

Terry Taplin
Councilmember District 2

SUPPLEMENTAL AGENDA MATERIAL for Supplemental Packet 1

Meeting Date: July 25, 2023

Item Number: 38a

Item Description: Surveillance Ordinance items related to Fixed Automated License Plate Readers (ALPRs)

Submitted by: Councilmember Taplin

This Supplemental summarizes several important revisions made to Policies 422 and 1305, and provides additional background information responsive to community concerns.

Summary of Key Revisions in Item 38a

Revised language in **bolded text**.

- 422.5(h) & 1305.3(h): Department personnel may only access and use the ALPR system for official and legitimate **California law** enforcement purposes consistent with this Policy.
- 422.5(i) & 1305.3(i) Anyone who **intentionally** engages in an impermissible use of the ALPR system or associated scan files or hot lists **shall** be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies. Partial license plates reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.
- **422.5(j) & 1305.3(j): Anyone who negligently engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies. Partial license plates reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.**

- **422.10 OFFICE OF THE DIRECTOR OF POLICE ACCOUNTABILITY.** Any ALPR data or images that are utilized for an investigation that becomes evidence in a case will be made available to the Office of the Director of Police Accountability (ODPA) as it relates to a specific complaint of misconduct. Additionally, the results of any audits will be shared with the ODPA upon their completion.
- **1305.12 AUDITING AND OVERSIGHT.** ALPR system audits will be conducted by the Professional Standards Bureau’s Audit and Inspections Sergeant on a regular basis, at least biannually. The data from the fixed ALPRs shall be reported annually in the Surveillance Technology Report. **Any ALPR data or images that are utilized for an investigation that becomes evidence in a case will be made available to the Office of the Director of Police Accountability (ODPA) as it relates to a specific complaint of misconduct. Additionally, the results of any audits will be shared with the ODPA upon their completion.**

Cost-Effectiveness and Efficacy

As stated in Attachment 6 of item 38a: “BPD is proposing in this item a *two-year trial period* wherein the data can be tracked in the Annual STO report.” [emphasis added]

Several concerns raised about the cost-effectiveness of ALPRs raise empirical questions that have proven difficult for criminologists to quantify in the real world.¹ The complexity is only compounded where public safety interventions are implemented in a holistic framework that addresses accountability, prevention, and “social determinants” of crime. For example, the City of Vallejo found that ALPRs attached to police vehicles enabled a 140% increase in detection of stolen vehicles, while arrests were more efficient with stationary ALPRs in fixed locations.² Recovering stolen vehicles for low-income workers who need their vehicles to reach their places of employment—in and of itself an important policy outcome—may have indirect, long-term positive impacts on public safety that are nevertheless difficult to disaggregate from other variables. While aggregate outcomes would be analyzed *quantitatively*, ALPRs also have *qualitative* impacts on individual investigations and investigatory capacity writ large.³ For example, ALPR technology can contribute to corroboration of suspect alibis, but it would be exceedingly difficult to quantify such benefits, e.g. in terms of “marginal innocent suspects acquitted.”

However, the relationship between solving crimes and deterring them is well-documented, and to the extent that ALPRs increase clearance rates, the impact on public safety outcomes is fairly straightforward. Notably, research including Bun et al. (2020) has found that “increasing the risk of apprehension and conviction exhibits a much larger effect in reducing crime compared to raising the expected severity of

¹ Lum, C., Koper, C. S., Willis, J., Happeny, S., Vovak, H., & Nichols, J. (2018). The rapid diffusion of license plate readers in US law enforcement agencies. *Policing: An International Journal*, 42(3), 376-393.

² Potts, J. (2018). Research in brief: assessing the effectiveness of automatic license plate readers. *POLICE CHIEF*. Retrieved from <http://www.theiacp.org/sites/default/files/2018-08/March%202018%20RIB.pdf>

³ James J. Willis, Christopher Koper & Cynthia Lum (2018). The Adaptation of License-plate Readers for Investigative Purposes: Police Technology and Innovation Re-invention, *Justice Quarterly*, 35:4, 614-638, DOI: 10.1080/07418825.2017.1329936

punishment.”⁴ Ozer (2016) finds that ALPRs can increase apprehensions with the same level of officer resources and “amortises itself within less than one week for property crimes and less than a month for violent crimes,” essentially a cost-savings by enabling gains in labor productivity.⁵

