GOVERNMENT OF THE DISTRICT OF COLUMBIA
POLICE COMPLAINTS BOARD
OFFICE OF POLICE COMPLAINTS

Office of Police Complaints
Michael G. Tobin, Executive Director

POLICE COMPLAINTS BOARD
Paul Ashton, Chair
Commander Morgan Kane
Bobbi Strang
Jeffrey Tignor
Kurt Vorndran

PCB POLICY REPORT #20-2:
AUTOMATED LICENSE PLATE READERS

Introduction & Overview:

An automated license plate reader (ALPR)[1] is a surveillance technology used by many law enforcement agencies to capture the license plate number and location data of all passing cars.[2] ALPR systems can be mobile, mounted on the dash of police patrol vehicles, as well as stationary, at traffic lights and signs. ALPR systems capture license plate snapshots at the speed of thousands per minute, and law enforcement agencies store the information obtained in a searchable database. The retention of these images allows law enforcement officers and others to compare captured plate numbers against those of stolen vehicles, or conduct other investigations. This report examines the privacy concerns inherent in the retention of ALPR data as well as transparency concerns regarding the sharing of ALPR information with private companies.[3]

The use of ALPR technology can be a useful tool to aid in law enforcement's ability to solve crimes, but it also poses specific privacy concerns to those whose license plates are read. The information retained by ALPR technology "may be inaccurate, placed into databases and shared without restrictions on use, retained longer than necessary, and used or abused in ways that could infringe on individuals' privacy."[4]

According to the National Conference of State Legislatures, at least fourteen states in addition to the District have adopted legislation relating to the use of ALPR technology or the retention of data gained from ALPR technology.[5] The policies vary widely by state and even county, in regards to how long non-hit ALPR data may be stored.[6] "Non-hit" or "passive" data means

---

[1] Also known as License Plate Reader, or LPR.
[2] *See* https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers; http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx.
[3] The Police Complaints Board (PCB) is issuing this report pursuant to D.C. Code § 5-1104(d), which authorizes the Board to recommend to the District of Columbia Mayor, Council, MPD Police Chief, and the Director of District of Columbia Housing Authority reforms that have the potential to improve the complaint process or reduce the incidence of police misconduct.
[4] *See* http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx.
[5] *Id.*
[6] *See id.*

images of license plates that do not relate to any crime; in other words, the license plate information of innocent people. Retention policies run the gamut, with some mandating deletion within three minutes, to others that allow information to be stored indefinitely.[7]

Policies regarding transparency and specific purposes of use vary widely as well. For example, some departments specify that ALPR data is not to be used to monitor people exercising their first amendment rights (meaning officers could not use ALPR to detect who is protesting and use that information to target them), and some departments have specific regulations regarding sharing data with commercial entities.[8]

The debate is over how lawmakers and police department policies should balance the interests of crime solving against those of the privacy rights of community members. Currently, MPD and most other police departments have not publicly disclosed why they store innocent people's ALPR data for a particular length of time. According to Dr. Christopher Koper, Associate Professor in the Department of Criminology, Law and Society at George Mason University, police departments use stored ALPR information retroactively, as a pool of information at their fingertips to search if a crime does occur.[9]

There are no comprehensive statistics available that demonstrate the overall effectiveness of using non-hit, stored ALPR data to solve crimes. There are also no recent studies detailing the overall effectiveness of using ALPR data. However, a broad range of police agencies reported in 2012 that the use of ALPR technology substantially increased their number of auto theft arrests and vehicle recoveries.[10] Some argue that ALPR data assists law enforcement in solving some crimes faster than it would have without such data, but there is little to no research to back up this claim.[11]

Constitutional Rights:

The First Amendment of the United States Constitution includes the right of freedom of association.[12] The freedom to associate has long been recognized to include the right to keep such associations private.[13] Although there may not be a privacy issue with a single picture of a particular license plate being taken by law enforcement, if deleted shortly thereafter, privacy issues are created when such information is stored and later aggregated. ALPR technology can

---

[7] *See id.* (150 days, 60 days, 3 years, no limit, 3 minutes, 2 days, 21 days, 90 days, 30 days).
[8] *See* http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx; https://www.portofsandiego.org/harbor-police/compliance-with-sb34-license-plate-recognition-systems/file.html.
[9] Christopher Koper, Panel: *Technology and Policing*, CENTER FOR EVIDENCE-BASED CRIME POLICY SYMPOSIUM, George Mason University (June 26, 2017).
[10] Automated License Plate Recognition Systems, Policy and Operational Guidance for Law Enforcement, International Association of Chiefs of Police, 24 (2012). *See* Bruce Taylor et al., *Combating Vehicle Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology*, CRIMINAL JUSTICE REVIEW (2011).
[11] *See* https://netchoice.org/lprfacts/. Note, however, that the only statistic used here is self-reported opinions of various police agencies; other than that, only anecdotal evidence was used as a basis for ALPR effectiveness. *Id.*
[12] Randy L. Dryer et al., *Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother's Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action*, 55 Jurimetrics J., 225, 245 (2015). *See* U.S. CONST. Amend. I.
[13] *Id.*, at 245.

