

Page numbers for this agenda packet are marked in **GREEN** to distinguish them from the numbering within individual documents.

PUBLIC MEETING MATERIAL



**POLICE ACCOUNTABILITY BOARD
REGULAR MEETING AGENDA PACKET
October 7, 2026
6:30 PM**

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Joshua Buswell-Charkow	Stephanie Allan
Patrick DeTemple	Jasmina Viteskic
Anay Sharma	Dwayne Phillips (Alternate)

MEETING LOCATION

Office of the Director of Police Accountability
1900 Addison Street, Floor 3
Berkeley, CA 94704

Agenda Item Materials

Item	Description	Page
2	October 7, 2026 PAB Regular Meeting Agenda	1
4	Minutes for the Regular Meeting of September 23, 2026	7
8	Subcommittee List	13
9.b.i.	September 30, 2026 Memorandum from Board Member Allan to the PAB Titled "Recommendation that the City Council Hire an Independent Auditor Dedicated Exclusively to Monitoring and Auditing BPD's Use of Surveillance Technology"	16
9.b.ii.	Materials Presented at the September 23, 2026 PAB Regular Meeting re: Flock Automated License Plate Reader Audit	20

Off Agenda Reports

Item	Description	Page
1	Policy Review Status Updates	78
2	Legislative Updates Relevant to the PAB's Work	91
3	List of Remaining 2026 PAB Meetings	96

ITEM 2

October 7, 2026 PAB Regular Meeting Agenda



**POLICE ACCOUNTABILITY BOARD
REGULAR MEETING AGENDA
WEDNESDAY, OCTOBER 7, 2026
6:30 P.M.**

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Joshua Buswell-Charkow	Stephanie Allan
Patrick DeTemple	Jasmina Viteskic
Anay Sharma	Dwayne Phillips (Alternate)

MEETING LOCATION

Office of the Director of Police Accountability
1900 Addison Street, Floor 3
Berkeley, CA 94704

PUBLIC NOTICE

To access the meeting remotely: join from a PC, Mac, iPad, iPhone, or Android device using this URL: <https://us02web.zoom.us/j/89007838093>. If you do not wish for your name to appear on the screen, use the drop-down menu and click on “rename” to rename yourself to be anonymous. To request to speak, use the “raise hand” icon on the screen. To join by phone: Dial **1 669 900 6833** and enter Meeting ID **890 0783 8093**. If you wish to comment during the public comment portion of the agenda, press *9 and wait to be recognized.

LAND ACKNOWLEDGMENT

The City of Berkeley recognizes that the community we live in was built on the territory of xučyun (Huchiun (Hooch-yoon)), the ancestral and unceded land of the Chochenyo (Chochen-yo)-speaking Ohlone (Oh-low-nee) people, the ancestors and descendants of the sovereign Verona Band of Alameda County. This land was and continues to be of great importance to all of the Ohlone Tribes and descendants of the Verona Band. As we begin our meeting tonight, we acknowledge and honor the original inhabitants of Berkeley, the documented 5,000-year history of a vibrant community at the West Berkeley Shellmound, and the Ohlone people who continue to reside in the East Bay. We recognize that Berkeley's residents have and continue to benefit from the use and occupation of this uncaded stolen land since the City of Berkeley's incorporation in 1878. As stewards of the laws regulating the City of Berkeley, it is not only vital that we recognize the history of this land, but also recognize that the Ohlone people are present members of Berkeley and other East Bay communities today.

AGENDA**1. CALL TO ORDER AND ROLL CALL (2 MINUTES)****2. APPROVAL OF AGENDA (2 MINUTES)****3. PUBLIC COMMENT (TBD)**

Speakers are generally allotted up to three minutes but may be allotted less time if there are many speakers; they may comment on any matter within the Board's jurisdiction at this time, except confidential personnel matters.

4. APPROVAL OF MINUTES (5 MINUTES)

- a. Minutes for the Regular Meeting of September 23, 2026.

5. ODPa STAFF REPORT (10 MINUTES)

Announcements, updates, and other items.

6. CHAIR AND BOARD MEMBERS' REPORTS (10 MINUTES)

The Chair and Board Members report on their activities.

7. CHIEF OF POLICE'S REPORT (10 MINUTES)

Crime/cases of interest, community engagement/departments events, staffing, training, and other items of interest.

8. SUBCOMMITTEE REPORTS (10 MINUTES)

Report of activities and meeting schedule for all subcommittees, possible appointment or reassignment of members to subcommittees, and additional discussion and action as warranted for the subcommittees listed on the PAB's Subcommittee List included in the agenda packet.

9. DISCUSSION AND ACTION ITEMS (ESTIMATED TIME: 55 MINUTES)

The PAB will discuss and may act on the following items, including providing feedback, recommendations, or other directions, as appropriate.

- a. Action on Commendation of Interim Director Kathy Lee for Public Service to Berkeley (Cayetano) (5 Minutes)
- b. Berkeley Police Department's Flock Automated License Plate Reader Audits for January 2026 – June 2026 (Continued from September 23, 2026) – (20 Minutes)
 - i. Discussion and Action on Independent Auditor of Surveillance Technology Proposal (Allan)
 - ii. Discussion and Action on BPD ALPR Audit Report for January 2026 (Cayetano)
- c. Update on the Status of BPD Policy 300 "Use of Force" (Continued from September 23, 2026) (Cayetano) – (10 Minutes)
- d. Update on Evaluation of Responses to Request for Proposals for Public Safety Technology (Wilson) – (10 Minutes)
- e. Recommendations for Issuing PAB Commendations to Berkeley Police Department Officers Based on Commendations Received Between April and July 2026 (Buswell-Charkow) – (10 Minutes)

10. PUBLIC COMMENT (TBD)

Speakers are generally allotted up to three minutes but may be allotted less time if there are many speakers; they may comment on any matter within the Board's jurisdiction at this time, except confidential personnel matters.

11. CLOSED SESSION

CLOSED SESSION ITEMS

Pursuant to the Court's order in *Berkeley Police Association v. City of Berkeley, et al.*, Alameda County Superior Court Case No. 2002-057569, the Board will recess into closed session to discuss and act on the following matter(s):

- a. Conference With Labor Negotiators; Government Code § 54957.6
Designated representatives: Leah Wilson, Designated PAB Representative;
Katherine Lee, Interim Director of Police Accountability
Employee organization: Berkeley Police Association
- b. Case Updates and Recommendations Regarding Complaints Received by the ODPa:

i. 2023-CI-0016	xviii. 2026-CI-0019
ii. 2024-CI-0004	xix. 2026-CI-0020
iii. 2025-CI-0018	xx. 2026-CI-0021
iv. 2025-CI-0030	xxi. 2026-CI-0022
v. 2025-CI-0037	xxii. 2026-CI-0023
vi. 2026-CI-0001	xxiii. 2026-CI-0024

vii.	2026-CI-0002	xxiv.	2026-CI-0025
viii.	2026-CI-0005	xxv.	2026-CI-0026
ix.	2026-CI-0007	xxvi.	2026-CI-0027
x.	2026-CI-0008	xxvii.	2026-CI-0028
xi.	2026-CI-0009	xxviii.	2026-CI-0029
xii.	2026-CI-0010	xxix.	2026-CI-0030
xiii.	2026-CI-0011	xxx.	2026-CI-0031
xiv.	2026-CI-0012	xxxi.	2026-CI-0032
xv.	2026-CI-0015	xxxii.	2026-CI-0033
xvi.	2026-CI-0016	xxxiii.	2026-CI-0034
xvii.	2026-CI-0018		

END OF CLOSED SESSION**12.ANNOUNCEMENT OF CLOSED SESSION ACTIONS (1 MINUTE)****13.ADJOURNMENT (1 MINUTE)****Off Agenda Reports**

1. Policy, Practice, and Procedure Review Status Report
2. Legislative Updates Relevant to the PAB's Work
3. 2026 PAB Meeting Calendar

Communications Disclaimer

Communications to the Police Accountability Board, like all communications to Berkeley boards, commissions, or committees, are public records and will become part of the City's electronic records, which are accessible through the City's website. Please note: e-mail addresses, names, addresses, and other contact information are not required, but if included in any communication to a City board, commission, or committee, will become part of the public record. If you do not want your e-mail address or any other contact information to be made public, you may deliver communications via U.S. Postal Service or in person to the Board Secretary. If you do not want your contact information included in the public record, do not include that information in your communication. Please contact the Board Secretary for further information.

**Communication Access Information (A.R. 1.12)**

To request a disability-related accommodation(s) to participate in the meeting, including auxiliary aids or services, please contact the Disability Services specialist at 981-6418 (V) or 981-6347 (TDD) at least three business days before the meeting date.

SB 343 Disclaimer

Any writings or documents provided to a majority of the Board regarding any item on this agenda will be made available for public inspection at the Office of the Director of Police Accountability, located at 1900 Addison Street, Floor 3, Berkeley, CA 94704

Contact the Director of Police Accountability (Board Secretary) at:

1900 Addison Street, Floor 3, Berkeley, CA 94704

TEL: 510-981-4950 TDD: 510-981-6903 FAX: 510-981-4955

Website: <https://berkeleyca.gov/dpa>

Email: dpa@berkeleyca.gov

ITEM 4

Minutes for the Regular Meeting of September 23, 2026



**POLICE ACCOUNTABILITY BOARD
REGULAR MEETING MINUTES
WEDNESDAY, SEPTEMBER 23, 2026
6:30 P.M.**

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Joshua Buswell-Charkow	Stephanie Allan
Patrick DeTemple	Jasmina Viteskic
Anay Sharma	Dwayne Phillips (Alternate)

MEETING LOCATION

Office of the Director of Police Accountability
1900 Addison Street, Floor 3
Berkeley, CA 94704

MEETING MINUTES

1. CALL TO ORDER AND ROLL CALL AT 6:35 PM

Present:	Board Member Leah Wilson (Vice Chair)
	Board Member Stephanie Allan
	Board Member Patrick DeTemple
	Board Member Joshua Buswell-Charkow
	Board Member Anay Sharma
	Board Member Jasmina Viteskic
Absent:	Board Member Joshua Cayetano (Chair) ¹
ODPA Staff:	Kathy Lee, Interim Director of Police Accountability
	Jose Murillo, Policy Analyst
	Syed Mehdi, Data Analyst
	Daniel Weinberg, Investigator
BPD Staff:	Deputy Chief Jen Tate
	Lt. Jesse Grant

¹ Board Member Cayetano (Chair) was granted a leave of absence for the September 23, 2026 PAB Meeting.

2. APPROVAL OF AGENDA

Motion to approve the agenda.

Moved/Second (Buswell-Charkow/Viteskic) Motion carried.

Ayes: Viteskic, Wilson, Allan, Buswell-Charkow, DeTemple and Sharma.

Noes: None. Abstain: None. Absent: Cayetano.

3. PUBLIC COMMENT

4 Physically Present Speakers

2 Virtually Present Speakers

4. APPROVAL OF MINUTES

- a. Minutes for the Regular Meeting of September 9, 2026.

Motion to approve the minutes for the Regular Meeting of September 9, 2026.

Moved/Second (Buswell-Charkow/DeTemple) Motion carried.

Ayes: Viteskic, Wilson, Allan, Buswell-Charkow, DeTemple and Sharma.

Noes: None. Abstain: None. Absent: Cayetano.

5. ODPA STAFF REPORT

Interim Director Lee reported that the permanent Director's appointment was scheduled for City Council consideration on September 29, with a planned October 5 start date. A two-week overlap had been approved, and her final day as Interim Director was scheduled for October 16. ODPA staff met with Berkeley Law Police Review Project students about potential assistance to complainants and research support. Interim Director Lee also provided an update on vendor demonstrations, proposal evaluation, and reference checks for the public safety technology RFP.

6. CHAIR AND BOARD MEMBERS' REPORTS

The Vice Chair and Board Members reported on their activities since the last PAB meeting on September 9, 2026.

