January 29, 2014

Via electronic and United States mail

Alameda City Council
2263 Santa Clara Avenue
Alameda, CA 94501

Re: Analysis of Alameda's Draft Policy Manual for Automated License Plate Readers

Dear Alameda City Council:

Thank you for contacting the ACLU of Northern California regarding the City of Alameda's potential acquisition and use of automated license plate reader (ALPR) technology. We have reviewed a two-page draft policy manual numbered 462 ("draft policy manual") that contains provisions governing the use of ALPR technology and treatment of collected data.

In its current form, the draft policy manual lacks safeguards on the collection, use, and retention of any ALPR images and associated data and thus raises significant privacy and civil liberties concerns. For example, the manual directs officers to use ALPR in and around "major incidents," a broad statement that would permit officers to collect information on persons attending political protests or places of worship. In addition, few limits exist on access to ALPR records, inviting fishing expeditions for information on innocent people. In addition, members of the public lack a way to exercise meaningful oversight of the system and to access records collected about them. Finally, Alameda should engage the public in a debate about whether to acquire ALPR technology at all, and if so, for what purposes. For these and the additional reasons discussed below, Alameda's draft policy manual for ALPR does not contain sufficient civil liberties protections. Stronger, more comprehensive safeguards should be in place before ALPR is used. We urge Alameda not to adopt ALPR technology until a set of strong, enforceable safeguards is adopted following an open process of public input and debate.

The following document analyzes each section of the draft policy manual in turn, highlighting civil liberties issues and proposing safeguards Alameda should consider if the city decides to implement ALPR technology.[1] This analysis is intended to help Alameda determine how to balance legitimate public safety concerns with the civil liberties of all Alameda city residents.[2]

1. Privacy and civil liberties concerns raised by the use of ALPR

[1] The proposed safeguards in this document are based on the ACLU's report on ALPR, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, *available at* https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf, and on a draft document by the Department of Homeland Security, CCTV: Developing Best Privacy Practices, Report on the DHS Privacy Office Public Workshop, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.

[2] The contents of this document are not to be considered legal advice.

ALPR technology poses significant risks to privacy and civil liberties. ALPR consists of high-speed cameras and software that photograph every plate that comes into view, and many ALPR systems record the location of plates too. In some cases the photograph of the plate may also include the occupant of the vehicle.[3] ALPR's speed and capabilities allow law enforcement agencies to capture records relating to millions of drivers' movements over time. Databases containing aggregated ALPR records can be queried by individual plate, allowing officials to easily map out an innocent individual's movements over time and across cities, regions, and states. Some California agencies share their records with the federal government for other officials to access.[4] ALPR technology can be used to scan and record the vehicles at lawful protests, to track all movement in and out of an area[5], to specifically target certain neighborhoods[6] or organizations[7], or to place political activists on hot lists so that their movements trigger alerts.[8] Without proper safeguards and public oversight, the rich mosaic of records created by ALPR can easily be abused.

2. The Draft Policy Manual does not specify the purpose(s) justifying the adoption and use of ALPR

First, the "Purpose and Scope" section of the draft policy manual sets forth the basic purposes justifying the use of ALPR technology:

> **462.1 PURPOSE AND SCOPE**
>
> Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the California State Master Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. ALPRs may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

The draft policy manual fails to spell out the specific purposes justifying the use of ALPR. This paragraph describes a broad, and effectively limitless, set of purposes guiding ALPR's use. The terms such as "electronic surveillance" could entail surveillance of both lawful and unlawful

[3] A San Leandro man obtained records of the 112 times his vehicles had been photographed since 2008. One of the images showed him and his daughters stepping out of their vehicle in their driveway. Ali Winston, "License Plate Readers Tracking Cars," SFGATE, June 25, 2013, http://www.sfgate.com/bayarea/article/License-plate-readers-tracking-cars-4622476.php.

[4] Matthew Cagle, "Use of Automated License Plate Readers Expanding in Northern California, and Data is Shared With Feds," ACLU Free Future Blog, July 22, 2013, https://www.aclu.org/blog/technology-and-liberty-national-security/use-automated-license-plate-readers-expanding-northern.

[5] Cyrus Favriar, "Rich California Town Considers License Plate Readers For Entire City Limits," *Ars Technica* (Mar. 5, 2013) http://arstechnica.com/ tech-policy/2013/03/rich-california-town-considers-license-plate-readers-for-entire-city-limits/.

