June 19, 2024

Dear Council

I wrote extensively (via a couple of emails) and spoke briefly at the Council meeting on May 7, 2024 (emailed that as well) regarding Staff Report 24-080-CC regarding Automatic License Plate Readers.

Soody Tronson
Menlo Park Resident

Even though I was in attendance at the May 7, 2024, Council meeting, I left the meeting not entirely understanding what the next steps would be.

Issues Raised. On the one hand, many issues were raised about ALPRs, including:

- Negative impact on privacy rights,
- lack of substantiated data to support the expenditure and
- Efficacy (despite some "effectiveness" figures in the Staff Report, it was acknowledged during the meeting that the figures did not distinguish between coincidental correlation and causation).

Insufficient Data. While the Staff Report included statements such as "uptake in crime" etc.:

- There was no actual data on numbers or what type of crimes we were experiencing, nor was it known whether ALPRs would be beneficial to mitigating those "crimes."
- Nor did we hear of the circumstances of the Sharon Heights "burglaries" (e.g., will they have been mitigated with ALPR had they been placed where the City is proposing them to be installed, where the doors locked, were there any private cameras).

However, Council comments left me with the impression that reducing the duration of data storage was all that was needed (from 6 months to 30 days).

Accountability. During Council discussions, the Council emphasized that they would hold Flock "accountable." However, it is unclear what the Council's reference to "accountability" exactly means. If Flock fails to protect the data, what consequences will it face? So far, laws only provide for a "notice" requirement and nothing more. That is NOT the same as accountability. For example, sometimes the software will be plain wrong. There is little for the wrongly accused people to clear their names. As for Flock? It's not the company's problem. As its head of marketing states, using the software inappropriately would be a "breach of contract."[1] But that is hardly a mechanism for accountability.

Request. I request clarification on:

- What information (e.g., substantiated data-driven success and failures of the ALPR (related to the "crimes in Menlo Park") does the MPPD have to come back with to support its request to implement fixed ALPRs?
- What is the "accountability" or consequences the vendor or the MPPD will face if either breaches the terms of the "agreement" or laws?

[1] https://www.latimes.com/business/story/2019-09-12/flock-safety-license-plate-readers-los-angeles

- How do you determine the sufficiency of the data-retention period: 2 hours, 24 hours, 30 days, or six months? New Hampshire, for example, mandates footage of non-hit plates be deleted after three minutes.
- Can we have a report on the usage of various "surveillance technology" tools and military equipment MPPD is using?

ALPR Lack of Efficacy. Further, as provided in more detail below, despite the surge in their popularity, the efficacy of ALPRs has largely evaded serious inquiry. A project by the Secure Justice Org. reviewed the investigative leads generated by the ALPRs and the recovery of stolen cars in the City of Piedmont between 2013 and 2019 while comparing occurrences of motor vehicle theft before and after the ALPRs between 2004 and 2021.[2] In the Piedmont Study, the following observations resulted from the analyzed data, which point to the lack of efficacy of ALPRs:

- The ratio of Piedmont's ALPR systems license plate hits-to-investigative leads for law enforcement is subjectively low; less than 0.3% of hits equate to leads;
- The positive correlation between license plate hits, and investigative leads is weak;
- The positive correlation between plate "hits" and stolen vehicle recoveries is weak, indicating more plate hits do not necessarily entail more vehicle recoveries;
- There is statistical support that vehicle thefts after ALPRs are installed are observed to be lower, and
- The market value of recovered stolen vehicles during the years observed exceeds the City's costs to purchase the cameras. Still, given the absence of evidence of a causal relationship between ALPRs and recovered vehicles, it is not suggested that the costs to the City have been recuperated.