7. CHIEF OF POLICE'S REPORT

Deputy Chief Tate reported on recent vehicle burglaries and an assault investigated as a hate crime, community events, and staffing. BPD has 151 of 164 authorized officer positions filled, nine recruits in the academy, and 18 of 25 dispatcher positions filled. She acknowledged Secure Justice's letter concerning the ALPR audit and said BPD would review it. She also discussed the mutual aid air support item scheduled for City Council on September 29 and requested clarification of the Board's proposed policy language.

8. SUBCOMMITTEE REPORTS

Subcommittee chairs provided updates on ongoing policy review work, legislative matters, and other committee activities.

9. DISCUSSION AND ACTION ITEMS

- a. Status of Responses to Request for Proposals for Public Safety Technology (Wilson)

The Board discussed data access, security, and independent auditing of the proposed technologies. Board Member Sharma was asked to summarize his research on independent audit providers and potential costs in a memo to inform a possible Board recommendation. No formal action was taken.

- b. Amendment to BMC Chapter 2.99 to Establish Surveillance Technology Accountability Requirements and to Revise the Annual Surveillance Technology Reporting Schedule (ODPA)

Interim Director Lee summarized the proposed surveillance technology ordinance amendments. The Board discussed whether further revisions may be needed after the technology vendors are selected. No action was taken.

- c. Berkeley Police Department Flock Automated License Plate Reader Audits – January 2026 – June 2026 (Cayetano)

Motion to continue Item 9c to the October 7, 2026 Board meeting

Moved/Second (DeTemple/Sharma) Motion carried.

Ayes: Viteskic, Wilson, Buswell-Charkow, DeTemple and Sharma.

Noes: None. Abstain: Allan. Absent: Cayetano.

- d. Updated Policy Review Proposal for 2025-PR-0004 (ODPA)

Motion to approve staff's proposal to continue with the policy review for 2025-PR-0004.

Moved/Second (DeTemple/Viteskic) Motion carried.

Ayes: Viteskic, Wilson, Allan, Buswell-Charkow, DeTemple and Sharma.

Noes: None. Abstain: None. Absent: Cayetano.

- e. BPD Policy 300 "Use of Force" (Cayetano)

Chair Cayetano was absent, so the Board did not discuss the item. No action was taken.

10. PUBLIC COMMENT

2 Physically Present Speakers

1 Virtually Present Speaker

11. CLOSED SESSION

CLOSED SESSION ITEMS

Pursuant to the Court's order in *Berkeley Police Association v. City of Berkeley, et al.*, Alameda County Superior Court Case No. 2002-057569, the Board will recess into closed session to discuss and act on the following matter(s):

- a. Conference With Labor Negotiators; Government Code § 54957.6 Designated representatives: Leah Wilson, Designated PAB Representative; Katherine Lee, Interim Director of Police Accountability Employee organization: Berkeley Police Association

The Board considered matters related to the ongoing meet-and-confer process concerning permanent regulations and provided updates regarding the ongoing meet-and-confer process.

- b. Case Updates and Recommendations Regarding Complaints Received by the ODPa:

2025-CI-0018

Motion to accept staff's recommendations for Allegations 1, 2, 4, 5, 6, and 7, excluding Allegation 3, and to add a section describing the procedural history, including tolling issues, ODPa's efforts to fully and fairly investigate the complaint, and the Board's direction.

Moved/Second (Wilson/Viteskic) Motion carried.

Ayes: Viteskic, Wilson, Allan, DeTemple, Buswell-Charkow and Sharma.

Noes: None. Abstain: None. Absent: Cayetano.

Motion to accept staff's recommendations in 2025-CI-0018

Moved/Second (Wilson/Allan) Motion failed.

Ayes: Wilson, Allan and DeTemple.

Noes: Buswell-Charkow, Viteskic and Sharma. Abstain: None. Absent: Cayetano.

Motion to modify staff's recommendation for Allegation 3.

Moved/Second (Allan/Buswell-Charkow) Motion failed.

Ayes: Viteskic, Buswell-Charkow and Sharma.

Noes: DeTemple, Wilson and Allan. Abstain: None. Absent: Cayetano.

2025-CI-0037**Motion to accept staff's recommendations for Complaint 2025-CI-0037.**

Moved/Second (Allan/Wilson) Motion failed.

Ayes: Wilson, Allan and DeTemple.

Noes: Buswell-Charkow and Viteskic. Abstain: Sharma. Absent: Cayetano.

Motion to accept staff's recommendations except for Allegations 3 & 6 in ODPa Complaint 2025-CI-0037.

Moved/Second (Buswell-Charkow/Sharma) Motion carried.

Ayes: Buswell-Charkow, Viteskic, Wilson, Sharma and DeTemple.

Noes: Allan. Abstain: None. Absent: Cayetano.

Motion to accept staff's recommendation for Allegation 3 in ODPa Complaint 2025-CI-0037.

Moved/Second (Viteskic/Wilson) Motion carried.

Ayes: Viteskic, Wilson, Allan and DeTemple.

Noes: Buswell-Charkow. Abstain: Sharma. Absent: Cayetano.

Motion to modify staff's recommendation for Officer 2 in Allegation 6 of ODPa Complaint 2025-CI-0037.

Moved/Second (Buswell-Charkow/Viteskic) Motion failed.

Ayes: Buswell-Charkow, Viteskic and Sharma.

Noes: Allan, Wilson and DeTemple. Abstain: None. Absent: Cayetano.

Motion to add a procedural section for all cases affected by tolling dispute.

Moved/Second (Wilson/Viteskic) Motion carried.

Ayes: Allan, Wilson, DeTemple, Buswell-Charkow, Viteskic and Sharma.

Noes: None. Abstain: None. Absent: Cayetano.

Motion to accept staff's recommendation for Officer 2 in Allegation 6.

Moved/Second (Buswell-Charkow/Sharma) Motion carried.

Ayes: Allan, DeTemple, Wilson, Buswell-Charkow, Viteskic and Sharma.

Noes: None. Abstain: None. Absent: Cayetano.

2026-CI-0009

Motion to accept staff's recommendations for Complaint 2026-CI-0009.

Moved/Second (Buswell-Charkow/Sharma) Motion carried.

Ayes: Viteskic, Wilson, Allan, DeTemple, Buswell-Charkow and Sharma.

Noes: None. Abstain: None. Absent: Cayetano.

END OF CLOSED SESSION

12. ANNOUNCEMENT OF CLOSED SESSION ACTIONS

Vice Chair Wilson announced the closed session actions.

13. ADJOURNMENT AT 9:15 PM

Motion to adjourn. Moved/Second (Wilson/Buswell-Charkow). The meeting was adjourned at 9:15 PM by unanimous consent.

ITEM 8
Subcommittee List

Updated on 10/2/2026



SUBCOMMITTEE LIST

Important Note: As of October 2, 2026, the PAB has 7 of its 9 seats filled, resulting in a quorum of 4 members. Subcommittees must be composed of fewer than a quorum and may not consist of a single member. Accordingly, vacancies must be filled or the subcommittee must be disbanded. If disbanded, its work can be reassigned to individual board members or formally paused or discontinued. For additional information on subcommittee requirements, please visit Chapter II Section 5 of the City of Berkeley's Commissioner's Manual:

<https://berkeleyca.gov/sites/default/files/documents/Commissioners%27%20%26%20Board%20Members%27%20Manual%202025%20Edition.pdf#Page=30>

Subcommittee	Board Members	Chair	BPD Reps
Policy Reviews Formed 11-08-2023 Scope Expanded 12-11-2024 to include BWC Policy Review Scope Expanded 09-09-2026 to include EIS Update Process	Cayetano DeTemple <u>Public members:</u> Kitt Saginor	N/A	Deputy Chief Tate Sgt. Rafferty
Metrics & Operations Formed 02-05-2025 after the Budget & Metrics and Operations & Processes Subcommittees were consolidated into one	Wilson Vacant	N/A	N/A
Outreach & Engagement Formed 11-08-2023 Scope Expanded 03-02-2024 Formerly "Commendations"	Allan Buswell- Charkow	N/A	N/A

Updated on 10/2/2026

Policies and Practices on Encampment Clearances Formed 6-25-2025	Wilson Sharma	TBD	TBD
--	------------------	-----	-----

LIAISON LIST

Liaison Name	Assignment
Cayetano	Represent the PAB in the BPD UOF Policy Update Process
Wilson	Represent the PAB in the Regulations Negotiation Process
Wilson	Tier 1 Evaluator for Public Safety Technology Proposals
DeTemple	Tier 1 Evaluator for Public Safety Technology Proposals
Sharma	Tier 2 Evaluator for Public Safety Technology Proposals

POLICY COMPLAINTS ASSIGNED TO BOARD MEMBERS

Policy Review #	Assigned Board Member(s)	Description
2025-PR-0001	Cayetano Sharma	BPD Policy 1004 "Anti-Retaliation" & BPD Policy 1010 "Personnel Complaints"

ITEM 9.B.I.

**September 30, 2026 Memorandum from Board Member Allan
to the PAB Titled “Recommendation that the City Council
Hire an Independent Auditor Dedicated Exclusively to
Monitoring and Auditing BPD’s Use of Surveillance
Technology”**



MEMORANDUM

Date: September 30, 2026
To: Honorable Members of the Police Accountability Board
From: Board Member Stephanie Allan
Subject: Recommendation that the City Council Hire an Independent Auditor Dedicated Exclusively to Monitoring and Auditing BPD's Use of Surveillance Technology

After reviewing the report sent to the PAB by Secure Justice and the report on the additional surveillance technology requested by BPD, I want to recommend to the PAB that an independent auditor be hired to monitor and audit the use of this expansive surveillance technology.

Independent audits provide a level of credibility to the service being audited. Having the same agency provide the audit creates a conflict of interest (self audit) while an independent audit creates accountability and public trust. The community will have a harder time believing the department if they are reviewing themselves. In comparison, an independent audit comes from a neutral party. Given the strong public sentiment regarding Flock and police surveillance, I think it's essential that there be an independent mechanism to oversee the use of such surveillance technology.

Additionally, I believe the reasons independent audits are needed are highlighted by the Secure Justice (SJ) Sept. 19, 2026 letter to the PAB, Executive Director Brian Hofer that details several security lapses in the audit Secure Justice did of BPD's Flock system.

Federal agents at the No. California Regional Intelligence Center (NCRIC) were allowed to query BPD's ALPR data in apparent violation of SB34 [although SJ Exec. Director Hofer did not exam the date for compliance with SB34], and BPD policy 1305. While Exec. Director Hofer focused on Flock, as the primary surveillance tool BPD used, we need to expand his recommendations to include all the surveillance technology BPD is seeking.

SJ also detailed the inadequacy of BPD's methodology in auditing access to ALPR data or examining "the enormous volume of third-party access." Additionally, BPD's auditing doesn't test for Berkeley's "most concrete privacy safeguards," the deletion of ALPR data after 30 days. In fact, BPD audit protocol "contains no retention or deletion

test at all.” And, in other jurisdictions that have cancelled Flock contracts over failure to delete data within a specified time, it was learned that Flock retained data indefinitely.