With the Berkeley Police Department’s severe staffing vacancy rate and the City’s significant increase in property crimes, the opportunity cost of *not* increasing investigative capacity over the status quo in the near future is substantial. As of July 2023, BPD reported a staggering 66% *year-over-year increase in auto thefts*. BPD estimates that the loss of vehicles alone has cost Berkeley residents \$1,949,386 this year, which does not include the potential cost of lost wages or other damages. In 2022, Berkeley saw a 48% *increase in catalytic converter thefts over the previous year*. Moreover, it is estimated that a single gun homicide directly costs state taxpayers \$1 million, and costs Californians \$9 million when including externalities imposed on family members, survivors, and the community at large.⁶

While a two-year trial period may be sufficient to demonstrate a positive effect, ALPRs are not an entirely novel, experimental technology, nor do they present a real opportunity cost with respect to other holistic public safety efforts such as Berkeley Ceasefire. Neighboring jurisdictions utilizing ALPRs in the inner East Bay now include: Bay Area Rapid Transit (BART), City of Richmond, City of El Cerrito, City of Oakland, City of Piedmont, City of Emeryville, City of Alameda, City of San Leandro, City of Hayward, City of Newark, City of Fremont. Lacking the tools that neighboring jurisdictions have to solve crimes itself presents a significant opportunity cost. The City of Berkeley has nothing to gain from being alone among its peers in its limited investigative capacity.

Civil Liberties

In response to concerns from the Police Accountability Board regarding reproductive rights, the Public Safety Policy Committee of the City Council recommended the addition of “California” to “legitimate law enforcement purposes” in the ALPR use policies. The revised language now includes “California law” in order to include protections for reproductive rights under state law. Specifically, Assembly Bill 1412 (2022) made revisions to the Penal Code prohibiting California law enforcement authorities from cooperating with investigations, arrest, or surveillance of any person seeking a legal abortion in California. Moreover, the California Department of Justice issued Bulletin # 2022-DLE-13 in October 2022 with best practices for AB-1412 compliance (see Attachment 3).

⁴ Bun, M. J., Kelaher, R., Sarafidis, V., & Weatherburn, D. (2020). Crime, deterrence and punishment revisited. *Empirical economics*, 59, 2303-2333. Retrieved from <https://link.springer.com/article/10.1007/s00181-019-01758-6>

⁵ Ozer, M. (2016). Automatic licence plate reader (ALPR) technology: Is ALPR a smart choice in policing?. *The Police Journal*, 89(2), 117-132. Retrieved from https://www.researchgate.net/profile/M-Ozer/publication/301920403_Automatic_licence_plate_reader_ALPR_technology_Is_ALPR_a_smart_choice_in_policing/links/60a296ab45851502e66b3feb/Automatic-licence-plate-reader-ALPR-technology-Is-ALPR-a-smart-choice-in-policing.pdf

⁶ <https://everytownresearch.org/report/economic-cost-calculator/>

The latest revision also clarifies that “Reasonable suspicion or probable cause is not required before using an ALPR *database*” rather than to ALPRs themselves. This does not change the legal parameters of enforcement, but ensures that ALPRs increase investigative capacity in a meaningful way.

ATTACHMENTS

1. Policy 422
2. Policy 1305
3. California DOB Bulletin # 2022-DLE-13

Fixed Automated License Plate Readers (ALPRs)-

422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology. Department Personnel shall adhere to the requirements of Fixed ALPRs in this policy as well as the corresponding Surveillance Use-Fixed ALPRs policy-1305.

422.2 POLICY

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CBP).

422.3 DEFINITIONS

- (a) Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images to lists of known information of interest.
- (b) ALPR Operator: Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.
- (c) ALPR Administrator: The Investigations Bureau Captain or the Chief's designee, serves as the ALPR Administrator for the Department.
- (d) Hot List: A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, CA DMV, Local BOLO's, etc.
- (e) Vehicles of Interest: Including, but not limited to vehicles which are reported as stolen, display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.

-
- (f) Detection: Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.
 - (g) Hit Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

422.4 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Berkeley 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. It may also be used to gather information related to active warrants, suspect apprehension and stolen property recovery. Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

422.4.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Only properly trained sworn officers, crime analysts, communication operators, records clerks, parking enforcement officers, and police assistants are allowed access to the ALPR system or to collect ALPR information.
- (b) Ensuring that training requirements are completed for authorized users.
- (c) ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.
- (d) Ensuring procedures are followed for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Working with the Custodian of Records, or vendor on the retention and destruction of ALPR data.ensuring this policy and related procedures are conspicuously posted on the City's website.