Vulnerability of ALPR. The Cybersecurity and Infrastructure Security Agency (CISA), a component of the U.S. Department of Homeland Security, released an advisory last week that should be a wakeup call to the thousands of local government agencies around the country that use ALPRs to surveil the travel patterns of their residents by scanning their license plates and "fingerprinting" their vehicles.[3] The bulletin outlines seven vulnerabilities in Motorola Solutions' Vigilant ALPRs, including missing encryption and insufficiently protected credentials.[4]

Vast Data & Breach. It's a general tenet of cybersecurity that you should not collect and retain more personal data than you are capable of protecting. More than 125 law enforcement agencies reported a data breach or cyberattacks between 2012 and 2020, according to research by former EFF intern Madison Vialpando.[5] The Motorola Solutions article claims that ransomware

[2] https://static1.squarespace.com/static/5edeeebc3032af28b09b6644/t/64a46a417c2a6637212e1ce3/1688496710563/2021_11_30_alpr.pdf

[3] https://www.cisa.gov/news-events/ics-advisories/icsa-24-165-19

[4] https://slate.com/technology/2019/09/flock-automatic-license-plate-readers-neighborhood-surveillance.html

[5] https://www.youtube.com/watch?v=58lICmpJTCk

attacks "targeting U.S. public safety organizations increased by 142 percent" in 2023. Yet, the temptation to "collect it all" continues to overshadow the responsibility to "protect it all." What makes the latest CISA disclosure even more outrageous is it is at least the third time in the last decade that major security vulnerabilities have been found in ALPRs. There have been numerous data breaches over the previous few years.[6]

Vigilantism. While this particular proposal was for the City to acquire Flock, the whole company (and those similar to it) are problematic, to say the least. The direct marketing of such products by Flock (and others) to individuals raises perhaps the most worrisome concern: encouraging vigilantism. These extralegal movements organized to take the law into one's own hands have long been with us. In his classic 1975 study "Strain of Violence," historian Richard Maxwell Brown observed that American vigilantism is an indigenous and deeply rooted part of our shared history. We have a lot of experience with private citizens meeting out their own versions of justice, and it is largely an ugly one.

Thank you. Meanwhile, I applaud Council Member Betsy Nash for not supporting such a governmental overreach. I also wish to thank Council Member Drew Combs for acknowledging that while a handful of Sharon Heights residents were there to support the implementation of ALPRs, we should not lose sight of the unheard voices of many more residents who were not in attendance. We cannot follow the voice of a handful to abridge the civil rights of the many or to justify such an expenditure throughout the City.

Further. The Staff Report (page H-1.2) stated, "In addition to the ALPR, the MPPD also proposed deployment of gunshot detection technology and its relative pricing as a companion to fixed ALPR deployment."

While there are hypes about these surveillance tools, such as ShotSpotter, most are not even effective in what they preach. ShotSpotter, a controversial police technology company, uses money, influence, and secrecy to benefit its bottom line. According to ShotSpotter, it supposedly yields a 97% accuracy rate. However, Boston Police records show nearly 70% of ShotSpotter surveillance technology (another technology used by police) alerts led to dead ends.

Senators Markey, Warren, and Rep. Pressley's Letter. On the ShotSpotter surveillance tool which MPPD is considering, on May 14, 2024, Senators Ed Markey and Elizabeth Warren and Rep. Ayanna Pressley issued a letter asking the U.S. Inspector General to investigate DHS grant funding spent on the ShotSpotter acoustic gunshot detection system, including whether ShotSpotter's use may lead to violations of Title VI of the Civil Rights Act of 1964.

It seems that the City of Menlo Park is too eager to not only abridge our civil liberties but also waste our money (yes, whether it's M.P., State, or Federal money, it's all our money, one way or another) on harmful toys.

Government officials across the U.S. frequently promote the supposed, and often anecdotal, public safety benefits of automated license plate readers (ALPRs), but rarely do they examine how this very same technology poses risks to public safety that may outweigh the crimes they are attempting to address in the first place. When law enforcement uses ALPRs to

[6] https://www.eff.org/deeplinks/2024/06/new-alpr-vulnerabilities-prove-mass-surveillance-public-safety-threat

document the comings and goings of every driver on the road, regardless of a nexus to a crime, it results in gargantuan databases of sensitive information, and few agencies are equipped, staffed, or trained to harden their systems against quickly evolving cybersecurity threats.