Given these deficiencies and others detailed in the SJ letter of 9/16/26, it is clear that more comprehensive audit standards and practices are essential, especially in light of the six technology areas BPD is asking to expand:

- ALPR’s
- Fixed Video Camera (Pan-tilt-zoom)
- Drone as First Responder (DFR)
- Field-Deployed Drones (Unmanned Aerial Systems)
- Community Video Stream Integration
- Investigative Software

Auditing this expansive use of surveillance technology on a regular basis, be it monthly, quarterly, is beyond the capacity of BPD or the City Auditor. An independent auditor is needed, perhaps located in the City Auditor’s department, who can implement SJ’s audit recommendations:

- A complete audit methodology, including population sizes, sampling methodology, selection procedures and the rationale for the sample size;
- Total BPD and third-party query volumes during the audit period;
- A breakdown of third-party searches by agency and user, including the number of searches attributable to each;
- A specific SB34 compliance audit addressing Civil Code section 1798.90.51 through 1708.90.55, rather than BPD Policy 1305 alone

Additionally, an independent auditor is required who can implement SJ’s further recommendations:

- The complete audit methodology, including population sizes, sampling methodology, selection procedures, and the rationale for the sample size;
- Total BPD and third-party query volumes during the audit period;
- A breakdown of third-party searches by agency and user, including the number of searches attributable to each;
- A specific SB34 compliance audit addressing Civil Code sections 1798,90.51 through 1798.90.55, rather than BPD Policy 1305 alone;
- A complete accounting of the federal agent searches reflected in BPD’s own Flock audit logs, including the users, agencies, number of searches and disposition of all resulting surveillance information;
- Identification of every fusion center, information-sharing network, task force, or intermediary-including NCRIC and WSIN- that had direct or indirect ability to query Berkeley surveillance data during the audit period;
- An audit specifically designed to determine whether any California user searched Berkeley data at the request of, on behalf of, or for the benefit of a federal or out-of-state agency;

- An explanation of exactly which fields were available in Flock's Organization and Network audit logs after Flock's December 2025 changes;
- The criteria used by Flock's audit-assistance tools and an explanation of what forms of improper access or sharing those tools cannot detect;
- A complete inventory of every category of Berkeley-derived information all vendors/Flock retain or generate - including raw reads, images, audit records, metadata, vehicle attributes or finger prints, speed or driving-pattern information, analytics, anonymized or aggregated derivatives, backups, and other telemetry - together with retention period, deletion process, and contractual authority for each;
- An explanation of whether Flock or any vendor selected retain any Berkeley-derived data after the 30-day customer-facing retention period or after contract termination, including anonymized or derivative data, and whether Berkeley expressly approved each such retention or secondary use.

The cost for this independent auditor should be a part of the contracts for the six technology areas for which RFP's were issued.

ITEM 9.B.II.

**Materials Presented at the September 23, 2026 PAB Regular
Meeting re: Flock Automated License Plate Reader Audit**

Flock Automated License Plate Reader Audit

January 2026 - June 2026



Berkeley Police Department Memorandum



To: Chief Louis

From: Arlo Malmberg, Strategic Planning and Accountability Manager

RE: Flock Automated License Plate Reader Audit - January 2026 to June 2026

OVERVIEW

The Berkeley Police Department's Strategic Planning and Accountability Manager conducted an audit of the Flock ALPR system to assess compliance with Policy 1305, Surveillance Use Policy- Fixed Automated License Plate Reader (ALPR). The audit scope included access records for the Flock ALPR system between January 1, 2026 and June 30, 2026.

BACKGROUND

Policy 1305 outlines the requirements for use and access to the Flock ALPR systems by BPD staff. The policy mandates biannual audits of the ALPR system to ensure compliance and detect any unauthorized access or data breaches.

SCOPE AND METHODOLOGY

The scope of this audit included all access records for the Flock ALPR system between January 1, 2026 and June 30, 2026.

The audit methodology involved:

1. Reviewing system access records for the specified timeframe from the Flock platform.
2. Analyzing the records for any instances of unauthorized access, data breaches, or prohibited uses as stipulated in Policy 1305.
3. For each search pattern flagged by Flock's audit assistance tools, reviewing the associated incident documentation to verify that the queried license plate was connected to the underlying incident.

FINDINGS

Objective 1: BPD - Authorized Access

Criteria:

1305.3 AUTHORIZED AND PROHIBITED USES (j): " 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."

Inspection Procedure:

- Review all access records for the Flock ALPR system during the audit period.
- Verify user roles.



Berkeley Police Department Memorandum



Findings:

- All access to the Flock ALPR system was made by authorized personnel.

Objective 2: BPD - Permitted Uses

Criteria:

1305.3 AUTHORIZED AND PROHIBITED USES (k): "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."

Inspection Procedure:

- Query access records for terms associated with impermissible use.
- Confirm that each search recorded a case/incident number and/or reason.
- Randomly select 100 searches and verify alignment between investigation and search.
- Review all search patterns flagged by Flock's audit assistance tools during the audit period.

Findings:

- No impermissible uses detected across officer activity. Reasons documented in line with Policy 1305's requirement to capture case/incident number and/or reason.
- All randomly selected searches were verified to align with the documented case/incident.



Berkeley Police Department Memorandum



- Flock's audit assistance tools flagged 35 search patterns during the audit period. For each, the associated incident documentation was reviewed and the queried plate was verified as connected to the incident. No pattern lacked a corresponding incident connection.

Objective 3: External - Authorized Access

Criteria:

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....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)."

Inspection Procedure:

- Query access records for Federal and out-of-state agencies.

Findings:

- No Federal or out-of-state agencies searched across BPD's ALPR network.

Objective 4: External – Permitted Uses

Criteria:

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....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)."

Inspection Procedure:

- Query access records for terms associated with impermissible use.

Findings:

- 0 searches referenced "ICE" or "CBP"
- 0 searches related to federal immigration enforcement

Secure Justice Letter

Regarding BPD's Flock ALPR Audit

January 2026 - June 2026

September 19, 2026



September 19, 2026

VIA E-MAIL ONLY

Police Accountability Board
City of Berkeley
1900 Addison Street, Fl. 3
Berkeley, CA 94704
E-Mail: dpa@berkeleyca.gov

RE: BPD Flock Audit – January through June 2026

Dear Chair and Members of the Police Accountability Board:

Secure Justice writes regarding the Berkeley Police Department's recently completed audit of its Flock automated license plate reader system covering January 1 through June 30, 2026.

The three-page memorandum is not sufficient to establish compliance. It provides conclusions, but virtually none of the underlying evidence necessary for the Board or the public to evaluate those conclusions. More importantly, it omits the most consequential compliance issue now confronting Berkeley's ALPR program: BPD's own Flock audit logs show that federal agents at the Northern California Regional Intelligence Center (NCRIC) were permitted to query Berkeley's ALPR data. Secure Justice possesses and has personally reviewed those BPD audit logs. That federal access violated SB 34's restrictions on disclosure and access to ALPR information.

This is not a hypothetical concern, and it cannot be resolved by reporting that no federal agency directly appeared as the searching agency during the January-June 2026 audit period. The NCRIC/Western States Information Network (WSIN) episode demonstrates that federal and out-of-state agencies can obtain the benefit of local ALPR searches through users or intermediaries that appear facially authorized. A meaningful audit therefore must ask not only who entered the query, but who requested it, for whose investigation it was performed, what purpose justified it, and where the resulting information went.

1. The audit does not evaluate compliance with SB 34.

The audit says its purpose was to assess compliance with BPD Policy 1305. Its methodology was to review Flock access records for unauthorized access, data breaches, and uses prohibited by that policy. SB 34 is never identified as an audit criterion. The memorandum therefore does not determine whether Berkeley complied with the independent requirements imposed by California's ALPR statutes, Civil Code sections 1798.90.5 et seq.

Among other requirements, Civil Code section 1798.90.52 requires an ALPR operator to maintain a record of access that includes the date and time, query data, the username of the person accessing the information and the organization or entity with which the person is

PAB
Flock Audit
Page 2 of 7

affiliated, and the purpose for accessing the information. California law also restricts disclosure and use of ALPR information. An audit designed to establish that Berkeley's ALPR program is compliant must test those statutory requirements directly, not merely compliance with a local policy.

That omission is especially serious here because Secure Justice's review of BPD's own audit logs shows actual federal access to Berkeley ALPR data through NCRIC. The audit should have identified, quantified, and analyzed that access under SB 34. It did not.

2. BPD's own logs show federal agents at NCRIC queried Berkeley data.

Secure Justice has obtained and personally reviewed BPD's Flock audit logs. Those records show BPD allowing federal agents associated with NCRIC to query Berkeley's ALPR data. This was not merely a theoretical configuration, an ambiguous vendor setting, or an outside agency's problem. Berkeley's own records document federal access to Berkeley ALPR information, as NCRIC was granted unfettered direct access by Berkeley, and because no human is involved in real-time in evaluating requests for data. We are suing neighboring Oakland in part due to their unlawful sharing of ALPR data with federal task forces at NCRIC, in violation of SB 34. The WSIN story broke months after our lawsuit was filed, but it will be at issue in the future trial.

That access is directly relevant to SB 34 compliance and to Berkeley's own restrictions on federal immigration use. Yet the current audit contains no accounting of those federal searches, no identification of the federal users or agencies, no analysis of their purposes, no explanation of how access was authorized, no examination of what information was returned, and no discussion of whether BPD disclosed ALPR information in violation of state law.

An audit that purports to determine whether external access was authorized, while failing to address known federal access reflected in BPD's own logs, cannot reasonably be treated as a complete compliance audit.

3. The NCRIC/WSIN warning confirms why BPD's methodology is inadequate.

In June 2026, NCRIC warned Bay Area law-enforcement partners that SFPD's ALPR audit had identified 'data sharing compliance issues' involving federal and out-of-state law-enforcement requests handled through WSIN. The warning explained that WSIN serves as an after-hours center for law-enforcement support centers including NCRIC, and that WSIN analysts with ALPR access had performed searches for investigations by federal law-enforcement agencies and agencies outside California. After SFPD identified the problem, the analysts' ALPR access was disabled and WSIN instituted corrective policies and training.

This matters because it exposes the central flaw in BPD's current audit. BPD's stated external-access procedure was simply to query access records for 'Federal and out-of-state agencies,' after which it concluded that '[n]o Federal or out-of-state agencies searched across BPD's ALPR network.' That methodology does not detect proxy or intermediary searches. An NCRIC or WSIN user may appear in the log as the person conducting the search even when the actual requester and beneficiary is a federal or out-of-state agency.

The relevant question is therefore not merely who pressed the search button. It is who requested the search, on whose behalf it was conducted, what purpose supported it, and who received the results. The audit does not demonstrate that BPD investigated any of those questions.

4. The audit's keyword search for ICE and CBP is not a meaningful federal-access audit.

For external permitted uses, BPD states that it queried access records for terms associated with impermissible use and reports that zero searches referenced 'ICE' or 'CBP' and zero searches related to federal immigration enforcement. That is not enough.

A prohibited federal search does not become lawful because the user omitted the words 'ICE' or 'CBP' from the reason field. Nor will a keyword search reveal a federal nexus where a California intermediary enters a facially legitimate investigative description, case number, offense, or other generic purpose while performing the search for a federal agent.

The NCRIC/WSIN warning confirms this precise problem: the WSIN analysts entered facially legitimate criminal purposes, including serious offenses, while the searches were being performed for federal or out-of-state investigations. BPD's own logs further demonstrate why Berkeley cannot equate the absence of an incriminating keyword with the absence of prohibited federal access.

5. The audit does not meaningfully examine the enormous volume of third-party access.

BPD's audit gives materially more scrutiny to its own comparatively small volume of searches than to third-party access. For internal searches, BPD randomly selected 100 searches, reviewed associated incident documentation, and reviewed 35 patterns flagged by Flock's audit-assistance tools. For external use, however, the described methodology largely consists of agency-category and keyword searches.

Based on previously reported volumes, BPD itself conducts roughly 1,000 queries per month, while third-party activity has been approximately 160,000 queries per month (based on BPD's Flock Audit logs review). If those figures remained representative during this six-month audit period, that would mean approximately 6,000 BPD queries compared with approximately 960,000 third-party queries. Yet the memorandum provides no comparable substantive sampling or validation of that vastly larger external universe.

A sample of 100 is not inherently invalid. The problem is that BPD provides no population size, sampling protocol, confidence level, expected error rate, stratification, or explanation for why 100 searches were sufficient. More importantly, the audit does not disclose a meaningful sample at all for the category generating the overwhelming majority of searches and presenting the greatest data-sharing risk.

6. Flock's December 2025 audit-log changes create an unresolved SB 34 problem.

The audit period begins January 1, 2026, immediately after Flock changed what information appeared in Network Audit Logs. Flock removed fields including officer identity and open-text search reasons from those network logs. Those fields bear directly on information California law requires operators to maintain, including the identity of the user and the purpose for access.

The obvious question is therefore: what records did BPD use in 2026 to establish the identity, agency affiliation, and purpose associated with every third-party search? The audit never answers it.

