities like homeowner associations, banks, and insurance agencies also purchase ALPR technology.[15] For example, Hamptons Homeowners Association in Sacramento County, California purchased nine cameras from Flock Safety that effectively covered every entrance and exit in their neighborhood. They then have the option to share any information related to suspected criminal activity with the local police department.[16]

LEGAL STATUS

Current Legislation

At the Federal level, regulation of ALPRs is nonexistent, while at the state level, it is the exception rather than the rule, as only sixteen states have enacted some form of regulation.[17] Until 2016, New Hampshire had an outright ban on ALPRs. They have since lifted the ban while explicitly restricting ALPRs to well-defined uses, including a provision that all records of plates must be destroyed within three minutes unless they result in a match with a hot list.[18] In contrast, Colorado allows agencies to keep images obtained from passive surveillance for up to three years.[19] Other states regulate who can use ALPRs, where they can use them, and when they can access the data.[20] As most jurisdictions have zero laws regarding ALPRs, law enforcement and private actors can use the technology however they wish.

77% of police departments serving populations of over 100 thousand used ALPR technology

Case Law

The Supreme Court has not yet ruled on whether accessing historical ALPR information requires a warrant, and lower court decisions rely on state laws. A recent case regarding cell phone location data, *Carpenter v. US* (2018), may indicate how the Justices would rule on historical ALPR data. In a 5-4 decision, the Court ruled that the government violated the Fourth Amendment by accessing historical cell site information (CSLI) without a search warrant.[21] In two recent cases in which plaintiffs sought to restrict law enforcement's access to information gathered by ALPR technology, appeals courts and State Supreme Courts did not extend the Carpenter decision to ALPR data.[22]

Beyond Fourth Amendment concerns, cases related to state privacy laws have arisen as well. The Virginia Supreme Court ruled in *Neal v. Fairfax County Police Department* (2020) that the use of ALPRs by law enforcement did not violate the Virginia Data Act, as it said the ALPR system did not constitute an "information system."[23] In *Kansas v. Glover* (2020), the Supreme Court did decide on whether a license plate search can give law enforcement justification for a traffic stop. The Justices ruled in an 8-1 decision that if a license plate search shows that a driver has had their license revoked, then this gives the police reasonable justification to stop a car.[24]

Even when ALPRs work as intended, the vast majority of images taken are not connected to any criminal activity. According to an ACLU report about Maryland law enforcement, for every one million plates scanned, only 47 had a potential association with a serious crime.

ANALYSIS

Accuracy

Recent studies examining the accuracy of ALPRs show that they often misread license plates, leading to disastrous real-world consequences. IPVM, a video surveillance research group, found in an independent investigation that the readers incorrectly identified states on license plates about ten percent of the time.[25] The nonprofit BetaGov found significantly worse results in a randomized control trial: 37 percent of sampled "hits" from stationary ALPRs and 35 percent from mobile units were misreads.[26]

Inaccurate ALPR readings have led police to detain innocent people. In 2009, police handcuffed a Black woman named Denise Green and held her at gunpoint after an ALPR incorrectly identified her vehicle as stolen.[27] In a similar incident, police accused Brittany Gilliam of driving a stolen car based on flawed ALPR data. Gilliam and her passengers, four Black girls aged 17, 14, 12, and 6, were forced to lie on the ground as they were handcuffed. Similar to Denise Green, the ALPR had incorrectly read Gilliam's license plate, and her car was, in fact, not stolen.[28]

ALPR errors arise not only from shortcomings internal to their technology but from the hot lists they depend on to provide matches. An out-of-date database was to blame when Brian Hofer, the chair of Oakland's Privacy Advisory Commission, was detained at gunpoint because an ALPR alerted officers that he was driving a stolen vehicle. Someone had stolen the car in the past, but it was recovered, and law enforcement had not accurately updated the hotlist.[29]

However, even in a best-case scenario, with a functioning ALPR and a maintained hot list, mistakes can still arise. Police apprehended and handcuffed Zach Norris, the former Director of the Ella Baker Center for Human Rights, who had just returned from a hike with his wife. Someone had switched his license plate with one involved in an armed robbery.[30] Illustrating how even perfectly functioning surveillance technology can lead to problematic encounters with the police.