422.5 OPERATIONS

An ALPR shall only be used for official law enforcement business.

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil

Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used in conjunction with any routine patrol operation or to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR [database](#).
- (c) Partial license plates and unique vehicle descriptions reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.
- (d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- ~~(e)~~ If [practicable/feasible](#), the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert. Once an alert is received, the operator should confirm that the observed license plate from the system matches the license plate of the observed vehicle. Before any law enforcement action is taken because of an ALPR alert, the alert will be verified through a CLETS inquiry via MDT or through Dispatch.
- ~~(e)~~~~(f)~~ Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)
- ~~(f)~~~~(g)~~ Hot Lists. Designation of hot lists to be utilized by the ALPR system shall be made by the ALPR Administrator or his/her designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's LPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's LPR system will not have access to real time data. Occasionally, there may be errors in the LPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:
 - (1) Verification of status on a Hot List. An officer must receive confirmation, from a Berkeley Police Department Communications Dispatcher or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).
 - (2) Visual verification of license plate number. Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number

captured (read) by the LPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Department members alerted to the fact that an observed motor vehicle's license plate is entered as a Hot Plate (hit) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable basis exists before a Department member would have a lawful basis to stop the vehicle.

(3) Department members will clear all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR Hit and the arrest, then the Department member shall update with the Communications Dispatcher and original person and/or a crime analyst inputting the vehicle in the hot list (hit).

(4) General Hot Lists (SVS, SFR, and SLR) will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

(5) All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR Administrator.

(6) Administrator (or his/her designee) before initial entry within the ALPR system. The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the Department member's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles that have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

- Entering Department member's name
- Related case number.
- Short synopsis describing the nature of the originating call

~~(g)~~(h) Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited.

Permitted/Impermissible Uses. The ALPR system, and all data collected, is the property of the Berkeley Police Department. Department personnel may only access and use the ALPR system for official and legitimate [California](#) law enforcement purposes consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

1. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

-
2. Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
 3. Use Based on a Protected Characteristic. It is a violation of this policy to use the LPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
 4. Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
 5. First Amendment Rights. It is a violation of this policy to use the LPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

(i) Anyone who intentionally engages in an impermissible use of the ALPR system or associated scan files or hot lists ~~may~~ shall be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies. Partial license plates reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.

(j) Anyone who negligently engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies. Partial license plates reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

422.6 DATA COLLECTION AND RETENTION

The Investigations Division Captain is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures. ~~The Department should if feasible find a solution to transfer evidentiary hit data into its digital evidence repository through secure integration. Evidentiary hit data shall be transferred into the Department's digital evidence repository through secure integration.~~

All ALPR data downloaded to the ALPR server should be stored for no longer than 30 days, and in accordance with the established records retention schedule. Thereafter, ALPR data should 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 discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server and uploaded into BPD's digital evidence repository.

ALPR vendor, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. The ALPR vendor will purge their data at the end of the 30 days of storage. However, this will not preclude Berkeley Police Department from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established City of Berkeley retention schedule mentioned above or outlined elsewhere. Relevant vehicle data are scans corresponding to the vehicle of interest on a hot list. The ALPR vendor and Department shall ensure that the necessary data is captured and stored to accurately report the relevant data required in the Annual Surveillance Technology report. Once the City Council approves the Annual Surveillance Technology report all said data may be purged so long as it doesn't violate the Retention guidelines.

Restrictions on use of vendor Data: Information gathered or collected, and records retained by the vendor's cameras or any other Berkeley Police Department ALPR system will not be sold, accessed, or used for any purpose other than legitimate [California](#) law enforcement or public safety purposes.

422.7 ACCOUNTABILITY

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (c) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate [California](#) law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.
- (d) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the consent of the Chief of Police or City Manager (i.e. If transportation department requested volume of vehicular traffic associated with specific events, it could conceivably be provided with the count of vehicles, but not the specific license plates with appropriate permissions).
- (e) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (f) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biennial.

-
- (g) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate [California](#) law enforcement purposes.
 - (h) Every ALPR Detection Browsing Inquiry must be documented by either the associated Berkeley Police case number or incident number, and/or a reason for the inquiry

For security or data breaches, see the Records Release and Maintenance Policy.