This problem is magnified by the NCRIC access documented in BPD's logs. If the audit record available to Berkeley no longer reliably displayed the identity and purpose necessary to trace a

PAB
Flock Audit
Page 4 of 7

search to its ultimate requester, BPD cannot simply conclude that external access was authorized without explaining the alternative records and verification process it used. If other records exist, the audit should identify and produce them. If they do not, BPD has a more fundamental SB 34 compliance problem.

7. Verifying a legitimate investigation does not establish lawful data sharing.

BPD reports that Flock's audit-assistance tools flagged 35 search patterns and that BPD verified the queried plates were connected to underlying incidents. That establishes, at most, an investigative connection. It does not establish that the person or agency requesting the search was legally entitled to obtain Berkeley ALPR information.

The NCRIC/WSIN incident makes this distinction concrete. NCRIC's warning states that the affected WSIN searches involved legitimate criminal investigations, including serious offenses, while simultaneously acknowledging that the searches were being performed for federal or out-of-state agencies and had created data-sharing compliance issues. A search can be connected to a real crime and still constitute an unlawful disclosure of Berkeley ALPR data.

The audit therefore must test both questions independently: whether a search had a legitimate investigative purpose, and whether Berkeley was legally permitted to provide its ALPR information to the ultimate requester.

8. The audit does not test whether Flock complied with Berkeley's data-retention and deletion requirements.

The audit also fails to test one of Berkeley's most concrete privacy safeguards: whether ALPR data was deleted when Berkeley's policy and vendor obligations required deletion. Policy 1305.8 provides that Berkeley ALPR data should be stored for no longer than 30 days absent a defined evidentiary or legal basis for preservation and expressly states that the ALPR vendor will purge its data at the end of 30 days. Berkeley's original surveillance acquisition materials likewise represented that the vendor would purge its hosted data after 30 days.

Yet BPD's audit contains no retention or deletion test at all. It does not report whether the auditor selected records older than 30 days and attempted to retrieve them; whether Flock certified deletion; whether backend, derivative, telemetry, analytics, or other copies persisted after the customer-facing retention window; whether any data had been placed into longer-term storage; or whether Flock retained or generated information beyond the data types disclosed to and approved by Berkeley. An audit of contractual and policy compliance should test what the vendor retained, not merely what the user interface allowed BPD to see.

Recent events in other jurisdictions make that omission especially important. In Marietta, Oklahoma, Police Chief Brett Harris entered an August 2026 council meeting supporting continued use of Flock cameras. During the meeting, after a Flock representative explained the company's retention practices, Harris stated that he had learned Flock retained data beyond the 30-day period he understood had been agreed upon - describing the retention as indefinite - and immediately withdrew his support. The council then voted not to continue with Flock. Harris explained that the department would not support retention beyond the agreed 30-day limit because, in his words, the data was not actually gone. (KXII, Aug. 20, 2026; KTEN, Aug. 2026.)

PAB
Flock Audit
Page 5 of 7

Sheboygan, Wisconsin presents a related warning about both retention and undisclosed data categories. Sheboygan's agreement provided for deletion of information after 30 days. But Flock later approached the City about providing up to five years of anonymous data concerning driving patterns and speeding. That disclosure raised the obvious question of how Flock could offer years of historical vehicle-behavior data derived from a system the City understood to operate under a 30-day deletion requirement, and it revealed a category and secondary use of data that had not been part of the City's public understanding of the ALPR program. Sheboygan ultimately voted unanimously not to renew its Flock contract. (TMJ4, Sept. 2026.)

These examples do not by themselves establish that Flock retained Berkeley's raw ALPR records beyond 30 days. But they make it unreasonable for a Berkeley compliance audit simply to assume deletion occurred because the contract and policy required it. The entire point of an audit is to verify performance against the requirement. BPD should have independently tested whether Berkeley data was actually purged at the required time, what information Flock continued to retain or derive after purge, and whether any retained metadata, analytics, speed information, vehicle fingerprints, or other derivative information fell outside what Berkeley approved or was told the system collected.

This is particularly important because Berkeley's own 2026 PAB materials have already identified post-termination and derivative-data concerns in Flock's Master Services Agreement, including a provision described as granting Flock a perpetual license to retain anonymized derivatives of City data after termination. A serious audit therefore should distinguish among raw ALPR reads, customer-visible records, audit logs, metadata, derived or anonymized datasets, and other telemetry; identify the retention period applicable to each; and verify actual deletion rather than assuming all of those categories disappear when a 30-day customer retention window expires.

9. The audit provides conclusions without the underlying evidence.

The memorandum contains essentially no primary-source audit material. There is no anonymized or redacted audit-log sample, no list of external agencies or users, no search-volume totals, no breakdown by agency or purpose, no sampling worksheet, no explanation of the 35 Flock-generated flags, no statistical analysis, and no documentation showing how BPD excluded indirect federal or out-of-state access.

The Board is therefore being asked to accept the Department's conclusions without the evidence necessary to independently evaluate them. That is particularly problematic for civilian oversight. An audit that cannot itself be audited provides little accountability.

What the Board should require before accepting this audit

- The complete audit methodology, including population sizes, sampling methodology, selection procedures, and the rationale for the sample size.
- Total BPD and third-party query volumes during the six-month audit period.
- A breakdown of third-party searches by agency and user, including the number of searches attributable to each.
- A specific SB 34 compliance audit addressing Civil Code sections 1798.90.51 through 1798.90.55, rather than Policy 1305 alone.

PAB
Flock Audit
Page 6 of 7

- A complete accounting of the federal-agent searches reflected in BPD's own Flock audit logs, including the users, agencies, dates, purposes, number of searches, and disposition of resulting ALPR information.
- An explanation of why federal agents associated with NCRIC were permitted to query Berkeley ALPR data, who authorized that access, when BPD learned of it, and what corrective action was taken.
- Identification of every fusion center, information-sharing network, task force, or intermediary - including NCRIC and WSIN - that had direct or indirect ability to query Berkeley ALPR data during the audit period.
- An audit specifically designed to determine whether any California user searched Berkeley data at the request of, on behalf of, or for the benefit of a federal or out-of-state agency.
- An explanation of exactly which fields were available in Flock's Organization and Network Audit Logs during the audit period and how BPD verified user identity, agency affiliation, and purpose after Flock's December 2025 changes.
- The criteria used by Flock's audit-assistance tools and an explanation of what forms of improper access or sharing those tools cannot detect.
- A substantive review of third-party searches that does not depend on keywords such as 'ICE' and 'CBP.'
- A retention-and-deletion audit that independently verifies whether Flock purged Berkeley's ALPR data after 30 days except where a documented exception applied, including test retrieval of records outside the retention window and documentation of the deletion method.
- A complete inventory of every category of Berkeley-derived information Flock retains or generates - including raw reads, images, audit records, metadata, vehicle attributes or fingerprints, speed or driving-pattern information, analytics, anonymized or aggregated derivatives, backups, and other telemetry - together with the retention period, deletion process, and contractual authority for each category.
- An explanation of whether Flock retains any Berkeley-derived data after the 30-day customer-facing retention period or after contract termination, including anonymized or derivative data, and whether Berkeley expressly approved each such retention or secondary use.
- Sufficient underlying, appropriately redacted audit materials to permit the PAB and Office of the Director of Police Accountability to independently evaluate BPD's conclusions.

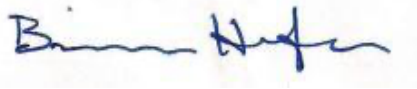
These requests go to the basic questions an ALPR audit must answer: Who accessed Berkeley's surveillance data? Who requested the search? Why was it conducted? Who received the results? Was that access and disclosure lawful? And what evidence demonstrates those conclusions?

Here, those questions are not academic. BPD's own audit logs document federal agents accessing Berkeley ALPR data through NCRIC. The regional NCRIC/WSIN warning independently confirms the mechanism by which federal and out-of-state investigations obtained the benefit of local ALPR systems through intermediaries. Against that factual backdrop, a three-page memorandum, an unexplained sample of 100 internal searches, vendor-selected flags, and keyword searches for 'ICE' and 'CBP' are not sufficient to establish compliance.

PAB
Flock Audit
Page 7 of 7

We respectfully ask the Board to require BPD to conduct and disclose a genuine SB 34 compliance audit, including a complete accounting of the federal access already documented in Berkeley's own records, before accepting the Department's conclusion that external access and use were authorized.

Sincerely,

A handwritten signature in blue ink, appearing to read "Brian Hofer", is shown on a light-colored background.

Brian Hofer
Executive Director
(510) 303-2871
brian@secure-justice.org
<https://secure-justice.org/>
San Francisco Bay Area, CA

Chief NCRIC Communication

June 18, 2026

September 23, 2026
PAB Regular Meeting

33

Good morning,

I wanted to brief you on a news story that broke yesterday and will likely generate some attention in our community, as it relates to ALPR technology in a neighboring jurisdiction. The events did not impact our own camera network, but just wanted to make sure you were aware and had some additional context.

I've attached the story below for you, but in short, SFPD has indicated that a routine audit found its Flock license plate reader network had been queried on behalf of out-of-state and federal agencies through NCRIC (Northern California Regional Intelligence Center), reportedly by analysts on a related law enforcement intelligence network (Western States Information Network (WISN)). SFPD has indicated that the queries did not reference immigration or reproductive rights matters, did not involve ICE or DHS, and were for the purpose of investigating serious and violent crimes. The issue with the searches is that SB34 says clearly that ALPR data cannot be shared with out-of-state or Federal entities. SFPD shared that it disabled NCRIC's access upon discovery of this issue. While we have not had direct contact with SFPD regarding this issue, and the numbers are SFPD's own and may be refined as the full audit comes out, we do know that due to our restrictive share settings, **these searches did not access our network.**

This is an SFPD finding, not a Berkeley one, because last year we proactively acted to prevent this exact risk. A year ago, we proactively turned off statewide lookup and narrowed our ALPR data sharing to our nine Bay Area counties, specifically because broad statewide/national querying created exposure we wanted to avoid. Narrowing access allowed us greater control and limited data sharing to surrounding jurisdictions where there was more likely to be a connection to our cases or regional crime issues. Further, we also continue to require waivers from agencies we share with, audit regularly, and pause/remove agencies if there are any improper uses. These proactive steps materially reduced the pathway by which an outside agency could reach Berkeley data through a multi-agency search and provided a process to identify and address any potential issues.

As some additional context on NCRIC, it is the regional intelligence "fusion center" for Northern California, created under the post-9/11 DHS information sharing framework, and it functions as a hub where member agencies' data, including ALPR, can be shared across jurisdictions. Again, we do not share ALPR data with NCRIC. NCRIC's stated policy is that it shares ALPR data only with California agencies, not federal or out-of-state. I have included below the language from an email I received yesterday evening from Mike Sena, the Executive Director of NCRIC. It appears to have been sent broadly to all partner agencies and provides more detail from the SFPD audit and the searches.

State law and Berkeley's sanctuary city values matter deeply to us. We have witnessed the tremendous benefits of this technology but understand how important it is to safeguard the data and be transparent about any issues. We have a responsibility to handle these issues with care, precision, and integrity so our actions reflect our commitment to privacy, transparency, and the trust of the community.

Please let me know if you'd like to discuss further or need additional information,

33

Jen

Link to NBC Bay Area Story:

[License plate readers 'improperly' accessed, SFPD says – NBC Bay Area](#)

Excerpt from email from Mike Sena, Executive Director of NCRIC:

SFPD recently conducted an ALPR audit that identified data sharing compliance issues related to federal and out of state law enforcement requests for investigative support by the Western States Information Network (WSIN). For five decades WSIN has provided vital law enforcement deconfliction and analytical support to state and local law enforcement agencies across California that has kept officers safe, reduced duplication of effort, and helped solve major crimes.

WSIN also serves as the after-hours center or law enforcement support centers across the state, including the NCRIC, and a few of their analysts have had access to ALPR data to support local and state law enforcement agency cases. SFPD identified that the WSIN analysts had submitted the lawful purposes in the details of the free text area of the system for criminal violations ranging from homicide, human trafficking, and other violent crimes, and included that the search was being performed for investigations by Federal law enforcement agencies or law enforcement agencies outside of California.