Widespread Use. While the City touts the widespread adoption of these surveillance tools as justification to purchase and use them, it should actually be a wakeup call to us all that before too long, if we don't object, we will have no more rights left.

For more resources, please see the following sections.

1. ALPR

1.1. Technology

ALPR systems gather data on passing cars in a manner that greatly exceeds human observation. The stated intention of such a system was that before the prevalence of ALPR technology, law enforcement officers would need to confirm plates visually and subsequently compare the license plate number with a database or central dispatch. ALPRs have the potential to mitigate staffing limitations and other associated labor and human capital costs.[7] ALPRs use a combination of high-speed cameras and computer software to log every license plate that passes by the camera. 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. Yet, 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.

ALPR cameras may be subdivided into two major groups in terms of their mount: Stationary and Mobile. In the case of stationary ALPR, when data is retained over a period, the analysis would be able to determine the frequency of a particular license plate traveling past a given camera network. It would likewise be able to determine travel patterns, plausibly allowing the investigators **to deduce** a driver's place of living or place of employment. Data ascertained by these systems are used to conduct primarily three generalized forms of investigation: real-time, historical, **and predictive**.

1.2. Data Sharing

Data collected at local agencies is shared with will pass through and be retained in the standard database that MPPD currently uses through the Northern California Regional Information Center (NCRIC).[8] The NCRIC may disseminate ALPR data to any governmental entity with an authorized law enforcement or public safety purpose for access to such data. The NCRIC assumes no responsibility or liability for the acts or omissions of other agencies in making use of the ALPR data properly disseminated.[9]

[7] https://ncric.ca.gov/wp-content/uploads/2024/05/NCRIC-ALPR-POLICY-2024.pdf

[8] https://ncric.org/html/ALPR-FAQ-Feb-2015.pdf

[9] https://ncric.org/html/NCRIC%20ALPR%20PIA.PDF

The NCIC database against which cars are automatically run is problematic because it is exempted from the 1974 Privacy Act, meaning accuracy and timeliness of the data are not required. Additionally, the retention period is dangerous because it can reveal sensitive information like places of worship, medical visits, relationships, and political activities. Furthermore, the 30-day period is a Flock promise and is not legally guaranteed; it could be extended on a whim. And despite saying data is not shared with other parties without consent, the fine print (section on releasing ALPR data) in Flock's privacy policy explains that Flock may "access, use, preserve and/or disclose the footage to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if Flock has a good faith belief that" it is necessary to protect the rights of another party or if it is an emergency. In these cases, the company simply notifies the user. This extremely vague statement allows Flock unlimited control over sensitive data, which it could sell.[10] This problem can be mitigated by states implementing data-sharing laws and shorter retention periods like New Hampshire, which mandates footage of non-hit plates be deleted after three minutes.[11]

Notwithstanding the various issues, including those raised above, if such systems were to be implemented, you should get the shortest retention period you can in our community. From worst to best, ACLU has provided approaches that can be taken to the retention of ALPR data.[12]

1.3. Aggregate Data from Private ALPRs

Law enforcement use of ALPR data is not limited to reads captured by departments' own devices; many departments have contracts with vendors that grant them access to private databases containing scans from private ALPRs and from other local and federal law enforcement agencies. For example, Vigilant Solutions (owned by Motorola Solutions), a leading provider of ALPR data to police based in Livermore, California, sells access to its database of more than 5 billion license plate scans collected across the country, including 1.5 billion reads provided by law enforcement agencies. This process creates a revolving door of license plate scans from law enforcement to Vigilant Solutions back to law enforcement agencies.[13]

In light of the wide saturation of license plate readers, it is critical that the use of these devices be accurate, bias-free, and protective of established legal values and constitutional rights. Unfortunately, publicly available information suggests that this is not the case. This may explain why at least 16 states have passed laws regulating the use of ALPRs or the use of data collected by the devices.[14]

1.4. ALPR EFFICACY

[10] https://www.acluok.org/en/news/threat-privacy-and-civil-liberties-automatic-license-plate-readers#:~:text=The%20NCIC%20database%20against%20which,the%20data%20is%20not%20required.