[6] Paul Lewis, "CCTV Aimed at Muslim Areas in Birmingham to be Dismantled," *The Guardian* (Oct. 25, 2010) http://www.guardian.co.uk/uk/2010/oct/25/birmingham-cctv-muslim-areas-surveillance.

[7] Adam Goldman & Matt Apuzzo, "With Cameras, Informants, NYPD Eyed Mosques," *Associated Press* (Feb. 23, 2012) http://www.ap.org/Content/AP-In-The-News/2012/Newark-mayor-seeks-probe-of-NYPD-Muslim-spying.

[8] Richard Bilton, "Camera Grid to Log License Plates," *BBC* (May 22, 2009) http://news.bbc.co.uk/2/hi/programmes/whos_watching_you/8064333.stm.

activities but, very troublingly, nowhere specifies the purpose for which such "electronic surveillance" is to be conducted. The use of data collected by ALPR for "homeland security" implies the data will be shared with federal authorities, a practice that may run afoul of state privacy protections. *See White v. Davis*, 13 Cal.3d 757, 775-76 (Cal. 1975) (discussing Article 1, Section 1 of the California Constitution and noting that routine monitoring of innocent persons in order to collect information not relating to illegal activities constitutes a "prima facie violation of the state constitutional right of privacy").

A meaningful planning process, including an articulation of needs and purposes and a privacy impact assessment, should be conducted before Alameda adopts ALPR technology. The purposes guiding ALPR's use should be articulated before the public has decided to adopt the surveillance technology. This decision should follow a multi-step process that includes both internal and public deliberation. We understand the City Council has already approved application for grant funding to acquire an ALPR system. Any grant application would need to specify the intended purpose of this system, and then be binding on the City if the City wishes to uses any funds granted. Before any grant application is submitted, here are some steps that Alameda can take to ensure whether ALPR is necessary and appropriate for the City, and if so, what it should be used for:

- ***Determine the law enforcement purpose(s) that would justify obtaining ALPR.*** Here are a few points to consider:

    - Ask what Alameda's current law enforcement strategy is and what role ALPR would play in that strategy.
    - Ask what ALPR is intended to do—this may include assisting in crime detection, crime prevention, or criminal investigations, or to secure critical infrastructure from possible terrorist threat.
    - To the extent feasible, Alameda should conduct a study or literature review of the effectiveness of ALPR for the stated purpose(s), in part to determine how ALPR might be employed effectively (or how it may not be helpful). Make the results of any research or studies available to the public.
    - Evaluate whether there are alternative means of addressing the stated proposed purpose(s), particularly alternatives that are less intrusive on privacy and civil liberties. Alternatives may include area lighting, community policing, or crime prevention programs to address root causes.
    - Conduct cost-benefit analysis of the privacy issues that weighs multiple factors, including locations, number of cameras, capabilities, type of network, database design, storage/retention, active/passive monitoring, security measures, and alternatives.

- ***Release a privacy impact assessment to the public.*** Prepare a public-facing privacy impact assessment that includes answers to the above questions, the mission of the system, how the system will be authorized, how the cameras will be used, the rules of operation, and the privacy and civil liberties protections in place to prevent misuse or abuse.

- ***Involve the community in the decision making process about whether to adopt ALPR***:

    - The process of considering adoption of ALPR should be public, including notice to the public at large and to community stakeholders. Public hearings, a voter referendum or neighborhood canvassing are all acceptable means that should be considered in seeking the public's approval.
    - The assessment described above should be made available to the public. Make as much as the agency's documentation (e.g., policy, standard operating procedures, cost-benefit analysis) available to the public.
    - Provide an opportunity for meaningful public comment. This presents decisionmakers with the opportunity to assess community support.