After notification of SFPD's preliminary audit findings, the WSIN analysts' ALPR system access was turned off. WSIN Director Kent Shaw and his team have taken immediate action to educate the employees and put policies and training in place to address the data sharing issues that were identified through the audit.



Chief Jennifer Louis
BERKELEY POLICE DEPARTMENT
(510) 981-5700

Follow us on:



Flock Automated License Plate Reader Audit

January 2025 - June 2025



BERKELEY POLICE DEPARTMENT MEMORANDUM



To: Chief Louis

From: Arlo Malmberg, Strategic Planning and Accountability Manager

RE: Flock Automated License Plate Reader Audit – January 2025 to June 2025

OVERVIEW

The Berkeley Police Department's Strategic Planning and Accountability Manager conducted an audit of the Flock ALPR system to assess compliance with Policy 1305, Surveillance Use Policy – Fixed Automated License Plate Reader (ALPR). The audit scope included access records for the Flock ALPR system between January 1, 2025 and June 30, 2025. The audit methodology involved analyzing these access records for unauthorized access, data breaches, and prohibited uses.

The audit found 100% compliance by Berkeley PD personnel with ALPR policy and 100% compliance with authorized access by external agencies. The audit also found 99.81% compliance with permitted search reasons by external agencies.

BACKGROUND

Policy 1305 outlines the requirements for use and access to the Flock ALPR systems by BPD staff. The policy mandates biannual audits of the ALPR system to ensure compliance and detect any unauthorized access or data breaches.

SCOPE AND METHODOLOGY

The scope of this audit included all access records for the Flock ALPR system between January 1, 2025 and June 30, 2025.

The audit methodology involved:

1. Reviewing system access records for the specified timeframe from the Flock platform.
2. Analyzing the records for any instances of unauthorized access, data breaches, or prohibited uses as stipulated in Policy 1305.



BERKELEY POLICE DEPARTMENT MEMORANDUM



SUMMARY OF FINDINGS

Objective #	Audit Objectives	% Meeting Standards
1	BPD – Authorized access	100%
2	BPD – Permitted uses	100%
3	External – Authorized access	100%
4	External – Permitted uses	99.81%

DETAILED FINDINGS

Objective 1: BPD – Authorized Access

Criteria:

1305.3 AUTHORIZED AND PROHIBITED USES (j): " 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."

Inspection Procedure:

- Review all access records for the Flock ALPR system during the audit period.
- Verify user roles.

Findings:

- All access to the Flock ALPR system was made by authorized personnel.

Objective 2: BPD – Permitted Uses

Criteria:

1305.3 AUTHORIZED AND PROHIBITED USES (k): "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



BERKELEY POLICE DEPARTMENT MEMORANDUM



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."

Inspection Procedure:

- Query access records for terms associated with impermissible use.
- Confirm that each search recorded a case/incident number and/or reason.

Findings:

- No impermissible uses detected across officer activity. Reasons documented in line with Policy 1305's requirement to capture case/incident number and/or reason.

Objective 3: External – Authorized Access

Criteria:

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....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)."

Inspection Procedure:

- Query access records for Federal and out-of-state agencies.

Findings:

- No Federal or out-of-state agencies searched across BPD's ALPR network.

Objective 4: External – Permitted Uses



BERKELEY POLICE DEPARTMENT MEMORANDUM



Criteria:

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....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)."

Inspection Procedure:

- Query access records for terms associated with impermissible use.

Findings:

- 0.19% of searches made reference to a federal agency acronym.
- All of those searches were broad searches of all available California networks; none targeted Berkeley specifically.
- 1 search included the term "ICE", and 2 included the term "CBP". These searches correspond to "statewide lookup" searches that affected all California agencies that had the "statewide lookup" feature enabled at the time. We have since disabled this feature (see Departmental Actions below).
- As verified in Objective 3, no federal agencies, and no agencies outside of California accessed Berkeley's ALPR network.
- The presence of those terms does not by itself establish a violation of California law or Policy 1305. We cannot conclude a state-law violation from reason-field text alone. For example, 5 searches included the term "DHS." Upon closer examination, they were in reference to DHS PD, or Desert Hot Springs Police Department.

DEPARTMENTAL ACTIONS

Recognizing potential risks revealed both via this audit and as discovered by incidents in other jurisdictions, BPD implemented several preventative measures to further protect Berkeley data while still maintaining the technology's public safety value.

- **Access narrowing during audit.** After the finding above, by order of the Chief, BPD tightened access in response to community concerns and to align strictly with Policy 1305's sharing provisions:
 - Revoked network access for all agencies outside the nine Bay Area counties plus Sacramento County.
 - Turned off the statewide lookup tool.
 - Nationwide lookup had already been disabled before rollout.



BERKELEY POLICE DEPARTMENT MEMORANDUM



- Since undertaking these actions, 0 searches have referenced “ICE”, “CBP”, or any other federal immigration enforcement agency.
- **Ongoing controls.** BPD now by protocol will revoke sharing for any agency if a search reason appears to fall outside of that which is permitted by BPD policy, ordinance or law until that agency provides a written explanation and assurances that its use of our data is consistent with Policy 1305 and California law.
 - To promote regional compliance, we will notify requesting agencies whenever a search reason includes language that may fall outside the allowable parameters.
 - To ensure continued full compliance internally, BPD will conduct roll call training regarding use policies for ALPRs, access controls and the intersection with state law and the recently passed Sanctuary City Ordinance.

VENDOR ACTIONS

Flock acknowledged that permissive default sharing was a flaw and has taken corrective steps to support California law and Berkeley’s Sanctuary City policy.

- Flock shifted to **restrictive-by-default sharing**, paused all federal pilots, created a distinct “Federal” organization label, removed federal users from Statewide and National Lookup, and began publishing ongoing compliance updates.
- Flock now enforces state-border sharing limits, **prevents federal or out-of-state access to California data**, blocks searches tied to immigration or reproductive-health enforcement through keyword filters, and presents clearer prompts on share requests.
- Flock is developing **proactive audit alerts** for 2026 to make it easy to screen for unpermitted uses in real time.

PAB Letter to City Council Regarding

**Annual Surveillance Technology Report - November 10,
2025**



Josh Cayetano | Chair
Police Accountability Board
JCayetano@berkeleyca.gov

November 10, 2025

VIA ELECTRONIC MAIL

Honorable Mayor Ishii and Members of the Berkeley City Council
Council@berkeleyca.gov
2180 Milvia Street
Berkeley, CA 94704

Re: Item 11 - Annual Surveillance Technology Report for Body Worn Cameras, GPS Trackers, Fixed Surveillance Video Cameras, Parking Enforcement Officer Automated License Plate Readers, the Street Level Imagery Project, Unmanned Aerial Systems, and Fixed Automated License Plate Readers

Dear Honorable Mayor Ishii and Members of the Berkeley City Council:

On behalf of the Police Accountability Board (PAB), I write to highlight three concerns regarding Berkeley Police Department's (BPD) Annual Surveillance Technology Report (or "Report"), currently Item 11 on the Berkeley City Council's action calendar for its November 10, 2025, meeting.¹

First, the Report was published to the Council's action calendar without input from or even advance notice to the PAB. BPD Policy 1305.12 specifically requires that the results of any audits of ALPR data—like the audit described in the Report—be shared with Office of the Director of Police Accountability (ODPA) upon their completion.² More fundamentally, as we explained in a recent letter regarding BPD's unilateral proposal to encrypt radios,³ both the Council and the

¹ At its November 6, 2025 meeting, the PAB voted 5-0 to approve a Motion to authorize Chair Cayetano to send a letter to the City Council, either prior to the November 10th Regular Council meeting or at a later appropriate time, to address procedural and substantive concerns regarding the Annual Surveillance Technology Report and to reiterate the PAB's opposition to the use of Flock. Video recording can be accessed at the following link with relevant remarks at [01:17:56]: <https://youtu.be/lPytFxB6jyw?si=eu9uiwxrvfYYZiiQ>

² See Attachment 1: BPD Policy 1305 – Fixed ALPR

³ October 28, 2025 ODPA Letter to Council Re: Importance of Proper Vetting for Public Safety Policy Changes — Concerns About

public benefit from the PAB's review of public safety items submitted on behalf of BPD prior to their publication. In this instance, if the PAB was provided with the draft prior to publication, the PAB could have informed BPD and the City Manager that Berkeley Municipal Code 2.99.020(2)(c) requires that the Report include a summary of complaints received by the City, including the PAB, and provided BPD and the City Manager with that relevant information.⁴ The day that the ODPa and the PAB noticed that the Report did not include the required information, we notified the City Manager and Chief Louis.

Specifically, the PAB and ODPa notified the City Manager of two complaints involving the use of body-worn camera, a surveillance technology enumerated in BMC 2.99.020.⁵ In response, the Chief argued that the complaints should not be included in the Report because the allegations were not raised by a member of the public in their initial complaint. The PAB respectfully disagrees. If that were true, complaints alleging failure to follow BPD's body-worn camera policy would rarely, if ever, be included in the Report because complainants are routinely prevented from accessing body worn camera footage under current BPD practices. Omitting the types of complaints that the PAB identified would circumvent the purpose of the Surveillance Technology Ordinance by decreasing transparency and depriving the Council of the data that ensures the safeguards of the people's civil liberties have been "strictly observed."⁶ We ask Council to require BPD to supplement this year's annual report with all complaints about Surveillance Technology, including the ones submitted to the PAB, and "any information about violations or potential violations of the Surveillance Use Policy" as required by law.⁷

Second, pages 40 to 45 of the Report describe the results of a Flock ALPR audit conducted by BPD, which inexplicably refuses to conclude that one or more external agencies searched Berkeley

Item 18 "Authorization to Encrypt Berkeley Police Department Primary Radio Channels" https://berkeleyca.gov/sites/default/files/documents/2025-10-28%20DPA%20Ltr%20to%20CoB%20Council-%20Radio%20Encryption%20Concerns_Final.pdf

⁴ Berkeley Municipal Code 2.99.020(2)(c) plainly states that the Report shall include "[a] summary of each complaint, if any, received by *the City* about the Surveillance Technology."

⁵ 2024-CI-0031, Allegation 6: Improper Police Procedures (Improper body-worn camera use) – Whether the subject officers activated their BWC as required by policy; 2025-CI-0018, Allegation 6: Improper Police Procedures (Improper body-worn camera use) – Whether the subject officers activated their BWC as required by policy.

⁶ BMC 2.99.010 states that "In addition to applicable local, state, and federal law, legally enforceable safeguards, including robust transparency, oversight, and accountability measures, are important in the protection of civil rights and civil liberties" and "Data reporting measures will enable the City Council and public to confirm that mandated civil rights and civil liberties safeguards have been strictly observed."

⁷ The Ordinance explicitly mandates that BPD include "any information about violations or potential violations of the Surveillance Use Policy." BMC 2.99.020(2)(d).

and other California cities' ALPR data for the purposes of federal immigration enforcement, a practice that violates BPD policy. BPD explains that an unidentified number of external law enforcement agencies entered "ICE" once and "CBP" twice in the reason field when it searched the statewide ALPR data, including Berkeley's. BPD does not explain which California agencies improperly accessed ALPR data, nor does it explain when BPD identified the non-compliant use of the statewide ALPR data lookup function. Notwithstanding the reference to ICE and CPB, BPD does not conclude that there was a violation of California law or Policy 1305, reasoning that "the presence of [terms associated with impermissible use] does not by itself establish a violation."

Despite the vague description and the equivocal conclusion, BPD explains in detail the remedial actions that it took to narrow access to ALPR data and reassure the community that a future violation is unlikely. Besides disabling the statewide lookup tool feature, BPD states that it will now revoke sharing for any agency that uses a term associated with impermissible use until they have provided a written explanation and assurances that the use of Berkeley's data is consistent with California law and Policy 1305.⁸ These measures have not been formally memorialized in BPD Policy at the time of this writing.