[11] https://www.gencourt.state.nh.us/rsa/html/XXI/261/261-75-b.htm

[12] https://www.aclu.org/news/privacy-technology/how-to-pump-the-brakes-on-your-police-departments-use-of-flocks-mass-surveillance-license-plate-readers

[13] https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations

[14] https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes

Despite the surge in their popularity, the efficacy of ALPRs has largely evaded serious inquiry. A project by the Secure Justice Org., reviewed the investigative leads generated by the ALPRs and the recovery of stolen cars in the City of Piedmont between the years 2013–2019, while comparing occurrences of motor vehicle theft before and after the ALPRs, between 2004–2021.[15] In the Piedmont Study, the following observations resulted from the analyzed data:

- The ratio of Piedmont's ALPR systems license plate hits-to-investigative leads for law enforcement is subjectively low, less than 0.3% of hits equate to leads;
- The positive correlation between license plate hits and investigative leads is weak;
- The positive correlation of plate "hits" and stolen vehicle recoveries is weak, indicating more plate hits does not necessarily entail more vehicle recoveries;
- There is statistical support that vehicle thefts after ALPRs are installed are observed to be lower; and
- The market value of recovered stolen vehicles during the years observed exceeds the City's costs to purchase the cameras but given the absence of evidence of a causal relationship between ALPRs and recovered vehicles, it is not suggested that the costs to the City have been recuperated.

The low ratio of hits to investigative leads casts doubt on the practical significance of the reliability of ALPRs to translate hits of license plates to investigative leads for law enforcement. The findings also show that the correlation between license plate hits and investigative leads is statistically weak and the correlation of plate hits and stolen vehicle recoveries is also statistically weak. The low degree of correlation fails to demonstrate that plate hits are a strong predictor of the desired responses. However, the average number of stolen vehicles since the installation of ALPRs is observed to be lower than years prior, and sample means comparisons are statistically significant. Though the collection of this data does not meet the standards of a controlled study, for which those tests are most useful. With numerous variables, it would be improper to make the firm conclusion that ALPRs are an effective treatment for deterring vehicle theft. However, that possibility is not rejected. Despite the market value of recovered vehicles exceeding the camera costs, given the lack of evidence supporting a strong relationship between the cameras and recovered vehicles, it cannot be determined that the camera costs were recuperated.[16]

The use of ALPRs is "almost entirely unregulated and can be subject to abuse," according to a report from the University of Michigan.[17] **This is especially true at the federal level, which has no guidelines for ALPR usage**. As a result, "law enforcement and private actors can use the technology however they wish," the report added. There have also been reported instances of police officers using data collected from ALPRs to "get information on romantic partners,

[15] https://static1.squarespace.com/static/5edeeebc3032af28b09b6644/t/64a46a417c2a6637212e1ce3/1688496710563/2021_11_30_alpr.pdf

[16] https://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.

[17] https://stpp.fordschool.umich.edu/news/2023/automated-license-plate-readers-widely-used-subject-abuse

business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work," the report said.