Privacy

Even when ALPRs work as intended, the vast majority of images taken are not connected to any criminal activity. According to an ACLU report about Maryland law enforcement, for every one million plates scanned, only 47 had a potential association with a serious crime.[31] Many other analyses have shown similar results, with the Minnesota State Patrol reporting that of the roughly 1.7 million scans between 2009 and 2011, only 0.05% of those led to an arrest or citation.[32] These staggering numbers show how ALPRs scan and track millions of people who have not broken any laws.

As most jurisdictions have no policies regarding retention limits, many agencies keep these scans on innocent people indefinitely. This can allow the government to maintain an overarching and potentially unconstitutional level of surveillance and can lead to misuse by individuals.

Misuse and Disparate Impact

Many departments that utilize ALPRs do not have any policies in place that could prevent potential misuse of the technology. Without these policies, there have been many instances of individual officers abusing ALPRs. A 2016 Associated Press report discovered hundreds of cases of officers all over the country who had misused confidential databases "to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work."[33] For example, they identified a case of a Colorado marshal who asked employees to run license plate checks on every white pickup truck as he believed his girlfriend was having an affair with a man who owned a white truck.[34] More recently, in November 2022, Wichita Police revoked access to Flock license plate readers for the entire department after a lieutenant was arrested for using the technology to stalk his ex-wife.[35]

Police have also targeted religious minorities and communities of color on numerous occasions. An Associated Press report found the NYPD to have deliberately scanned every vehicle parked near mosques in New York and New Jersey, clearly targeting Muslim communities.[36] Additionally, an investigation by the Electronic Frontier Foundation discovered that Oakland police were disproportionately using the technology in Black and Latino neighborhoods.[37]

Reproductive rights advocates are now raising alarms about the ways police and others could use ALPRs for the targeting of abortion clinics in the wake of the Supreme Court's Dobbs decision that overturned Roe v. Wade.[38]

POLICY RECOMMENDATIONS

Given the potential risks associated with ALPRs, we recommend that communities concerned about the use of ALPRs should consider: a ban, moratorium, or the implementation of the safeguards listed below.

Banning ALPRs or Moratoriums

An effective and straightforward option would be for policymakers to outright ban license plate readers. Many jurisdictions across the country have chosen this option, including cities in California, Indiana, and New York.[39] Recently, the City Council of Ypsilanti, Michigan, voted to ban the technology.[40] It may be difficult to generate enough political willpower to counter law enforcement's likely support of ALPRs, making a moratorium a more realistic compromise. This would give policymakers the time to develop the appropriate policies that ensure the harm posed by the technology is limited.

Enforcing Appropriate Safeguards

In communities where ALPR technology is already in place and utilized, legislators should put in place preventative measures to mitigate the risks outlined above. Instead of merely punishing officers after they misuse the technology, policies and procedures need to be implemented that provide proactive oversight that can prevent abuses. These should include:

Retention Limits

- Police should not be allowed to store any data long term on license plates that do not match hot lists.
- The ALPR system should not be allowed to store or transmit plate images and associated data unless the alert resulted in legal action (e.g., New Hampshire policy).

Requiring Warrants

- Police must have warrants for any historical searches of ALPR data.

Transparency

- Policies governing ALPR use should be publicly available for all community members to access. Community members should be able to know exactly:
    - Where law enforcement places the cameras?
    - What kind of cameras the department has access to (mobile, stationary, etc.)?

    - If the department has access to a third-party database and if the party shares their information with others or a centralized database.
    - What are the retention limits?
    - What specific circumstances can an officer conduct a historical search?
    - How do plates get added to hot lists, and how are those lists maintained over time?
- Community members should be able to provide feedback on those policies.

Auditing

- Ongoing monitoring and periodic audits should take place to identify both misuse of the technology and any disparate impacts the technology is having.
- All information regarding the use of the technology should be recorded, including but not limited to:
    - For automatic alerts: Reason for the alert, the outcome of the alert, whether the information was shared with others
    - For historical searches: Reason for any search, which officer conducted the search, time, and location of the search

The University of Michigan's Science, Technology, and Public Policy (STPP) program is a research, education, and policy engagement center concerned with cutting-edge questions at the intersection of science, technology, policy, and society. This memo was written as part of STPP's community partnerships initiative, where we work with organizations that have concerns related to a current or anticipated science or technology issue. If you want us to take a deep dive into the implications of an emerging technology in your community, or if your city is considering implementing ALPRs and you want more information, contact us at **stpp@umich.edu**.