Third, while the PAB appreciates BPD's commitment to remediating the non-compliance and the steps that it has taken to ensure future compliance with California law and Policy 1305, the Council should take notice of the timing of the ALPR audit report and its presentation. BPD identified the noncompliant use of Flock ALPR data in July 2025, before its presentation to Council, requesting that the City contract with Flock for its external fixed surveillance cameras. In its materials that were submitted pursuant to the Surveillance Technology Ordinance, BPD did not mention that it identified a potential policy violation of Policy 1305 or Berkeley's sanctuary city resolution.⁹ In fact, the PAB submitted materials, urging Council to adopt revisions to the Fixed Surveillance Camera Use Policy, citing data security issues that were reported in *other* jurisdictions' and still,

⁸ At the PAB meeting on November 5, 2025, BPD refused to identify the agencies responsible for the potential breach because "those fall under investigatory records that aren't released publicly."

Relevant remarks [40:42] <https://youtu.be/1PytFxB6jvw?si=gCtR8SUAWQy7gqOC&t=2442>

⁹ See Attachment 2: STO Submission for External Fixed Surveillance Cameras: BPD stated that "[s]afeguarding privacy from potential misuse, particularly concerning federal immigration enforcement, is critical. Protections include state law (e.g., SB 54 prohibits sharing certain information for federal immigration enforcement), alignment of BPD policy with state law, Flock's terms forbidding such sharing, and prompt notification procedures if federal access is requested.....Use will comply with California SB 54, prohibiting data sharing for federal immigration enforcement. Flock's Terms of Agreement also forbid sharing data with federal immigration agencies. The City will be notified if federal authorities request access, allowing for intervention and oversight."

BPD did not mention, either in its papers or at the hearing, the breach that it identified. BPD, in other words, was less than forthcoming about the data security issues with Flock Safety.

The PAB recommended to Council, and Council agreed, to subject external fixed surveillance camera data to the same audit procedures as ALPR data based on the PAB's historic understanding of the audit procedure. After reviewing the audit report and considering the delayed notification to the PAB and the Council, the PAB recommends that the Council (1) shorten the timeframe of notification of a potential data breach; (2) require BPD to identify the agencies that accessed Berkeley's data for an improper purpose and the agencies that have had their access revoked as a result of the improper use; (3) memorialize the remedial controls that BPD implemented in Policies 1304 and 1305; and (4) require BPD or the City Manager to include an addendum or follow-up report on the identified instances of ODPa/PAB identified misuse in the surveillance report.

Respectfully submitted,



Joshua Cayetano | Chair
Police Accountability Board
City of Berkeley, CA

Cc: Paul Buddenhagen, City Manager
David White, Deputy City Manager
Jennifer Louis, Chief of Police
Jen Tate, Deputy Chief of Police
Hansel A. Aguilar, Director of Police Accountability
Farimah Brown, City Attorney
Mark Numainville, City Clerk

ATTACHMENTS: BPD Policy 1305 – Fixed ALPR
STO Submission for External Fixed Surveillance Cameras

ATTACHMENT 1
BPD Policy 1305 – Fixed ALPR

Surveillance Use Policy-Fixed Automated License Plate Readers (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

Berkeley Police Department
Law Enforcement Services Manual*Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)*

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

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 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.
- (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.)
- (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).
- (h) 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

Berkeley Police Department
Law Enforcement Services ManualSurveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

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 (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.
- (i) All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:
 1. Entering Department member's name
 2. Related case number
 3. Short synopsis describing the nature of the originating call
 - (j) 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.
 - (k) 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:

Berkeley Police Department
Law Enforcement Services Manual*Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)*

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.
- (l) Anyone who intentionally, or negligently, 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.
- (m) 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. 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

Berkeley Police Department
Law Enforcement Services ManualSurveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

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

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).

Berkeley Police Department
Law Enforcement Services Manual*Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)*

- (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 Office of Strategic Planning and Accountability 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.

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.

Berkeley Police Department
Law Enforcement Services Manual*Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)*

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 acknowledgment 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).
- (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 Office of Strategic Planning and Accountability 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 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 Office of Strategic Planning and Accountability 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.

Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

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.

1305.14 ATTACHMENTS

See attachment: [ALPR Acknowledgment Letter.pdf](#)

Attachments

Attachment

Law Enforcement Services Manual

ALPR Acknowledgment Letter.pdf



AUTOMATED LICENSE PLATE READERS DATA SHARING ACKNOWLEDGMENT LETTER

This letter is to certify that the (AGENCY NAME) has requested to receive data from the Berkeley Police Department's Automated License Plate Readers Program.

Data shared by the Berkeley Police Department will only be used for legitimate California law enforcement purposes ONLY, and not for other purposes such as immigration, personal use, harassment, and any other usages that are against the Berkeley Police Department's Policy.

By signing this letter, the representatives of (AGENCY NAME) agree to abide by this policy.

(Signature/Print name)

(Title/Rank)

(Date)

ATTACHMENT 2

STO Submission for External Fixed Surveillance Cameras



ACTION CALENDAR
July 22, 2025

To: Honorable Mayor and Members of the City Council
From: Paul Buddenhagen, City Manager
Submitted by: Jennifer Louis, Chief of Police
Subject: Surveillance Technology Ordinance Submission for External Fixed Surveillance Cameras (Flock Safety Condor Video Cameras)

RECOMMENDATION

Adopt a Resolution:

1. Accepting the attached Surveillance Acquisition Report for the Flock Safety Condor video cameras, pursuant to Berkeley Municipal Code (B.M.C.) Chapter 2.99.
2. Re-affirming the associated Berkeley Police Department (BPD) Use Policies (BPD Policy 351: External Fixed Video Surveillance Cameras and BPD Policy 1304: Surveillance Use Policy—External Fixed Video Surveillance Cameras), which were previously approved by Council on June 13, 2023.

CURRENT SITUATION AND ITS EFFECTS

This report is submitted in accordance with the Surveillance Technology Ordinance (STO) process, as codified in B.M.C. Chapter 2.99. The City is transitioning its External Fixed Video Surveillance Camera program to a new vendor, Flock Safety, and deploying Flock Safety Condor video cameras. This transition and the introduction of a new model of technology requires the submission of a Surveillance Acquisition Report for review and acceptance by the City Council.

This action will allow the Police Department to proceed with the camera installation plan as previously directed by Council, utilizing modern, solar-powered technology that resolves prior installation challenges and integrates with the City's existing Automated License Plate Reader (ALPR) network.

BACKGROUND

On October 12, 2021, and again on January 30, 2024, the City Council authorized the installation of an external fixed video surveillance camera program to enhance public safety. Subsequent analysis identified Flock Safety's solar-powered Condor cameras as

the most effective technology to meet the City's needs and overcome significant power supply and right-of-way challenges associated with the previous vendor. On March 18, 2025, Council approved updated locations for the cameras and directed BPD to initiate the STO review process.

The adoption of a new vendor and specific technology initiated the requirement under the STO to submit a new Surveillance Acquisition Report for approval by Council. The BPD policies governing the use of this technology—Policy 351 and Policy 1304—are not being changed. These Use Policies underwent the full STO review process, including pursuant to the ordinance, Police Accountability Board (PAB) review, and were formally approved by the City Council on June 13, 2023. They are included with this submission solely to fulfill the procedural requirements of the ordinance, which mandates that a complete package of STO documents be presented. Also pursuant to policy, this acquisition report and the previously approved policies were submitted to the PAB on June 19, 2025.

RATIONALE FOR RECOMMENDATION

Accepting the Surveillance Acquisition Report is the final procedural step required under the STO to implement the Council-approved External Fixed Video Surveillance Camera program with the selected vendor, Flock Safety. This action ensures the City remains in full compliance with its surveillance oversight laws while allowing the Police Department to deploy a critical tool to deter crime and support criminal investigations. The Flock Condor cameras offer superior technical capabilities and flexible installation options that will allow the project to be completed promptly and effectively.

Furthermore, the Flock Safety Condor cameras align with the City's high standards for data privacy and civil liberties protection. As detailed in the Surveillance Acquisition Report, the system employs robust, multi-layered security measures, including end-to-end encryption, secure cloud storage on AWS GovCloud, and strict access controls. The technology integrates seamlessly into the Police Department's existing workflows, operating on the same platform as the City's ALPR network, which maximizes its public safety value without creating new operational burdens. This combination of advanced security, adherence to strict use policies, and operational efficiency ensures that the deployment of these cameras fully meets the Council's original intent to enhance safety while upholding community values.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

Transitioning to solar-powered cameras will reduce the carbon footprint of this project.

FISCAL IMPACTS OF RECOMMENDATION

As detailed in the attached Surveillance Acquisition Report, Flock Safety Condor cameras are priced as a subscription service at \$5,000 per camera per year. For the 16 proposed cameras, the total annual cost is approximately \$80,000. This recurring

Surveillance Technology Ordinance Submission for
External Fixed Surveillance Cameras (Flock Safety Condor Video Cameras)

ACTION CALENDAR
July 22, 2025

cost includes hardware, installation, ongoing maintenance, cellular service, data hosting, and software updates. Funding for this program is allocated from the FY 2024 baseline Public Works budget, with sufficient funds available to cover operating costs for four years. Further use of the technology beyond the initial four years will require additional funding allocations.

CONTACT PERSON

Jennifer Louis, Chief of Police, (510) 981-5700

ATTACHMENTS

1. Resolution
2. Surveillance Acquisition Report: Flock Safety Condor Video Cameras
3. BPD Policy 351: External Fixed Video Surveillance Cameras (Approved 6/13/2023)
4. BPD Policy 1304: Surveillance Use Policy—External Fixed Video Surveillance Cameras (Approved 6/13/2023)

Surveillance Technology Ordinance Submission for
External Fixed Surveillance Cameras (Flock Safety Condor Video Cameras)

ACTION CALENDAR
July 22, 2025

RESOLUTION NO. ##,###-N.S.

**ACCEPTING THE SURVEILLANCE ACQUISITION REPORT FOR FLOCK SAFETY
CONDOR VIDEO CAMERAS**

WHEREAS, the City of Berkeley is committed to leveraging technology to enhance public safety while ensuring transparency, oversight, and the protection of civil liberties and civil rights, as codified in the Surveillance Technology Ordinance (B.M.C. Chapter 2.99); and

WHEREAS, the City Council previously authorized the implementation of an External Fixed Video Surveillance Camera program to aid in deterring crime and supporting criminal investigations; and

WHEREAS, the Police Department has, in accordance with B.M.C. 2.99.030, prepared and submitted a Surveillance Acquisition Report detailing the technology's description, purpose, location, impact, and safeguards; and

WHEREAS, the governing Use Policies for this technology, BPD Policy 351 and BPD Policy 1304, were previously reviewed and approved by the City Council on June 13, 2023, and are submitted herewith without change, pursuant to the requirements of the Surveillance Technology Ordinance.

NOW, THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the City Council hereby accepts the Surveillance Acquisition Report for the Flock Safety Condor Video Cameras, allowing the City Manager and Police Department to proceed with the acquisition and deployment of this technology in accordance with the report and the previously approved Use Policies.

Surveillance Acquisition Report: External Fixed Surveillance Cameras - Flock Safety Condor Video Cameras

This report is submitted in accordance with Berkeley Municipal Code (BMC) Chapter 2.99 concerning the Acquisition and Use of Surveillance Technology. The City of Berkeley is transitioning its External Fixed Video Surveillance Camera program vendor from Edgeworth Integration, LLC to Flock Safety and plans to deploy Flock Safety Condor video cameras.

1. Description (BMC 2.99.020(3)(a))

- Condor cameras capture high-definition video footage. PTZ models allow for remote control to pan, tilt, and zoom.
- They operate on the FlockOS platform, which is the same platform through which Berkeley PD currently accesses Automatic License Plate Readers (ALPR).
- The cameras do not record audio, and audio recording is explicitly prohibited by Berkeley policy for these types of cameras.
- The system utilizes AI for features like "People Detection Alerts" (identifying human presence without facial recognition) and "Visual Alerts" (tracking vehicles across feeds).
- Some models feature dual lenses to maintain wide-angle context while zoomed in.
- They offer features like 25x optical zoom and high-quality nighttime imagery.
- Crucially for Berkeley's deployment challenges, Flock offers solar-powered, LTE-enabled cameras, eliminating the need for direct electrical wiring or complex network infrastructure setup on city poles.
- Data is transmitted wirelessly via cellular connection to cloud storage. Flock provides installation, ongoing maintenance, cellular service, and software updates as part of its subscription model.