tell where someone is at a particular time on a particular day, and over time may track a person's movements.[14] "For example, ALPR systems could scan license plate numbers of vehicles parked at abortion clinics, drug treatment centers, or other locations that, while public, nonetheless may be considered private by the drivers of the vehicles."[15] This creates a potential privacy violation for drivers that they are being watched by the government, even if ALPR information is stored in the most benign and careful way, and for benign reasons. The inhibition comes from a person knowing that her driving habits have been collected and are being stored, without any suspicion that she has done anything wrong.[16] This is particularly applicable to ALPR data gathered from stationary spots such as a stoplight, since that ALPR system would capture data of all vehicles that stop at the light over a long period of time.[17] Thus, data retention of non-hit ALPR information causes a right to privacy issue if it is stored long enough to produce patterns of driver behavior.

The Fourth Amendment right against unreasonable searches is also applicable when discussing ALPR data. "The Supreme Court has made clear, location history can paint a detailed picture of our personal lives. The longer the data is stored, the more intimate the picture."[18] In Carpenter v. US, the Court held that while law enforcement viewing information such as location is not a "search," if historical data over a certain period of time is searched, the Fourth Amendment is implicated, and access to that data requires a warrant.[19]

A recent line of cases involving the nearby Fairfax County Police Department (FCPD), starting with *Neal v. Fairfax County Police Dep't*, 94 Va. Cir. 485, 486 (2016) considered the issue of whether license plate information is "personal information."[20] Under Virginia's Government Data Collection and Dissemination Practices Act, government agencies are not to collect "personal information" unless it is authorized by law.[21] After the case was sent back to the Circuit Court from the Virginia Supreme Court, on April 1, 2019, a Fairfax County judge granted the ACLU of Virginia's petition for an injunction prohibiting the FCPD from collecting and storing ALPR data outside of an investigation or intelligence gathering related to a criminal investigation.[22] While this case is not binding in DC, it is instructive and illustrates issues to be aware of.

A further privacy issue posed by law enforcement use of ALPR data is that of transparency; with what entities do police departments share ALPR data? Most private ALPR companies have partnerships with police departments, allowing officers access to large private databases.[23] This

---

[14] *Id.*
[15] *Id.* This includes first amendment activities such as peaceful protests, etc.
[16] *Id.* at 246.
[17] *Id.*
[18] Second Report of the Axon AI & Policing Technology Ethics Board: Automated License Plate Readers, Oct. 2019, available at: https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/Axon_Ethics_Report_2_v2.pdf.
[19] *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018).
[20] *Neal v. Fairfax County Police Dep't*, 94 Va. Cir. 485, 486 (2016).
[21] VA. CODE ANN §2.2-3800 (2001).
[22] *Neal v. Fairfax County Police Dep't*, 812 SE 2d 444 (Va. 2018); and https://acluva.org/en/cases/neal-v-fairfax-county-police-department.
[23] Dryer, *supra* note 12, at 247.

is a concern in part because private use of ALPR data is not held to the same privacy requirements as those used by government entities.[24] For example, the National Vehicle Location Service (NVLS), a database holding over 1.8 billion ALPR images, is run by a private company, Vigilant.[25] This database is the largest of its kind that exists, and pulls together data from law enforcement agencies as well as private sources, such as DRN, which includes 550 private repossession agencies and contributes millions of plates per month.[26]

> The database is used by more than 3,500 law enforcement agencies and 25,000 law enforcement investigators. Further, nothing prohibits those companies from selling or allowing access to private investigators, insurance companies, car rental companies, suspicious spouses, or others who may have an interest in tracking the movements of particular individuals or vehicles, including law enforcement.[27]

Allowing police departments to have access to such vast amounts of privately collected information is alarming, as it allows officers to access information far beyond the "jurisdictionally limited" ALPR data that they gather themselves.[28] This use of privately collected data is made worse when police departments are not transparent about how they collect ALPR data and who they share it with.