If Alameda decides to adopt ALPR, the following should also be considered:

- **Legal authority** – Whether Alameda has the legal authority to employ ALPR for the proposed purposes. For example, the extended surveillance of lawful activity, including associational activities, may violate constitutional rights of privacy and association. *See US v. Jones*, 132 S. Ct. 949, 964 (Alito, J., concurring) (asserting that the "longer term" GPS monitoring will in most instances violate the Fourth Amendment), *id.* at 956 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on" and suggesting that such monitoring violates the First Amendment); *see also White v. Davis*, 13 Cal.3d 757, 767 (Cal. 1975) (noting that even if "police surveillance…may not constitute a direct prohibition of speech or association, such surveillance may still run afoul of the constitutional guarantee if the effect of such activity is to chill constitutionally protected activity.")
- **Number of units** – What is the number of ALPR cameras necessary to accomplish the intended purpose(s)? Any excess surveillance capacity increases the chance of improper activity by operators.
- **Capabilities** – The ALPR system should be equipped with only those features or capabilities reasonably necessary to serve the purpose of the system. Technological features beyond license plate imaging and character recognition may pose significant civil liberties concerns. ALPR can be built to accommodate sophisticated features such as location tracking, magnification, night vision, infrared detection, and such features should be used only where absolutely necessary to accomplish well-articulated purposes. It is essential to clarify whether the system will be designed to accommodate such features and, if so, the addition of such features should only be permitted if expressly authorized by City Council and a privacy impact assessment along the lines of what we propose in this letter is conducted for each such feature.
- **Rollout** – ALPR systems should be limited in geographic scope and used only in areas where it is permissible and for law enforcement officers to look.

- **Reevaluation** – Continue to ask when designing, building, and operating the system, whether it is capable of effectively achieving the purpose(s) for which is was adopted and conversely whether it accomplishes unintended purposes.

3. Alameda must establish a system of supervision over the access to and use of ALPR equipment and data

> **462.2 ADMINISTRATION OF ALPR DATA**
> All installation and maintenance of ALPR equipment, as well as ALPR data retention and access shall be managed by the Bureau of Services Captain. The Bureau of Services Captain will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

Proper administration of ALPR equipment and data is key to preventing the technology's misuse. Before adopting ALPR, Alameda should determine whether resources will be available, long term, to properly operate the system. This should take into account funding, staffing, physical logistics, and maintenance, among other things. If Alameda adopts ALPR, designating a supervisor to oversee the system is an important first step, but it should be coupled with oversight of the persons allowed to access and use the ALPR equipment and data (see Section 6 of this document at pp. 8-11).

4. The lack of discernable limits on the use of ALPR allows for its widespread deployment and raises the possibility it will be used to arbitrarily target areas deemed "suspicious" as a general matter

The draft policy manual contains a section titled "ALPR Operation" that sets forth various parameters for the use of ALPR technology. First, subsections (a) and (b) describe the circumstances under which ALPR may be used:

> (a) An ALPR shall only be used for official and legitimate law enforcement business.
>
> (b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

Subsections (a) and (b) are very permissive and sanction the use of ALPR in a wide array of circumstances. Subsection (a) allows ALPR to be used for any "official and legitimate law enforcement business," including wherever police "patrol" or "investigate," and these broad statements effectively allow police to use ALPR wherever routine police duties are being exercised. In addition, Subsection (b) expressly disclaims the need for a legal justification such as reasonable suspicion or probable cause as a precondition to use. These subsections do not describe who will determine whether these use conditions are met (e.g., a supervising officer, the chief, or any officer). Few uses of ALPR technology by law enforcement will fall outside of what these subsections allow.

Under the draft policy manual, ALPR can be used to monitor and discourage constitutionally protected activities. On its face, subsection (c) encourages the use of ALPR in certain situations:

> (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

Subsection (c) directs officers to pay special attention to "major incidents." This directive is vague and invites operators to abuse their discretion by using ALPR in ways that infringe First and Fourth Amendment rights. ALPR data can easily reveal how citizens worship (e.g., a car parked in a church parking lot), who they associate with (e.g., the same ten cars frequent the same parking lot), and where they go over time. *See, e.g.*, *U.S. v. Jones*, 132 S.Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."). Limits on how ALPR may be used are necessary to respect these and other constitutionally protected activities.

a. The use of specifically targeted lists of plates, or "hot lists," will discourage the arbitrary collection of information about innocent residents

Somewhat unexpectedly, the draft policy manual does not identify as a proposed purpose the most common use of ALPR systems, which involves comparing scanned plates against a "hot list" of stolen vehicles or cars associated with Amber alerts. The use of a "hot list" can ensure the ALPR system is not used to target and record the movements of innocent drivers or employed in the absence of articulable cause.