Many civil rights groups have cautioned the widespread use of ALPRs as a potential violation of privacy.[18] ALPRs collect and store data on the cars they scan, and this data is "sometimes pooled into regional sharing systems," the American Civil Liberties Union (ACLU) reported. As a result, "enormous databases of innocent motorists' location information are growing rapidly," the ACLU added, and this information is often kept for years "with few or no restrictions to protect privacy rights." In the aftermath of Roe v. Wade being overturned, there are also concerns that state governments could use ALPRs to "track people trying to cross state lines" to get an abortion.[19]

In 2019, The California State Auditor Office conducted an audit of local law enforcement agencies' use of ALPRs that revealed the handling and retention of ALPR images and associated data did not always follow practices that adequately consider an individual's privacy. The audit resulted in introduction of SB 210, the License Plate Privacy Act, in 2021 which required that ALPR data – which in addition to license plate number, includes personal data like birth date and name – be deleted within 24 hours after a law enforcement agency determines that the license plate is not a match for a vehicle involved in criminal activity, quote, "ALPR data should only be retained when it is relevant to a criminal investigation." The Bill was held on suspense in Senate Appropriations Committee. With the failure of the bill, none of these safeguards are in existence. [20]

ALPR camera systems collect and store location information about drivers, including dates, times, and locations. This sensitive information can reveal where individuals work, live, associate, worship—or seek reproductive health services and other medical care.[21] Civil liberties groups have demand California police stop sharing drivers' location data with police in anti-abortion states. This sharing by 71 California police agencies in 22 counties (as of May 2023), violates state law and could be used by other states to identify and prosecute abortion seekers and providers.[22]

1.5. High error rates

Errors can arise in at least two ways — inaccurate hot lists and inaccurate reads. To be sure, license plate readers have had some high-profile successes.[23]

1.6. Privacy and data security concerns

[18] https://theweek.com/politics/section-702-government-spy-powers-debate

[19] https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/

[20] https://legiscan.com/CA/text/SB210/id/2238580

[21] https://www.eff.org/press/releases/civil-liberties-groups-demand-california-police-stop-sharing-drivers-location-data

[22] 2022 law (AB 1242)

[23] https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations

An extremely small percentage of cars scanned by ALPRs — generally far below 1 percent — are connected to any crime or wrongdoing.[24] For example, an audit found that 99.9 percent of the ALPR images stored by the LAPD are for vehicles not on a hot list at the time a license plate was scanned.[25] A 2019 California audit on Automated License Plate Readers, concluded:[26]

- 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.
- 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.

In addition to information generated by ALPRs, police officers can also add to and store sensitive information in the databases housing license plate scans through open text fields and hot lists available in the user interface. For example, the California state auditor found that law enforcement can input information including personal information such as names, addresses, dates of birth, and physical descriptions, and they can also store criminal justice information such as criminal charges and warrant information. License plate readers have also been known to capture private information, such as shots of children exiting a car in the driveway of a home or activity inside an open garage — information that surely should not be retained. This is information that goes far beyond the legitimate need to find stolen cars or vehicles linked to AMBER Alerts. The ongoing storage of this wide array of sensitive information also raises security concerns, as this information can be vulnerable to data breaches and hacking. The data security applied to ALPR data may not be commensurate with the sensitivity of the data being held. [27]

QUESTION: If an audit of the existing MPPD ALPR were conducted today, how would it fair?

The Cybersecurity and Infrastructure Security Agency (CISA), a component of the U.S. Department of Homeland Security, released an advisory last week that should be a wakeup call to the thousands of local government agencies around the country that use ALPRs to surveil the travel patterns of their residents by scanning their license plates and "fingerprinting" their

[24] https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations

[25] https://information.auditor.ca.gov/reports/2019-118/summary.html

[26] https://information.auditor.ca.gov/reports/2019-118/summary.html

[27] https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations

vehicles.[28] The bulletin outlines seven vulnerabilities in Motorola Solutions' Vigilant ALPRs, including missing encryption and insufficiently protected credentials.[29]

1.6.1. Vulnerabilities Detected by CISA.

- Authentication Bypass Using an Alternate Path or Channel,
- Cleartext Storage in a File or on Disk,
- Use of Hard-coded Credentials,
- Insufficiently Protected Credentials,
- Missing Encryption of Sensitive Data, Authentication Bypass by Capture-replay