The American Civil Liberties Union (ACLU), argues that people should be aware of and able to access any data belonging to a car that they own if their information is being stored in such a database.[29] Police departments should also be transparent by disclosing if a third party has access to their ALPR data (and who the third party is), and should not share ALPR data with third parties who do not adhere to the same "retention and access principles."[30]

These concerns are exacerbated by the fact that there is evidence of police departments using ALPR data for investigations around First Amendment protected activity, both by law enforcement and groups with a particular political agenda.[31] There is also the possibility that ALPR data could be abused by those with access, as there have been documented cases of officers using ALPR data to stalk or harass individuals, or to tamper with and sell records they obtained.[32] Finally, as with any large data collection there is the risk of data breaches, which can

---

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Dryer, *supra* note 12, at 247.
[29] American Civil Liberties Union, *You Are Being Tracked, How License Plate Readers Are Being Used To Record Americans' Movements*, ACLU REPORT 32-33 (2013).
[30] *Id.*
[31] *See, e.g.*, Adam Goldman & Matt Apuzzo, With Cameras, Informants, NYPD Eyed Mosques, ASSOCIATED PRESS (Feb. 23, 2012), https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques (discussing NYPD tracking all of the vehicles outside of particular mosques); Brian M. Rosenthal, Anti-Abortion Activists Adopt a New Tactic: Tracking License Plates, HOUS. CHRON. (Aug. 13, 2014), , , https://www.houstonchronicle.com/news/politics/texas/article/Anti-abortion-activists-adopt-a-new-tactic-5687420.php (reporting on the safety risks and privacy risks experienced by people entering abortion clinics whose license plates are tracked by anti-abortion activists.)
[32] *See* Sadie Gurman, AP: Across US, Police Officers Abuse Confidential Databases, ASSOCIATED PRESS (Sept. 28, 2016), https://apnews.com/699236946e3140659fff8a2362e16f43.

lead to personal data being used for inappropriate or unlawful purposes.[33] For example, a 2015 research study by the Electronic Frontier Foundation found more than 100 exposed ALPR systems online, "often with totally open web pages accessible by anyone with a browser."[34] Three years later, a similar investigation found that little had improved, with the information from more than 150 ALPR cameras searchable on the internet, most using factory-default passwords.[35]

Metropolitan Police Department Policy:

The MPD General Order, "License Plate Reader Program,"[36] became effective in March 2014, and it describes the use of ALPR data for the MPD. ALPR technology is used on police vehicles and also mounted on poles or on the roadside in several areas.[37] Patrol car mobile data computers store ALPR data for up to 30 days, and then the ALPR system overwrites the data.[38] The same information is stored at MPD for up to 90 days and then destroyed.[39]

The General Order also states that "[t]hrough established agreements, MPD receives data and hits from other agencies' LPRs and handheld ticket issuance devices (e.g., the Department of Public Works or the Department of Transportation)."[40] There is no mention of third party databases or any additional detail given in regards to "other agencies" ALPR hits. The Order then goes on to disallow any civilian or sworn member from using the ALPR database for any purpose "other than official law enforcement purposes."[41] However, "official law enforcement purposes" is not further defined, and there is no specific mention of first amendment protections.

Recommendations:

To help improve and facilitate better relations, minimize the potential for constitutional violations, and increase trust between MPD officers and community members, the PCB recommends that:

1. MPD must ensure there is an easily identifiable and clear process for community members to obtain ALPR collected information about themselves. This can be accomplished through the existing FOIA process or some other means. The process should be outlined publicly on the MPD website, as the process for obtaining BWC footage currently is.

---

[33] *Supra*, Note 18.
[34] Cooper Quintin & Dave Maass, License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech, ELECTRONIC FRONTIER FOUND. (Oct. 28, 2015), https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive.
[35] See Zack Whittaker, Police License Plate Readers Are Still Exposed on the Internet, TECH CRUNCH (Jan. 22, 2019), https://techcrunch.com/2019/01/22/police-alpr-license-plate-readers-accessible-internet/.
[36] MPD uses the phrase License Plater Readers or LPRs, which is interchangeable with ALPRs.
[37] MPD General Order 303.09: License Plate Reader Program (Effective Date March 28, 2014).
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*

2. MPD must publicly identify any third parties that have access to the ALPR data and information, including other law enforcement agencies and private parties, and ensure all third parties adhere to the same principles as MPD in obtaining and deleting this information. MPD must also share publicly any ALPR databases, other than their own, to which MPD has access.[42]

3. MPD must be transparent with the community about all aspects of ALPR data collection. MPD must disclose how many systems and collection point receivers MPD has and what types; what, if any, safeguarding systems are in place to prevent the misuse of data (such as an audit schedule to detect any unauthorized access or sharing); whether any persons have been investigated and disciplined for noncompliance with ALPR policies, and costs associated with the purchase, operation, maintenance, and any data sharing. This information should be posted on the MPD website.

4. MPD must revise General Order 303.09 to further define "official law enforcement purpose." Given that multiple protests occur constantly in the District, MPD must specifically state in the General Order that using ALPR data to track those at a protest is not an acceptable "official law enforcement purpose."

[42] On September 14, 2020 MPD informed OPC that MPD does not currently share its LPR data with any private entities, and only has a Memorandum of Understanding with the United States Secret Service. MPD stated they will share LPR data with other law enforcement agencies upon request. The PCB still recommends that MPD make this information public, and continues to do so should other agreements be made in the future.