422.8 ALPR DATA DETECTION BROWSING AUDITS

It is the responsibility of the Sergeant of Audit and Inspections or the Chief's designee to ensure that an audit is conducted of ALPR detection browsing inquiries at least biennial. The Department will audit a sampling of the ALPR system utilization from the prior 24-month period to verify proper use in accordance with the above- authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the preceding 24-month period and determine if each inquiry meets the requirements established in policy section 462.6(e).

The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be filed and retained by the Professional Standards Bureau Captain. This audit should be shared in the Surveillance Ordinance reporting.

422.9 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

(a) A supervisor at the requesting agency will sign an acknowledgement letter stating that the shared data will only be used for the purposes that are aligned with the Berkeley Police Department's policy. The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement, these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CBP). *See attached letter.*

(b) The signed letter is retained on file. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

(c) All signed letters shall be routed to the Audit and Inspection Sergeant for compliance and reporting.

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

422.10 OFFICE OF THE DIRECTOR OF POLICE ACCOUNTABILITY

Any ALPR data or images that are utilized for an investigation that becomes evidence in a case will be made available to the Office of the Director of Police Accountability (ODPA) as it relates to

[a specific complaint of misconduct. Additionally, the results of any audits will be shared with the ODPa upon their completion.](#)

422.10422.11 TRAINING

The Personnel and Training Sergeant shall ensure that members receive department-approved training -in order to be -authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code § 1798.90.53

Surveillance Use Policy-Fixed ALPRs

1305.1 PURPOSE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology. Department Personnel shall adhere to the requirements of the Surveillance Use-Fixed ALPRs in this policy as well as the corresponding Use Policy -422.

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CBP).

1305.2 DEFINITIONS

- (a) Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images to lists of known information of interest.
- (b) ALPR Operator: Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.
- (c) ALPR Administrator: The Investigations Bureau Captain or the Chief's designee, serves as the ALPR Administrator for the Department.
- (d) Hot List: A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, CA DMV, Local BOLO's, etc.
- (e) Vehicles of Interest: Including, but not limited to vehicles which are reported as stolen, display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.
- (f) Detection: Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

- (g) Hit Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

1305.3 AUTHORIZED AND PROHIBITED USES

An ALPR shall only be used for official law enforcement business.

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used in conjunction with any routine patrol operation or to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR [database](#).
- (c) Partial license plates and unique vehicle descriptions reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.
- (d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

[\(e\)](#) If ~~practicable~~[feasible](#), the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert. Once an alert is received, the operator should confirm that the observed license plate from the system matches the license plate of the observed vehicle. Before any law enforcement action is taken because of an ALPR alert, the alert will be verified through a CLETS inquiry via MDT or through Dispatch.

~~(e)~~[\(f\)](#) Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)

~~(f)~~[\(g\)](#) Hot Lists. Designation of hot lists to be utilized by the ALPR system shall be made by the ALPR Administrator or his/her designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's LPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's LPR system will not have access to real time data. Occasionally, there may be errors in the LPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

(1) Verification of status on a Hot List. An officer must receive confirmation, from a Berkeley Police Department Communications Dispatcher or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).

(2) Visual verification of license plate number. Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the LPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Department members alerted to the fact that an observed motor vehicle's license plate is entered as a Hot Plate (hit) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable basis exists before a Department member would have a lawful basis to stop the vehicle.

(3) Department members will clear all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR Hit and the arrest, then the Department member shall update with the Communications Dispatcher and original person and/or a crime analyst inputting the vehicle in the hot list (hit).

(4) General Hot Lists (SVS, SFR, and SLR) will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

(5) All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR Administrator.

(6) Administrator (or his/her designee) before initial entry within the ALPR system. The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the Department member's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles that have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

- Entering Department member's name
- Related case number.
- Short synopsis describing the nature of the originating call

~~(g)~~(h) Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited.

Permitted/Impermissible Uses. The ALPR system, and all data collected, is the property of the Berkeley Police Department. Department personnel may only access and use the ALPR system for official and legitimate [California](#) law enforcement purposes consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

1. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible

from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

2. Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
3. Use Based on a Protected Characteristic. It is a violation of this policy to use the LPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
4. Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
5. First Amendment Rights. It is a violation of this policy to use the LPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

(i) Anyone who intentionally engages in an impermissible use of the ALPR system or associated scan files or hot lists ~~may~~ shall be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies. Partial license plates reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.