"Hot lists" require oversight and maintenance to ensure that data is not collected on innocent residents. Hot lists should be updated as often as practicable and, at a minimum, at the beginning of each shift. Whenever ALPR registers a hit, the law enforcement operator should not take other action until that person visually confirms that the plate matches the number and state identified in the alert, confirms that the alert is still active by calling dispatch and, if the alert pertains to the registrant of the car and not the car itself (for example in a warrant situation) develops a reasonable belief that the vehicle's occupant(s) match any individual(s) identified in the alert.

b. Training must be a structured, detailed process that includes all employees that may use or administer ALPR technology or databases

Subsection (d) conditions operation of ALPR equipment or access to ALPR data on receipt of department-approved training:

> (d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

This draft policy manual does not describe what "department-approved training" would consist of. Specifically, subsection (d) fails to specify whether the department or a third party will conduct training. Appropriate training is essential to preventing misuse of ALPR technology and data. Training should be provided to those operating ALPR and those with access to the

system, and it should be provided for all levels of systems operations, from technical personnel to administrator to oversight personnel.

Training should specifically address constitutional issues, case law, state and local legislation, ethical considerations, and departmental policy. This training should occur prior to any officer is assigned to use an ALPR unit or database and be followed by annual refresher training to reinforce the importance of acceptable behavior. Training is key to preventing agency liability, which may arise under privacy or tort law if information is mishandled or misused.

5. The use and retention of collected data should be limited to what is necessary to accomplish the specific purposes of the system, and it must take account of rights to access

The following section discusses the "collection and retention" of ALPR data. The first paragraph sets forth who may use the data:

> All data and images gathered by an ALPR are for the official use of the Alameda Police Department and because such data may contain confidential CLETS information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The provision governing use of ALPR data is overbroad and raises significant civil liberties concerns. First, the above paragraph states that collected data is for "official use." This policy should be more specific about what constitutes a permissible "official use" and should be guided by the purposes articulated during the planning process (discussed above at Sec. 1). Data collected with ALPR should not be used for a purpose other than one stated in this policy manual.

The above paragraph also raises at least two significant civil liberties concerns.

- ***The public's right of access.*** The first sentence of this paragraph limits the public's access to ALPR data, which may contravene the intent and text of both the California Public Records Act, Cal. Gov't Code § 6250 et seq., and the California Constitution, Art. I, § 3, subd. (b)(1). The public's right of access to records is discussed further at Sec. 6(d) on page 10 of this document.

- ***Rights of defendants.*** The second sentence of this paragraph only permits ALPR data to be shared "with prosecutors or others as permitted by law." In some cases, the law will require that data be shared with other parties; for instance, U.S. Supreme Court precedent may require the production of such information to defendants in criminal cases. *See Brady v. Maryland*, 373 U.S. 83 (1963).

a. Retention of ALPR data should be limited to a period necessary to accomplish the system's stated purpose(s)

The second paragraph of the "ALPR Data Collection and Retention" section describes the retention period for ALPR data:

> All ALPR data downloaded to the server should be stored for one year (Government Code § 34090.6), and thereafter may be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

Because ALPR technology can collect significant amounts of data about innocent citizens, the system should be designed to limit the amount of data that is retained. An ALPR system that collects minimal data reduces the likelihood that individual rights will be infringed, reduces maintenance and operating costs, decreases the chance of improper activity by system operators, and limits the costs of long-term data storage. Limiting the retention of data will also reduce the number of public requests for access to data. Data retention and storage can also be very expensive, and having more data on hand means having more useless data on hand as well. Decisions about data retention and disposal should be decided ahead of ALPR deployment.

ALPR data should not be retained in the first place, but if it is, Alameda should select a short retention period. No court has decided whether California law requires a specific retention period for data acquired using ALPR technology, but in no event should it be retained longer than required by California law.[9] The statute cited in the draft policy manual, Govt. Code. § 34096.6, does not on its face apply to ALPR because drivers going about their daily lives are not "regular and ongoing operations of [City of Alameda] departments" falling within the statute's discussion of "routine video monitoring." In fact, California law doesn't even require that ALPR data be retained in the first place—in other words, the fact that Alameda uses ALPR does not mean Alameda is required to retain information related to scanned plates.

The retention of data should be limited to a period necessary to accomplish the system's stated purpose(s). Where data is flagged pursuant to a hot list or a legitimate criminal investigation, a longer retention period commensurate with that reason may be appropriate provided that access and use of the data is limited. Thus, for example, if the purpose of the ALPR system is to compare vehicles against a "hot list" of stolen vehicles or vehicles associated with suspected kidnappings, there is no need to retain data beyond the point at which "hot list" vehicles have been identified and can be apprehended.