2. Purpose (BMC 2.99.020(3)(b))

The proposed purpose for the Flock Safety Condor cameras is to provide real-time awareness and investigative capacity in following use cases:

- To support specific and active criminal investigations.
- To support serious traffic-related investigations.
- To support police misconduct investigations, and
- To respond to and review critical incidents or natural disasters.

3. Location (BMC 2.99.020(3)(c))

The cameras are proposed for deployment adjacent to the following intersections, chosen for high pedestrian traffic and analysis of crime trends:

- | | |
|-------------------|----------------------------|
| • Center / MLK | • College / Ashby |
| • Milvia / Alston | • 9 th / Gilman |

Page 6 of 18

- Center / Shattuck
- University / Shattuck
- Cedar / Shattuck
- Durant / Telegraph
- 4th / Virginia
- University / MLK
- Solano / Colusa
- 4th / Hearst
- Adeline / Fairview
- Shattuck / Ashby
- 62rd / King
- College / Alcatraz

Additional potential locations if funding allows include Ashby Ave / Domingo Ave, Ashby Ave / San Pablo Ave, Dwight Ave / San Pablo Ave, and University Ave / San Pablo Ave. This plan reallocates previously approved locations now covered by ALPRs or facing installation barriers.

4. Impact (BMC 2.99.020(3)(d))

- The deployment aims to enhance public safety and aid investigations.
- As with any surveillance, there is a potential impact on privacy and civil liberties, specifically the expectation of anonymity in public spaces. The cameras will capture video of public areas with high foot traffic.
- Concerns regarding potential disparate impacts on specific communities are acknowledged. Mitigation measures (Section 5) and adherence to a strict Use Policy are intended to prevent discriminatory use.
- Safeguarding privacy from potential misuse, particularly concerning federal immigration enforcement, is critical. Protections include state law (e.g., SB 54 prohibits sharing certain information for federal immigration enforcement), alignment of BPD policy with state law, Flock's terms forbidding such sharing, and prompt notification procedures if federal access is requested.
- The technology provider, Flock Safety, states its video cameras do not use facial recognition technology. Berkeley city policy explicitly prohibits the use of facial recognition technology.

5. Mitigation (BMC 2.99.020(3)(e))

- A comprehensive Surveillance Use Policy specific to this technology is in place and enforced (Policy 1304), outlining authorized uses, data handling, retention, and oversight, consistent with BMC 2.99.020(4).
- Use will comply with California SB 54, prohibiting data sharing for federal immigration enforcement. Flock's Terms of Agreement also forbid sharing data with federal immigration agencies. The City will be notified if federal authorities request access, allowing for intervention and oversight.
- Data access will be restricted to authorized personnel via secure login credentials managed by the City. Audit trails will log all access. Role-based access controls are available to manage least privilege.
- Data will be encrypted during transmission (TLS 1.2+) and storage (AES-256) to mitigate cybersecurity risks and prevent unauthorized third-party access. Data is stored on AWS GovCloud meeting strict governmental security standards.
- Data will be retained for a limited period pursuant to the Department Use Policy, and automatically deleted thereafter using secure methods compliant with NIST 800-88 to reduce risks associated with unauthorized use.

- The technology will not be used for facial recognition or to unlawfully discriminate based on protected characteristics. The cameras will not be used for automated traffic enforcement.
- Signage will be posted in areas where cameras are deployed. This report and the subsequent Use Policy will be public documents.
- Using solar-powered cameras minimizes infrastructure impact and reliance on grid power at specific pole locations.

6. Data Types and Sources (BMC 2.99.020(3)(f))

- High-definition video recordings of public spaces. Associated metadata including date, time, and camera location. AI-derived alerts for human presence (without identification) or vehicle characteristics (if integrated with ALPR features).
- Video feeds directly from the Flock Safety Condor cameras affixed to City-owned poles or other suitable infrastructure in public rights-of-way. The system may integrate data/alerts from the City's existing Flock ALPR system.

7. Data Security (BMC 2.99.020(3)(g))

Flock Safety describes a multi-layered security architecture prioritizing encryption, data protection, and compliance. Key aspects include:

- Flock states its practices align with principles in the FTC Safeguards Rule and comply with frameworks like NIST CSF, NIST 800-53 Rev 5, and holds ISO 27001 certification.
- Flock employs dedicated security teams (Product Security, Corporate Security, Risk/Compliance) including a CISO and professionals with CISSP and CIPP certifications.
- Regular risk assessments (annual, utilizing NIST frameworks) are conducted, prioritized threats are tracked, and cyber threat intelligence is monitored. Quarterly security reviews and board transparency ensure oversight.
- Data is encrypted in transit (TLS 1.2+ or higher) and at rest (AES-256).
- Data is stored in Flock Safety's secure cloud environment (AWS, including AWS GovCloud for CJIS data accessible only by Law Enforcement), leveraging geographic redundancy and robust backup policies.
- Role-based access controls (RBAC) enforce least privilege for both customer administrators and Flock personnel. Access is centrally managed via an identity provider, reviewed quarterly.
- Multi-Factor Authentication (MFA) is required for privileged access and recommended for all users (supported methods include authenticator apps, SMS, customer SSO). SSO technologies (Azure AD, Okta, SAML) are supported.
- Regular security assessments (including OWASP checks, vulnerability scanning) are performed on in-house and third-party applications. Advanced tooling monitors platform, container, endpoint, and network security.
- Hardware/software inventories are actively managed. A formal SDLC process (Agile, GitHub for source code, Jira for tracking) governs changes, with mandatory reviews, testing, separation of environments, and infrastructure management via Terraform.
- Data is automatically deleted after the retention period pursuant to policy using secure methods (e.g., cryptographic wiping) aligned with NIST 800-88 guidelines.

- Continuous monitoring (including SIEM) detects unauthorized access attempts, security events, and logs privileged user access.
- Comprehensive security awareness training is mandatory for all personnel upon hire, annually, and for significant changes, covering policies, incident response, and role-specific duties.
- Flock undergoes regular third-party assessments including SOC 2 Type II (annually), ISO 27001 certification, and CJIS ACE compliance assessment. A formal third-party risk management program vets vendors integrated with Flock products.
- Flock maintains a documented incident response plan that is tested quarterly and reviewed annually, defining roles, responsibilities, and procedures for handling breaches.

8. Fiscal Impact (BMC 2.99.020(3)(h))

- Flock Safety cameras are priced as a subscription service at \$5,000 per camera per year. For the 16 proposed cameras, the annual cost is \$80,000. This includes installation, maintenance, data hosting, cellular connectivity, and software updates.
- The FY 2024 baseline Public Works budget allocated \$600,000 for external cameras. \$290,000 was disbursed to the previous vendor, Edgeworth; the City aims to reassign these funds to other projects. The remaining \$310,000 is sufficient to cover over four years of operating costs for the 16 Flock cameras. Recovering the \$290,000 could fund an additional four years.
- Ongoing costs include City staff time for system administration, oversight, auditing, and reporting, similar to the previous system. Specific costs are TBD but covered within existing departmental budgets.
- The City intends to seek grant funding to potentially offset purchase/subscription costs.

9. Third Party Dependence and Access (BMC 2.99.020(3)(i))

- The City will depend on Flock Safety for the camera hardware, the FlockOS software platform, cellular data transmission, cloud storage, system maintenance, and software updates. This is inherent in the subscription model.
- Flock Safety handles and stores the data on its cloud platform.
- The City owns the data. Flock Safety states it will not share or sell customer data. Access to the data by third parties (including Flock Safety personnel) is controlled by the City through permissions managed within the FlockOS platform. Any data sharing with other entities (e.g., other law enforcement agencies) would be governed by Berkeley PD's Surveillance Use Policy and applicable laws.
- The City's contract with Flock Safety will require the company to provide prompt notification of any data request from a federal agency. Flock will not release data unless legally compelled to do so by federal law, and in such cases, will provide the City with advance notice to the greatest extent possible before complying.

10. Alternatives (BMC 2.99.020(3)(j))

- Continuing with the originally approved vendor, Edgeworth Integration, was considered but deemed infeasible due to insurmountable technical challenges related to power requirements at proposed locations and installation delays.

Page 9 of 18

- Relying solely on traditional policing techniques (e.g., increased officer patrols) is an alternative but does not provide the persistent monitoring or video evidence capabilities offered by cameras.
- Deciding against deploying fixed video surveillance cameras altogether.

11. Experience of Other Entities (BMC 2.99.020(3)(k))

- Many cities, including neighboring jurisdictions like San Francisco, Oakland, and San Jose, utilize fixed surveillance cameras as a tool for public safety and crime deterrence, often with their own specific use policies.
- Flock Safety systems (including LPR and video) are used by numerous law enforcement agencies nationally. These agencies often cite benefits in investigations and situational awareness.

External Fixed Video Surveillance Cameras

351.1 PURPOSE AND SCOPE

This policy provides guidance for the placement and monitoring of City of Berkeley external fixed video surveillance cameras by the Berkeley Police Department (BPD).

This policy only applies to fixed, overt, marked external video surveillance systems utilized by the BPD. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Department, as authorized by the City Council for use by other City Departments. BPD Personnel shall adhere to the requirements for External Fixed Video Surveillance Cameras covered in this policy as well as the corresponding Surveillance Use Policy -1304.

351.2 POLICY

The Berkeley Police Department utilizes a video surveillance system to enhance its anti-crime strategy, to effectively allocate and deploy personnel, and to enhance safety and security in public areas. As specified by this policy, cameras may be placed in strategic locations throughout the City to record, deter, and solve crimes, to help the City safeguard against potential threats to the public, and to help manage emergency response situations during natural and human-made disasters, among other uses specified in Section 351.3.1.

Video surveillance in public areas will be conducted in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

351.3 OPERATIONAL GUIDELINES

Only City Council-approved video surveillance equipment shall be utilized. BPD members authorized to review video surveillance may only record and review public areas and public activities where no reasonable expectation of privacy exists and pursuant to Section 351.3.1. The City Manager shall obtain Council approval of any proposed additional locations for the placement and use of video surveillance technology.

351.3.1 PLACEMENT REVIEW AND MONITORING

Camera placement will only occur in locations approved by the City Council and will be guided by this policy and the underlying purpose or strategy associated with the overall video surveillance plan. As appropriate, the Chief of Police should confer with other affected City departments when evaluating camera placement. Environmental factors, including lighting, location of buildings, presence of vegetation or other obstructions, should also be evaluated when determining placement.

Camera placement includes existing cameras such as those located at San Pablo Park, the Berkeley Marina, and cameras placed in Council identified and approved intersections throughout the City, and potential future camera locations as approved by City Council.

Current City Council approved locations:

Page 11 of 18
Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

- 6th Street at University Avenue
- San Pablo Avenue at University Avenue
- 7th Street at Dwight Way
- San Pablo Avenue at Dwight Way
- 7th Street at Ashby Avenue
- San Pablo Avenue at Ashby Avenue
- Sacramento Street at Ashby Avenue
- College Avenue at Ashby Avenue
- Claremont Avenue at Ashby Avenue
- 62nd Street at King Street

The cameras shall only record video images and not sound. Recorded images pursuant to Section 351.5 may be accessed, reviewed, and used for specific criminal or BPD administrative investigations and video surveillance may be accessed and reviewed by authorized BPD personnel for the following purposes:

- (a) To support specific and active criminal investigations.
- (b) To support serious traffic-related investigations.
- (c) To support police misconduct investigations, and
- (d) To respond to and review critical incidents or natural disasters.

Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.

351.3.2 FIXED CAMERA MARKINGS

All public areas monitored by video surveillance equipment shall be marked in a conspicuous manner with unobstructed signs to inform the public that the area is under police surveillance.

351.3.3 INTEGRATION WITH OTHER TECHNOLOGY

The Department is prohibited from integrating or accessing system capabilities of the video surveillance system with other systems, such as gunshot detection, automated license plate recognition, facial recognition and other video-based analytical systems.