(j) Anyone who negligently engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies. Partial license plates reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

1305.4 DATA COLLECTION

The Investigations Division Captain is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures. ~~The Department should if feasible find a solution to transfer evidentiary hit data into its digital evidence repository through secure integration. Evidentiary hit data shall be transferred into the Department's digital evidence repository through secure integration.~~ Evidentiary hit data shall be transferred into the Department's digital evidence repository through secure integration.

All ALPR data downloaded to the ALPR server should be stored for no longer than 30 days, and in accordance with the established records retention schedule. Thereafter, ALPR data should 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 discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server and uploaded into BPD's digital evidence repository.

ALPR vendor, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. The ALPR vendor will purge their data at the end of the 30

days of storage. However, this will not preclude Berkeley Police Department from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established City of Berkeley retention schedule mentioned above or outlined elsewhere. Relevant vehicle data are scans corresponding to the vehicle of interest on a hot list. The ALPR vendor and Department shall ensure that the necessary data is captured and stored to accurately report the relevant data required in the Annual Surveillance Technology report. Once the City Council approves the Annual Surveillance Technology report all said data may be purged so long as it doesn't violate the Retention guidelines.

Restrictions on use of vendor Data: Information gathered or collected, and records retained by the vendor's cameras or any other Berkeley Police Department ALPR system will not be sold, accessed, or used for any purpose other than legitimate [California](#) law enforcement or public safety purposes.

1305.5 DATA ACCESS

- (a) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (b) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- (c) If practical, an operator should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

1305.6 DATA PROTECTION

Surveillance Use Policy-Fixed ALPRs

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (c) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate [California](#) law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.
- (d) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the consent of the Chief of Police or City Manager (i.e. If transportation department requested volume of vehicular traffic associated with specific events, it could conceivably be provided with the count of vehicles, but not the specific license plates with appropriate permissions).
- (e) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (f) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biennial.
- (g) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate [California](#) law enforcement purposes.
- (h) Every ALPR Detection Browsing Inquiry must be documented by either the associated Berkeley Police case number or incident number, and/or a reason for the inquiry

For security or data breaches, see the Records Release and Maintenance Policy.

1305.7 CIVIL LIBERTIES AND RIGHTS PROTECTION

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third-Party Data Sharing) protect against the unauthorized use of ALPR data. These policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

Surveillance Use Policy-Fixed ALPRs

1305.8 DATA RETENTION

All ALPR data belongs to the Department. All ALPR data downloaded to the ALPR server should be stored for no longer than 30 days, and in accordance with the established records retention schedule. Thereafter, ALPR data should 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 discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server and uploaded into BPD's digital evidence repository.

ALPR vendor, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. The ALPR vendor will purge their data at the end of the 30 days of storage. However, this will not preclude Berkeley Police Department from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established City of Berkeley retention schedule mentioned above or outlined elsewhere. Relevant vehicle data are scans corresponding to the vehicle of interest on a hot list. The ALPR vendor and Department shall ensure that the necessary data is captured and stored to accurately report the relevant data required in the Annual Surveillance Technology report. Once the City Council approves the Annual Surveillance Technology report all said data may be purged so long as it doesn't violate the Retention guidelines.

1305.9 PUBLIC ACCESS

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

The Department shall to the extent feasible aim to offer a transparency portal wherein the number of scans, hits, and queries is available to the public in real-time, or as near as real-time as feasible. All data shall be reported in the Annual Surveillance Technology Report.

1305.10 THIRD PARTY DATA-SHARING

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

(a) A supervisor at the requesting agency will sign an acknowledgement letter stating that the shared data will only be used for the purposes that are aligned with the Berkeley Police Department's policy. The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement, these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CBP). *See attached letter.*

(b) The signed letter is retained on file. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

(c) All signed letters shall be routed to the Audit and Inspection Sergeant for compliance and reporting.

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

1305.11 TRAINING

Training for the operation of ALPR Technology shall be provided by BPD personnel. All BPD

Surveillance Use Policy-Fixed ALPRs

employees who utilize ALPR Technology shall be provided a copy of this Surveillance Use Policy.


1305.12 AUDITING AND OVERSIGHT

ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually. The data from the fixed ALPRs shall be reported annually in the Surveillance Technology Report.