1.7. Data sharing concerns

Many vendors allow their law enforcement clients to share and receive ALPR data from other law enforcement agencies. For example, through Vigilant Solutions' Law Enforcement Archival Reporting Network (LEARN), police departments can elect to automatically share their collection of license plate reads with outside law enforcement partners that are also part of the network. These data sharing arrangements are not always made public or adequately tracked by police departments, which can result in impermissible or unaccountable sharing. An ACLU investigation found that more than 80 local police departments had set up their LEARN settings to share ALPR data with U.S. Immigrations and Customs Enforcement (ICE), even though the practice may violate local privacy laws or sanctuary policies.[30] In one instance, the California state auditor found that despite efforts to limit data sharing with ICE, confusing vendor settings had left three different ICE agencies with access to ALPR data from Marin County Sheriff's Office, frustrating compliance with a California law that places controls on local police cooperation with immigration authorities.[31]

1.8. Issues with Private ALPR

Given that ALPRs are often used to watch neighborhoods, many police departments tout them as tools to enhance community security. Flock Safety, an ALPR manufacturer, claims to have "reduced crime in their cities' markets by 70% and have made more than 2,500 communities safer," the Pensacola News Journal reported. Flock allows communities to receive a consistent stream of data about neighborhood crimes, including burglary, home theft, vandalism and mail theft, according to its website.

As more companies sell ALPRs to homeowners, additional data sharing concerns emerge. For example, this trend allows police officers to expand the reach of their surveillance systems by providing them with access to private device feeds that may be outside the scope of law enforcement policies governing their own equipment (if any exist at all). When police officers

[28] https://www.cisa.gov/news-events/ics-advisories/icsa-24-165-19

[29] https://slate.com/technology/2019/09/flock-automatic-license-plate-readers-neighborhood-surveillance.html

[30] https://casetext.com/statute/revised-statutes-of-nebraska/chapter-60-motor-vehicles/article-32-automatic-license-plate-reader-privacy-act/section-60-3206-governmental-entity-duties-report-contents

[31] https://information.auditor.ca.gov/pdfs/reports/2019-118.pdf

solicit data from private ALPR systems, the decision to share information is up to the individual homeowner or the private company providing the service. While companies may maintain privacy policies that explain the situations in which they share information with law enforcement, the policy only covers the company and the person who purchased the devices. The registered owners of vehicles tracked and logged by these private devices will not receive notice or an opportunity to object to data sharing arrangements between police and private individuals. For example the FLOCK Privacy Policy states: "We may also access, use, preserve and/or disclose your personal information or Recordings to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if we have a good faith belief that such access, use, preservation or disclosure is reasonably necessary to: (a) comply with a legal process or request; (b) enforce our Terms of Service, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Flock, its users, a third party, or the public as required or permitted by law.[32]

While this particular proposal was for the City to acquire Flock, the whole company (and those similar to it) are problematic to say the least. The direct marketing of such products by Flock (and others) to individuals raises perhaps the most worrisome concern: encouraging vigilantism. These extralegal movements, organized to take the law into one's own hands, have long been with us. In his classic 1975 study "Strain of Violence," historian Richard Maxwell Brown observed that American vigilantism is an indigenous and deeply rooted part of our shared history. We have a lot of experience with private citizens meting out their own versions of justice, and it is largely an ugly one.

1.9. Work Arounds

Automatic license plate recognition systems are a mass surveillance technology designed to identify owners of vehicles by computer using optical character recognition (OCR) to automatically read your license plate. Like other forms of automated photo enforcement and redlight camera use, the rate of their proliferation is outstripping the rate of privacy laws to limit their use on Constitutional grounds.

Such systems have been used to track movements of millions of law-abiding motorists as well as gathering information about people who attend public events–such as gun-shows and political rallies. These systems are also being used by both governmental and privately-owned companies to collect meta-data, which is a fancy term to describe the aggregation of plate recognition data to determine the movements of motorists and the places they frequent. This data can be used to build a profile of any given citizen.