6. Alameda's policy manual does not articulate specific constraints how ALPR data may be used

The last section of the draft policy manual, 462.5 -- Accountability and Safeguards, describes access to and use of stored data:

[9] For an example of a reasonable retention period, current California law sets forth a retention period of 60 days for plates captured by the California Highway Patrol's ALPR technology. *See* Cal. Vehicle Code § 2413.

All saved data will be closely safeguarded and protected by both procedural and technological means. The Alameda Police Department will observe the following safeguards regarding access to and use of stored data:

(a) All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Supervisor and processed in accordance with applicable law.

(b) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes.

(e) ALPR system audits should be conducted on a regular basis.

a. Use of collected ALPR data should be explicitly limited to expressly articulated law enforcement purposes

Allowing ALPR data to be used for "legitimate law enforcement purposes" is impermissibly broad. Subsection (c) of the "Accountability and Safeguards" section states that access ALPR data is permitted for "legitimate law enforcement purposes only" and sets forth two examples of such use. The subsections provide no guidance as to the definition of this term and do not describe who will determine whether these use conditions are met (e.g., a supervising officer, the chief, or any officer). Few access cases will fall outside of subsection (c).

Use ALPR data only to investigate hits or for ongoing criminal investigations. To further these purposes, ALPRs should be used by law enforcement agencies only to investigate hits and in other circumstances in which law enforcement agents reasonably believe that the plate data are relevant to an ongoing criminal investigation. Law enforcement must have reasonable suspicion that a crime has occurred before examining collected license plate reader data; they must not examine license plate reader data in order to *generate* reasonable suspicion.

Emergency uses of ALPR data should be limited and subject to oversight. Of course, there may be emergency circumstances where obtaining preauthorization to run a plate is not possible. The circumstances that constitute permissible emergency uses should be made clear to operators in training and written policies, and such uses should be documented and reviewed as soon as practical.

b. Sharing of ALPR data should be strictly limited

Generally speaking, data sharing should be limited to those individuals and agencies with a legitimate interest in an ongoing investigation of a plate that has been recorded using ALPR. Specifically, the articulated purposes justifying the collection of ALPR data in the first place should limit the number of individuals with outside access, the type and quantity of data shared, and the time that those individuals are permitted to retain it.

Written authorization should be required for release of ALPR data. ALPR data should not be released unless written authorization is made through an authorized chain of command, acting in accordance with relevant privacy laws. In no event should license plate reader data be shared

with third parties that do not conform to Alameda's retention and access principles, and the City should be transparent regarding with whom license plate reader data are shared, including any regional databases.

c. Oversight and auditing mechanisms must be built into the draft policy manual

Alameda should provide adequate supervision of access to ALPR technology and databases in order to reduce the risk of misuse or abuse. This oversight will both improve the way the system works and help reduce the potential for liability due to misuse. Specifically, oversight of the ALPR system should involve:

- Permitting access to an ALPR database only to officers trained in the departments' policies governing such databases.
- Establishing a control log that documents the names and hours of personnel working each shift and authorized to access any ALPR database; names, times and purpose of entry into the ALPR center by non-assigned personnel; all requests for footage or images and the purpose of each such request; and details regarding the sharing of any ALPR data. To some extent this may be done in automated fashion by the measures in the next bullet.
- Use of automated operator logon, access control, and other standard audit features to ensure a clear audit trail is maintained. This enables tracking of abusive use of ALPR assets back to the individual who violated a policy.
- Implement appropriate encryption, watermarking, and other chair-of-custody processes to ensure that ALPR footage and images are appropriately handled.
- Conducting periodic audits of the system to ensure that all policies are adhered to. Preferably, professional boards or outside government agencies should conduct independent audits.
- Prohibiting officers from sharing or making copies of data located on an ALPR system without supervisor authorization.
- Providing sanctions against misuse and abuse of ALPR systems, as well as remedies for people who may be harmed by those types of abuse and misuse.
- Creation of technological and administrative safeguards, such as minimization procedures for plates inadvertently collected but not contained within hot lists.
- Defining consequences for misuse or abuses of the system as part of the written policy and ensuring that all users receive training regarding these consequences.

d. Public oversight of Alameda's use of ALPR is essential

First, Alameda should compile annual reports detailing how law enforcement uses ALPR. Annual public reporting of how Alameda uses ALPR would enable members of the public to assess how the system is being used. This report should include statistics and information including but not necessarily limited to:

- Specific geographical areas where ALPR was deployed.
- Number of plate reads per month by all ALPR units.
- Number of unique plates captured per month.