[Any ALPR data or images that are utilized for an investigation that becomes evidence in a case will be made available to the Office of the Director of Police Accountability \(ODPA\) as it relates to a specific complaint of misconduct. Additionally, the results of any audits will be shared with the ODPA upon their completion.](#)

1305.13 MAINTENANCE

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain or his or her designee. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data. Equipment maintenance shall be provided by the vendor.

<p>California Department of Justice DIVISION OF LAW ENFORCEMENT John D. Marsh, Chief</p> 	<h1>INFORMATION BULLETIN</h1>	
<p>Subject: Recent Penal Code Amendments Prohibiting Law Enforcement from Cooperating with Other States' Investigations of Abortions that are Legal in California</p>	<p>No. 2022-DLE-13</p>	<p>Contact for information: John D. Marsh, Chief Division of Law Enforcement (916) 210-6300</p>
	<p>Date: October 20, 2022</p>	

TO: All CALIFORNIA DISTRICT ATTORNEYS, CHIEFS OF POLICE, SHERIFFS, AND STATE LAW ENFORCEMENT AGENCIES

California has recognized and supported reproductive freedom and access to safe, legal abortion for over half a century. Recently, the Governor signed Assembly Bill (AB) 1242 into law effective September 27, 2022. AB 1242 made several changes to the Penal Code as part of California's commitment to protecting individuals who provide, obtain, or assist others in obtaining abortions that are legal under California law.

This bulletin provides information to help law enforcement ensure their practices are consistent with the changes to the Penal Code. Specifically, this bulletin provides guidance about Penal Code sections 629.51, 629.52, 638.50, 638.52, 1269b, 1551, 1524, 1524.2, and 13778.2.

Context for the Changes to the California Penal Code

After the U.S. Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* (2021) holding there is no federal constitutional right to abortion, some states have outlawed abortion in some or all circumstances, and authorized civil suits and criminal prosecutions of those who perform, seek, obtain, or assist others in seeking or obtaining abortions.

Law enforcement in states where abortion is illegal may try to enlist California law enforcement to arrest, extradite, or obtain or share information about individuals for abortion-related activities that are legal here. Examples of such activities may include: procuring, providing, or obtaining a prescription for mifepristone or misoprostol (pills used for, among other things, medication abortion) and the taking of such medication; the use of the internet or web or phone-based apps to procure, provide, or obtain such medication or a surgical abortion; and providing or obtaining in-clinic or surgical abortion without medical or other justification (as defined by the demanding state).

The laws discussed below make it illegal for California law enforcement to assist in out-of-state investigation and enforcement efforts related to providing, facilitating, or obtaining an abortion that is lawful under California law, or intending or attempting to do the same. It is possible, however, that out-of-state law enforcement seeking California's assistance may not disclose to California law enforcement that their request is about abortion-related activity by characterizing it as, for example, child endangerment, child abuse, drug abuse, concealing a death, or murder.

For that reason, California law enforcement should carefully examine requests from law enforcement in states where abortion is illegal to ensure they are not assisting with the investigation or prosecution of abortion-related activity that is legal in California, in addition to complying with the other changes to California's Penal Code.

As of the date of this publication, states that have implemented abortion bans following the *Dobbs* decision include: Alabama, Arizona, Arkansas, Florida, Georgia, Idaho, Indiana*, Kentucky, Louisiana, Mississippi, Missouri, North Carolina, North Dakota*, Ohio*, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, West Virginia, Wisconsin, and Wyoming*.

The Changes to the California Penal Code

The following changes have been made to the Penal Code:

- Arrests and Information Sharing
 - State and local law enforcement agencies and officers are prohibited from arresting or participating in the arrest of someone for performing, obtaining, or helping someone obtain a legal abortion in California. (Pen. Code, § 13778.2, subd. (a).)
 - State and local public agencies and their employees are prohibited from cooperating with or providing information to any individual, agency, or department from another state about a legal abortion in California. Sharing such information with federal law enforcement agencies is also not permitted, unless required by federal law. (Pen. Code, § 13778.2, subd. (b).)
- Wires, Electronic Communications, Pen Registers, Trap and Trace Devices, and Warrants
 - No court may issue ex parte orders authorizing (i) interception of wire or electronic communications, or (ii) the installation and use of pen registers or trap and trace devices, and no search warrants may be issued, for the purpose of investigating or recovering evidence of a "prohibited violation." (Pen. Code, §§ 629.52, subd. (e), 638.52, subd. (m), 1524, subd. (h).)
 - "Prohibited violation" is defined as any violation of law that creates liability for, or arising out of, either of the following:
 - (i) Providing, facilitating, or obtaining an abortion that is lawful under California law.
 - (ii) Intending or attempting to provide, facilitate, or obtain an abortion that is lawful under California law.
 - "Facilitating" means assisting, directly or indirectly in any way, with the obtaining of an abortion that is lawful under California law.
 - (Pen. Code, §§ 629.51, subds. (5)(A)-(B)), 638.50, subd. (d).)