While a good GPS radar detector or WAZE can alert you to the presence of fixed camera systems they can't prevent your plate from being photographed.

There is an increasing effort by the states to design license plates to specifically reflect infrared light in the near-infrared spectrum and be easily recognizable to the OCR (optical character recognition) function of these systems. Plates that have very light solid light

[32] FLOCK Privacy Policy: https://www.flocksafety.com/privacy-policy

backgrounds and dark characters are the easiest to read as these systems rely on sufficient contrast between them.

The most desired plates, for a motorist concerned with maximizing their privacy, would be those with complex (i.e., "noisy) backgrounds and holographic elements.

There are some active systems (ALPR blockers or ALPR jammers) that are available that flash-back when flashes are detected, but we haven't found them to be sufficiently reliable in preventing plates from being read or photographed. Now that many of these systems have shifted to using I.R. photography and IR-flash photography, these ALPR jammers are unfortunately even less effective as they are only designed to work in the visible spectrum.

There are active and passive license plate reader jammer out there. One such countermeasure is called the Veil Stealth Coating. Veil is a broad-band infrared-absorbing coating designed to be applied to plates and clear license plate covers and absorbs the light used by these systems. Plates which are treated will appear very dark to these systems imaging components making optical character recognition much more difficult to perform since these systems need sufficient contrast between the numbers and letters and the background of the plate. (see picture below). Veil absorbs a wide spectrum of infrared light which makes its effective at countering a variety of these systems which operate on different I.R. wavelengths including, 810nm, 850nm, 940nm, and 950nm.[33]

So, what is next? Do we think that those professional car thieves or otherwise, won't be using these tool to circumvent ALPRs?

It is important to ask serious questions about surveillance technology because modern surveillance technology really has a direct impact on the ability of people to live free, fulfilling, and, frankly, safe lives. Systems like automated license plate readers, like drones, even video cameras that have been around for decades, massively expand the government's power to be able to watch us to be able to track where we go and who we associate with. And with that comes power, right? That increases the government's ability, and specifically, in many cases, law enforcement ability to watch people, to watch list people, to bring the light weight of the criminal justice system and the carceral system down on people. Because surveillance massively expands these powers that the government traditionally just didn't have, it's really something we have to pay attention to. And it cuts across not just the criminal legal system, but everything from immigration to access to social services to now receiving access to reproductive care is impacted by surveillance.[34]

Article one, section one of the California's constitution creates an express right to privacy that is unique, is different, and it's more of an affirmative right than the federal constitutional right, which is framed as a negative right. And that right was actually put into the constitution by voters.

Sometimes agencies will say they will want to use them to search for stolen vehicles or Amber Alerts. But the reality is that most ALPR programs operate in what's called a dragnet

[33] https://www.stealthveil.com/guides/anpr-alpr-countermeasures-blockers-and-privacy/

[34] https://btlj.org/2022/12/berkeley-technology-law-journal-podcast-automatic-license-plate-readers-with-aclu-attorney-matt-cagle/

fashion, which means the cameras are always on and they're just collecting any vehicle that passes within the sights of those cameras. And that includes our locations, that includes where we're at, and people that have nothing to do with an active investigation or any of the sort of core public safety concerns in the community. That might not be a satisfying answer. But I think the onus is really on police to explain better how these systems are being used and why they actually do provide a public safety benefit, because it's very often not clear that that benefit exists.

Over the last decade, **California** has built up some of the nation's strongest driver privacy protections, thanks to the hard work of activists, civil rights groups, and elected leaders. Automatic license plate readers collect and store highly sensitive information that can reveal where we work, live, worship, or seek reproductive health services. Sharing any ALPR information with out-of-state or federal law enforcement agencies has been forbidden in California since 2016. One law in particular, often called **S.B. 34** (a 2016 law) on the books for half a dozen years at this point), prohibits police from circulating detailed maps of people's driving patterns with the federal government and agencies in other states– a protection that has only grown more important with the end of Roe v. Wade and the subsequent surge in abortion criminalization.