- The geographic locations where stationary ALPR units were deployed.
- Examples of routes travelled by vehicles equipped with ALPR technology.
- Number of 'hits' registered by ALPR units, and instances where hits led to apprehensions or solved crimes.
- Any instances of misuse of ALPR equipment or databases, and any sanctions levied as a result.
- Any sharing of ALPR-related information with third parties, including but not limited to law enforcement entities.

Second, the annual report should be made publicly available. Additionally, allowing members of the public or press to inspect any ALPR equipment at appropriate times can help build community trust in the system. Access to such facilities may be conditioned on the receipt of an adequate and legitimate request.

Finally, citizens should be able to find out if plate data of vehicles registered to them are contained in the Alameda's database, if the information has been retained. They should also be able to access the data. At the same time, access rights should not be used to justify retention of footage. This policy should also apply to disclosure to a third party if the registered vehicle owner consents, for criminal defendants seeking relevant evidence, for civil litigants seeking evidence relevant to a pending claim.

The underlying data should also be available pursuant to Public Records Act (PRA) requests, subject to the deidentification of identifying information such as vehicle license plate numbers. The public has a right to this data because it sheds light on how ALPR technology works, how it is being implemented, and whether policies are being followed. However, identifying information should be redacted to protect privacy interests of drivers; individual license plate numbers, for example, should each be substituted for unique identifiers before such records are produced. This unique ID would protect the privacy of individuals associated with plates in ALPR databases while allowing the public to learn generally about the scope of plates captured by the technology. Where the City can verify that a person is requesting their own plate, the City need not deidentify records describing that person before producing them.

e. Security and data integrity best practices are key to preventing misuse of ALPR data

Finally, the computer systems that communicate and store ALPR data should be secured in a manner that prevents loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of data.

The following steps can help ensure data security and integrity:

- Network security, including the encryption of data in transit and in storage, when possible.

- Safeguard and authenticate the stored camera data using appropriate physical, personnel, and technical security measures. Consider using digital watermarks, encryption, or other security and authentication techniques to secure the data.
- Consider how the system design may be used to authenticate and establish chain-of-custody for data that will potentially be used as evidence.
- Establish a data retention policy (see above at Sect. 5, pp. 7-8) that requires the purging of recorded images that lack evidentiary value or other value for a stated purpose of the system.
- Provide for procedures (a) to identify and secure data that should be retained as evidence or for other stated purposes; (b) to conduct for regularly scheduled review of all retained data; and (c) for the routine destruction/purging of data that does not have to be retained.
- Determine ahead of time how requests for stored data potentially related to third-party civil or criminal legal process will be handled.

7. Conclusion

We welcome Alameda's solicitation of our input as it reviews the appropriate safeguards related to ALPR. In this document, we have raised issues that we believe are essential for the City to consider and flesh out before making final decision on whether to move forward with ALPR. ALPR technology can be used to further important and legitimate law enforcement purposes, but like many technologies, ALPR must be used in a responsible manner because it is capable of invading the privacy and other protected rights of residents. Alameda should consider all of these issues in evaluating both the threshold question of whether ALPR makes sense for the City and if so, how it should be implemented.

As discussed above, this draft policy leaves many important issues unaddressed, including but not limited to specific purposes justifying the use of ALPR, guidance on how ALPR and collected records may be used by law enforcement in a way that protects civil liberties, public oversight of the system, data security and integrity measures, and the substance of both initial and follow-up training. If Alameda begins to use ALPR, we expect to see the policy manual updated with this and other essential detail that it currently lacks.

Sincerely,

Matthew Cagle, esq.
Technology and Civil Liberties Project
American Civil Liberties Union of Northern California

cc: Mayor Marie Gilmore and Vice Mayor Marilyn Ezzy Ashcraft (via email only)
cc: Alameda City Councilmembers Ashcraft, Chen, and Daysog (via email only)
cc: Alameda City Attorney Janet Kern (via email only)
cc: Alameda Assistant City Manager Alex Nguyen (via email only)