* Indicates that the ban has been temporarily blocked by court order.

- In order to obtain a search warrant for electronic communications under section 1524.2, out-of-state law enforcement must provide an attestation stating that the evidence being sought does not relate to an investigation or prosecution of a “prohibited violation.”
- Bail Schedule
 - The countywide bail schedule will set bail at zero dollars (\$0) for any individual who has been arrested in connection with a proceeding in another state regarding an individual performing, supporting, or aiding in the performance of a legal abortion in California, or an individual obtaining a legal abortion in California. (Pen. Code, § 1269b, subd. (f)(2).)
- Extradition of Fugitives
 - When an agency files a verified complaint under Penal Code Section 1551 regarding the extradition of an individual taken into custody on the basis of an out-of-state warrant, the filing agency must, within 24 hours, electronically transmit to the Attorney General's office a complete copy of the verified complaint, the out-of-state indictment, information, complaint or judgment, out-of-state warrant, and the affidavit upon which the out-of-state warrant was issued. (Pen. Code, § 1551, subd. (b).) These materials should be sent to Extradition@doj.ca.gov.
 - For additional information regarding extradition, please see Information Bulletin 2022-DLE-10, Non-Extradition of Individuals Providing Care to Out-of-State Patients in California, or Other Persons in California who Assist Out-of-State Patients in Seeking Abortion Care in California, <https://oag.ca.gov/system/files/media/2022-DLE-10.pdf>.

Best Practices

Below is a summary of best practices for compliance with these new laws.

Law Enforcement Training

All staff should receive training on the recent changes to the Penal Code. This training should include the following points:

- (1) California Law enforcement agencies should be careful, when sharing any information or otherwise cooperating with law enforcement from other states or federal agencies, to prevent information sharing about legal abortions in California.
- (2) Law enforcement agencies should closely examine any out-of-state arrest warrant prior to taking any person into custody or accepting bail based on an out-of-state warrant. Law enforcement is prohibited from cooperating where the arrest relates to an abortion that is legal in California, but the warrant may not clearly state that the offense is related to abortion.
- (3) Law enforcement agencies should be aware that there is no obligation that they make an arrest based on an out-of-state warrant.
- (4) Law enforcement should be careful when applying for authorization from a magistrate to intercept electronic communications or wires, to install trap and trace devices, or for warrants on behalf of other states to ensure the other states are not seeking information relating to abortions that are legal under California law.
- (5) Law enforcement agencies should immediately contact the California Attorney General's Office if they have any questions regarding an out-of-state warrant.

District Attorney-Specific Training

Reproductive rights crimes may not be clearly identified as such. Prosecutors should carefully review any out-of-state information requests before responding. Likewise, prosecutors should closely review out-of-state warrants and any supporting documents provided by the out-of-state agency, in consultation with the Attorney General's Office, before filing a complaint pursuant to Penal Code § 1551. Information about the underlying crime(s) may be found in the indictment, information, complaint, or affidavit and the out-of-state warrant provided by the demanding agency. Prosecutors should not rely solely on the statutes contained in the above documents, but should carefully review the underlying facts to ensure that activity associated with reproductive healthcare services is not improperly described as criminal conduct, including child neglect, child abuse, drug use, or murder. If the underlying facts cannot be readily determined from the documents provided by the demanding agency, additional documentation should be requested before filing a complaint pursuant to Penal Code § 1551.

Contact Information

The California Department of Justice is available to assist local law enforcement agencies in complying with the above-described amendments to the Penal Code. Should your agency or individual officers require technical assistance, please contact Division of Law Enforcement Chief John Marsh at (916) 210-6300 or (916) 210-7690, or Senior Assistant Attorney General Renuka George in the Department's Healthcare Rights and Access Section at Renuka.George@doj.ca.gov or (916) 714-3563.