ENDNOTES

[1] Electronic Frontier Foundation. "Automated License Plate Readers (ALPRs)," May 15, 2020. https://www.eff.org/pages/automated-license-plate-readers-alpr

[2] Kooser, Amanda. "Fake Cactuses Host Hidden License-Plate Cameras in Arizona Town." CNET, May 11, 2015. https://www.cnet.com/roadshow/news/license-plate-readers-hidden-in-fake-cactuses-in-arizona

[3] Barrett, Devlin. "Gun-Show Customers' License Plates Come Under Scrutiny." WSJ, October 3, 2016. https://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302;

Glenberg, Rebecca. "Virginia State Police Used License Plate Readers At Political Rallies, Built Huge Database | News & Commentary." American Civil Liberties Union, August 29, 2022. https://www.aclu.org/news/national-security/virginia-state-police-used-license-plate-readers

[4] Díaz, Ángel, and Rachel Levinson-Waldman. "Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use." Brennan Center for Justice, September 10, 2020. https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations

[5] Howle, Elaine M. "Automated License Plate Readers," February 13, 2020. https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf

[6] Talla, Vasudha and ACLU. "Documents Reveal ICE Using Driver Location Data From Local Police for Deportations | News & Commentary." American Civil Liberties Union, September 6, 2022.

[7] Department of Homeland Security. "Privacy Impact Assessment for the CBP License Plate Reader Technology," July 6, 2020. https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp049a-cbplprtechnology-july2020.pdf

[8] AFSC. "Motorola Solutions Inc." AFSC Investigate, March 4, 2021. https://investigate.afsc.org/company/motorola-solns

[9] Motorola Solutions. "License Plate Recognition," January 25, 2023. https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems.html

[10] Electronic Frontier Foundation. "Automated License Plate Readers (ALPRs)," May 15, 2020. https://www.eff.org/pages/automated-license-plate-readers-alpr

[11] Cheng, Isabella. "Flock Raises Another $150 Million, Valuation Now At $3.5 Billion." IPVM, February 16, 2022. https://ipvm.com/reports/flock-e?code=wskdgsd

[12] Stanley, Jay. "Fast-Growing Company Flock Is Building a New AI-Driven Mass-Surveillance System." American Civil Liberties Union, March 3, 2022. https://www.aclu.org/report/fast-growing-company-flock-building-new-ai-driven-mass-surveillance-system

[13] Center for Evidence-Based Crime Policy AddressGeorge Mason University. "The Rapid Diffusion of License Plate Readers in US Law Enforcement Agencies," 2019. https://www.ojp.gov/ncjrs/virtual-library/abstracts/rapid-diffusion-license-plate-readers-us-law-enforcement-agencies

[14] Motorola Solutions. "License Plate Recognition," January 25, 2023.

[15] Flock Safety, 2023. https://www.flocksafety.com

[16] Holder, Sarah, and Fola Akinnibi. "Suburbs of Surveillance," August 4, 2021. https://www.bloomberg.com/tosv2.html?vid=&uuid=ef3123e7-9cf8-11ed-b269-466a444e6159&url=L25ld3MvZmVhdHVyZXMvMjAyMS0wOC0wNC9zdXJ2ZWlsbGFuY2Utc3RhcnR1cC1icmluZ3MtcG9saWNlLXRlY2gtdG8tbmVpZ2hib3Job29kcw==

[17] National Conference of State Legislatures. "Automated License Plate Readers: State Statutes," February 3, 2022. https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes

[18] Cuddemi, Jordan. "After Ban Ends, Sunapee Police Among First With Plate Reader." Valley News, June 18, 2018. https://www.google.com/url?q=https://www.vnews.com/Sunapee-Police-Will-Get-a-License-Plate-Reader-Other-N-H-Chiefs-Say-It-Isn-t-a-Priority-18117871

[19] National Conference of State Legislatures. "Automated License Plate Readers: State Statutes," February 3, 2022. https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes

[20] National Conference of State Legislatures. "Automated License Plate Readers: State Statutes," February 3, 2022. https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes

[21] Ng, Alfred. "Supreme Court Says Warrant Necessary for Phone Location Data in Win for Privacy." CNET, June 22, 2018. https://www.cnet.com/tech/mobile/supreme-court-says-warrant-necessary-for-phone-location-data

[22] "UNITED STATES V. YANG," May 4, 2020. https://cdn.ca9.uscourts.gov/datastore/opinions/2020/05/04/18-10341.pdf;