However, despite this law,

But dozens of California police departments have decided to defy the law, even after receiving clear guidance from California Attorney General Rob Bonta, the chief law enforcement officer in the state. ACLU of Northern California and its partners sent Attorney General Bonta a letter listing 35 police agencies that have refused to comply with the law and protect driver privacy. Many of these public agencies were sharing with hundreds of out-of-state, state and federal law enforcement agencies (e.g., Marin County Sheriff) for seemingly no reason at all, sending the sensitive locations of drivers across state lines into agency databases, where they couldn't then exercise any oversight over how the information was used.[35]

2. Gunshot Detection Technology

Public safety shouldn't rely on unproven, faulty technologies that threaten basic civil rights and civil liberties.

The Staff Report provided that (page H-1.2) in addition to the ALPR, the MPPD also proposed deployment of gunshot detection technology, and its relative pricing as a companion to fixed ALPR deployment. Gunshot detection technology has been removed from this current presentation and proposal, to be potentially explored at a later time.

While there are hypes about these surveillance tools, such as ShotSpotter, most are not even effective in what they preach. ShotSpotter, a controversial police technology company, uses money, influence, and secrecy to benefit its bottom line. According to ShotSpotter, it supposedly yields a 97% accuracy rate.

[35] https://www.aclu.org/news/privacy-technology/dozens-of-police-agencies-in-california-are-still-sharing-driver-locations-with-anti-abortion-states-were-fighting-back

However, Boston Police records show nearly 70% of ShotSpotter surveillance technology (another technology used by police) alerts led to dead ends.[36]

On the ShotSpotter surveillance tool which MPPD is considering, on MAY 14, 2024 Senators Ed Markey and Elizabeth Warren and Rep. Ayanna Pressley issued a letter asking the U.S. Inspector General to investigate DHS grant funding spent on the ShotSpotter acoustic gunshot detection system, including whether ShotSpotter's use may lead to violations of Title VI of the Civil Rights Act of 1964.[37]

The lawmakers wrote, "Several recent reports have cast substantial doubt on the accuracy and effectiveness of the 'ShotSpotter' gunshot detection system and have raised serious questions about its contribution to unjustified surveillance and over-policing of Black, Brown, and Latino communities... We request that the DHS Office of Inspector General (OIG) investigate DHS's spending of taxpayer dollars on ShotSpotter, including potential violations of Title VI of the Civil Rights Act of 1964, which prohibits recipients of federal financial assistance from discriminating based on race, color, and national origin."

What is the basis for MPPD considering this gunshot detection tool? Aside from civil liberties issues and the lack of efficacy, how many gunshots do we have in Menlo Park to justify such expenditure?

Other References. Here are a few more reference: [38] [39] [40] [41] [42] [43]

[36] https://data.aclum.org/2024/04/08/boston-shotspotter/

[37] https://www.markey.senate.gov/news/press-releases/senator-markey-colleagues-urge-dhs-to-investigate-federal-funding-of-shotspotter-gunshot-detection-system

[38] https://www.acluok.org/en/news/threat-privacy-and-civil-liberties-automatic-license-plate-readers#:~:text=Flock%20maintains%20the%20system%20is,in%20the%20criminal%20legal%20system

[39] https://www.eff.org/deeplinks/2022/11/rise-police-advertiser

[40] https://slate.com/technology/2019/09/flock-automatic-license-plate-readers-neighborhood-surveillance.html

[41] https://www.forbes.com/sites/thomasbrewster/2024/02/27/flock-safety-surveillance-broke-state-law/?sh=6d48f4102a8f

[42] https://www.beaconjournal.com/story/news/2022/06/14/norton-rejects-surveillance-cameras-week-after-akron-approval-flock-safety-privacy-hacking-license/7619817001/

[43] https://www.govtech.com/public-safety/vehicle-surveillance-prompts-privacy-concerns-in-wichita-kan