Torres, Gerald, Jeannie Suk Gersen, John Manning, Martha Minow, Sherrilyn Ifill, Gerald Torres, Jeannie Suk Gersen, John Manning, Martha Minow, and Sherrilyn Ifill. "Commonwealth v. McCarthy." Harvard Law Review, June 10, 2021. https://harvardlawreview.org/2021/06/commonwealth-v-mccarthy

[23] Electronic Frontier Foundation. "Neal v. Fairfax County Police Department," October 29, 2020. https://www.eff.org/cases/neal-v-fairfax-county-police-department

[24] "Kansas v. Glover." Oyez. Accessed January 25, 2023. https://www.oyez.org/cases/2019/18-556

[25] Stanley, Jay. "Fast-Growing Company Flock Is Building a New AI-Driven." American Civil Liberties Union, March 3, 2022. https://www.aclu.org/report/fast-growing-company-flock-building-new-ai-driven-mass-surveillance-system

[26] Potts, Jason. "Research in Brief: Assessing the Effectiveness of Automatic License Plate Readers," March 2018. https://www.theiacp.org/sites/default/files/2018-08/March+2018+RIB.pdf

[27] Crockford, Kade. "San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error | News & Commentary." American Civil Liberties Union, May 13, 2014. https://www.aclu.org/news/privacy-technology/san-francisco-woman-pulled-out-car-gunpoint-because

[28] Snowdon, Quincy. "Aurora Cop Disciplined after Forcing Black Girls to Lie Face down on Pavement Running for Las Animas County Sheriff." Sentinel Colorado, July 7, 2021. https://sentinelcolorado.com/news/metro/aurora-cop-disciplined-after-forcing-black-girls-to-lie-face-down-on-pavement-running-for-las-animas-county-sheriff

[29] Lecher, Colin. "Privacy Advocate Sues over License Plate Reader Error." The Verge, February 21, 2019. https://www.theverge.com/2019/2/21/18234785/privacy-advocate-lawsuit-california-license-plate-reader

[30] Norris, Zach. "Opinion: At Gunpoint, Police Handcuffed Me after License-Plate Reader Error." The Mercury News, June 24, 2021. https://www.mercurynews.com/2021/06/23/opinion-at-gunpoint-police-handcuffed-me-because-of-a-license-reader-error

[31] ACLU. "You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements," July 2013.

[32] ACLU. "You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements," July 2013.

[33] Gurman, Sadie. "AP: Across US, Police Officers Abuse Confidential Databases." AP NEWS, September 28, 2016. https://apnews.com/699236946e3140659fff8a2362e16f43/ap-across-us-police-officers-abuse-confidential-databases

[34] Gurman, Sadie. "AP: Across US, Police Officers Abuse Confidential Databases." AP NEWS, September 28, 2016. https://apnews.com/699236946e3140659fff8a2362e16f43/ap-across-us-police-officers-abuse-confidential-databases

[35] Loging, Shawn. "Kechi police lieutenant's arrest puts Flock technology under scrutiny," November 4, 2022. https://www.kwch.com/2022/11/04/kechi-police-lieutenants-arrest-puts-flock-technology-under-scrutiny

[36] Goldman, Adam, and Matt Apuzzo. "NYPD Defends Tactics Over Mosque Spying; Records Reveal New Details On Muslim Surveillance." Huffington Post, April 25, 2012. https://www.huffpost.com/entry/nypd-defends-tactics-over_n_1298997

[37] Gillula, Jeremy, and Dave Maass. "What You Can Learn from Oakland's Raw ALPR Data." Electronic Frontier Foundation, January 21, 2015. https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data

[38] Benson, Thor. "The Danger of License Plate Readers in Post-Roe America." WIRED, July 7, 2022. https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/amp

[39] Pedersen, Haley. "Communities Across the Country Reject Automated License Plate Readers." Electronic Frontier Foundation, August 21, 2019.

[40] Hakala, Josh. "Ypsilanti City Council Bans License Plate Readers Citing Invasion of Privacy." WEMU-FM, September 14, 2022. https://www.wemu.org/wemu-news/2022-09-14/ypsilanti-city-council-bans-license-plate-readers-citing-invasion-of-privacy

[41] NH Rev Stat § 261:75-b (2016) https://law.justia.com/codes/new-hampshire/2016/title-xxi/chapter-261/section-261-75-b