351.4 VIDEO SUPERVISION

Access to video surveillance camera data shall be limited to Berkeley Police Department (BPD) personnel utilizing the camera database for uses authorized above, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with Sections 351.6 or 1304.9 below. BPD members seeking access to the camera system shall obtain the approval of the Investigations Division Captain, or their designee.

Page 12 of 18
Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

Supervisors should monitor video surveillance access and usage to ensure BPD members are complying with this policy, other applicable department policy, and applicable laws. Supervisors should ensure such use and access is appropriately documented.

351.4.1 VIDEO LOG

No one without authorization will be allowed to login and view the recordings. Those who are authorized and login should automatically trigger the audit trail function to ensure compliance with the guidelines and policy.

351.4.2 PROHIBITED ACTIVITY

Video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Video surveillance systems shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.

Video surveillance systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

351.5 STORAGE AND RETENTION OF MEDIA

Video surveillance recordings are not government records pursuant to California Government Code 34090 in and of themselves. Except as otherwise permitted in this section, video surveillance recordings shall be purged within one hundred and eighty (180) days of recording. Recordings of incidents involving use of force by a police officer or involving, detentions, arrests, or recordings relevant to a formal or informal complaint against a sworn police officer shall be retained for a minimum of two years and one month. Recordings relating to court cases and complaints against BPD sworn officers that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to a police misconduct investigation shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Any recordings needed as evidence in a criminal or police misconduct proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

351.5.1 EVIDENTIARY INTEGRITY

All media downloaded and retained pursuant to this Policy shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to

Page 13 of 18
Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

351.6 RELEASE OF VIDEO IMAGES

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law, also referenced in Policy 1304.8.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records pursuant to Policy 804, Records Maintenance and Release.

Requests for recorded video from other law enforcement agencies shall be referred to the Investigations Division Captain, or their designee for release in accordance with this policy and must be related to a specific active criminal investigation.

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 25, Subdivision (20)(a).

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

351.7 VIDEO SURVEILLANCE AUDIT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. System audits will be conducted by the Office of Strategic Planning and Accountability on a regular basis, at least biennial.

BPD will enforce against prohibited uses of the cameras pursuant to Policy 1010, Personnel Complaints, or other applicable law or policy. The City Manager shall enforce against any prohibited use of cameras and/or access to data by other City of Berkeley personnel.

The audit shall be documented in the form 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 published on the City of Berkeley website in an appropriate location, and retained within the Office of Strategic Planning and Accountability.

351.8 TRAINING

All department members authorized to operate or access video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy, as well as review of relevant City of Berkeley laws and regulations. Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized

Page 14 of 18
Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804, Records and Maintenance.

351.9 MAINTENANCE

It shall be the responsibility of the Public Works Director to facilitate and coordinate any updates and required maintenance, with access limited to that detailed in the City Manager's promulgated policies.

Surveillance Use Policy-External Fixed Video Surveillance Cameras

1304.1 PURPOSE

This policy provides guidance for the use of City of Berkeley external fixed video surveillance cameras by the Berkeley Police Department (BPD).

This policy only applies to fixed, overt, marked external video surveillance systems utilized by BPD. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Department. Department personnel shall adhere to the requirements for External Fixed Video Surveillance Cameras covered in this policy as well as the corresponding Use Policy-351.

This Surveillance Use Policy is legally-enforceable pursuant to BMC 2.99.

1304.2 AUTHORIZED USE

Only BPD members who receive training on this policy, who are then granted access by an administrator may access the data from the video surveillance cameras. This data may only be accessed to further a legitimate law enforcement purpose, as listed in this Policy. Members must follow the necessary logging mechanisms, such as case number and case type when querying the database.

The cameras shall only record video images and not sound. Recorded images pursuant to Section 351.5 may be accessed, reviewed, and used for specific criminal or BPD administrative investigations and video surveillance may be accessed and reviewed by authorized BPD personnel for the following purposes:

- (a) To support specific and active criminal investigations.
- (b) To support serious traffic-related investigations.
- (c) To support police misconduct investigations, and
- (d) To respond to and review critical incidents or natural disasters.

Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.

The following are prohibited uses of the video surveillance system:

- (a) Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.
- (b) Video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.
- (c) Video surveillance systems shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Page 16 of 18
Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

- (d) Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.
- (e) Video surveillance systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

1304.3 DATA COLLECTION

The cameras will film and store video on City of Berkeley encrypted servers. License plate and facial recognition data hardware is not installed on the cameras and may not be installed or used unless approved by the City council. Audio is a standard feature of the camera, but is deactivated by the system administrator and may not be activated or used unless approved by the City Council. The cameras and storage devices shall be wholly owned and operated/maintained by the City of Berkeley.

1304.4 DATA ACCESS

Access to video surveillance cameras data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to Use Policy 351, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with 1304.9 below. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee.

Supervisors should monitor camera access and usage to ensure BPD members are complying with this policy, other applicable department policy, and applicable laws. Supervisors should ensure such use and access is appropriately documented.

1304.5 DATA PROTECTION

All data transferred from the cameras and the servers shall be encrypted. Access to the data must be obtained through the Public Works Department according to this policy and published regulations that limit access and use of data by Public Works and other City Departments and personnel. All system access including system log-in, access duration, and data access points is accessible and reportable and shall be documented by the Public Works Department's authorized administrator. All relevant recordings that are utilized will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804 Records and Maintenance.

1304.6 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. Provisions of this policy, including 1304.4 Data Access, 1304.5 Data Protection, 1304.7 Data Retention, 1304.8 Public Access and 1304.9 Third Party Data Sharing serve to protect against any unauthorized use of video

Surveillance Use Policy-External Fixed Video Surveillance Cameras

surveillance camera data. License plate and facial recognition data hardware is not installed on the cameras. Audio is a standard feature of the camera, but is deactivated by the system administrator. These procedures 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.

1304.7 DATA RETENTION

Video surveillance recordings are not government records pursuant to California Government Code 34090 in and of themselves. Except as otherwise permitted in this section, video surveillance recordings shall be purged within one hundred and eighty (180) days of recording. Recordings of incidents involving use of force by a police officer or involving detentions, arrests, or recordings relevant to a formal or informal complaint against a police officer shall be retained for a minimum of two years and one month. Recordings relating to court cases and complaints against BPD sworn officers that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to BPD administrative proceedings pursuant to this section shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court. All data will automatically delete after the aforementioned retention period by the System Administrator from Public Works.

Any recordings needed as evidence in a criminal or police misconduct proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

1304.8 PUBLIC ACCESS

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records pursuant to Policy 804.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

1304.9 THIRD-PARTY DATA-SHARING

Requests for recorded video from other law enforcement agencies shall be referred to the Investigations Division Captain, or their designee for release in accordance with this policy, and must be related to a specific active criminal investigation.

Data collected from the video surveillance system may be shared with the following:

- (a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- (b) Other law enforcement personnel as part of an active criminal investigation;

Page 18 of 18
Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

- (c) Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 125, Subdivision (20)(a).

1304.10 TRAINING

All BPD members authorized to operate or access video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy as well as review of relevant City of Berkeley laws and regulations.

Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized will be collected pursuant to Policy 802 Property and Evidence, and retained pursuant to Policy 804 Records Maintenance.

1304.11 AUDITING AND OVERSIGHT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. Video surveillance system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biennial.

BPD will enforce against prohibited uses of this policy pursuant to Policy 1010, Personnel Complaints or other applicable law or policy. The City Manager shall enforce against any prohibited use of the cameras and/or access to data by other City of Berkeley personnel.

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 placed into the annual report filed with the City Council pursuant to BMC Section 2.99.020 2. d., published on the City of Berkeley website in an appropriate location, and retained within the Professional Standards Bureau.

1304.12 MAINTENANCE

It shall be the responsibility of the Public Works Department to facilitate and coordinate any updates and required maintenance with access limited to that detailed in the City Manager's promulgated policies.

OFF-AGENDA 1
Policy Review Status Updates

Updated September 29, 2026



POLICY REVIEW STATUS REPORT

Guiding Authority

Section 125(3)(a)(1) and Section 125(17)(a) of the Berkeley City Charter¹

Case Load Overview

As of September 9, 2026, the Police Accountability Board (PAB) has two (2) active policy reviews. Since then, the ODPa has received three (3) additional policy complaints that it is currently assessing before presentation to the PAB.

Policy Review Number	2025-PR-0001
Policy Topic	Contact Between Complaint Subject Officer and Complainant During Calls for Service
Relevant Policy	BPD Policy 1004 "Anti-Retaliation" BPD Policy 1010 "Personnel Complaints"
Status	Open
Date Presented to the PAB	02/19/2025
Anticipated Completion	The review is currently being evaluated to determine the appropriate next steps and timeline for completion.
Assigned To	Chair Cayetano & Board Member Sharma
Summary	
The Complainant reported two interactions with BPD in January 2025, involving officers who were either subjects of their prior complaints to the PAB or involved in other litigation. They expressed concerns about potential retaliation or bias, believing they should not interact with officers they had previously filed complaints against.	
Activity Report	
On September 9, 2026, this policy review was reassigned to Chair Cayetano and Board Member Sharma. ODPa staff has transmitted the material relevant to the review.	

¹ Berkeley City Charter: <https://berkeley.municipal.codes/Charter/125>

Updated September 29, 2026

Policy Review Number	2025-PR-0004
Policy Topic	Public Recording of Police Activity
Relevant Policy	BPD Policy 426 "Public Recording of Police Activity"
Status	Open
Date Presented to the PAB	6/25/2025
Anticipated Completion	The review is currently being evaluated to determine the appropriate next steps and timeline for completion.
Assigned To	ODPA
Summary	
The Complainant expressed concerns with the Berkeley Police Department's General Order D-2, "Public Recording of Police Activity," (now BPD Policy 426) following an incident on June 4, 2025, in which they allege they were physically prevented by three officers from observing and documenting police activity at 8th and Harrison Street. The Complainant argues that the policy fails to clearly affirm the First Amendment rights of onlookers and does not adequately direct officers to limit the use of "police lines" to situations where such restrictions are necessary for officer safety or to protect the integrity of an investigation.	
Activity Report	
On September 23, 2026, the policy complaint was reassigned to ODPA staff after the scope of the review was reevaluated. The PAB requested that PAB complete the review within the next six months per the guidance in its policy manual.	

Attachments:

- Policy Complaint 2026-PR-0002
- Policy Complaint 2026-PR-0003
- Policy Complaint 2026-PR-0004

Policy/Practice/Procedure Form



Tracking Number ODPa-260922-497446

Created by - | 09/22/2026 | Version 1

Case Details (Version 1)

Personal Information

Basic Information

Email

First Name

Last Name

Phone

File Anonymously Yes

Work Telephone

Mailing Address

Street name

Apt/Unit

State California

City

Zip Code

Occupation

Demographics

Please provide as many details about the incident as possible. Your recollection about the incident is invaluable.

Date of Birth

Ethnicity

Race

Gender

Incident Details

Statement

I just saw in TikTok ABC News' report regarding your police department letting a male individual who climbed a gate with a weapon while following a woman go free. You guys are irresponsible. I'm almost certain you guys have arrested people for less. That could've been my sister as I think about her college years there. It's sad. I'm sure if that happened to someone related to you all that you would have had a different interaction. Do better.

Location of Incident (if applicable)

Date of Incident (if applicable)

Time of Incident (if applicable)

What changes to BPD policy, practice, or procedure do you propose?

Additional Information

Use this space for any additional information you wish to provide about your complaint. (Or, attach relevant documentation you believe will be useful to the Police Accountability Board in evaluating your complaint.)

Upload Document

Incident External Links

How Did You Hear About Us

Policy/Practice/Procedure Form



Tracking Number **ODPA-260922-497446**

Created by - | 09/22/2026 | Version 1

Attachments

No attachments available for this case.

Policy/Practice/Procedure Form



Tracking Number **ODPA-260929-626156**

Created by - | 09/29/2026 | Version 1

Case Details (Version 1)

Personal Information

Basic Information

Email

First Name

Last Name

Phone

File Anonymously ☒ Yes

Work Telephone

Mailing Address

Street name

Apt/Unit

State

City

Zip Code

Occupation

Demographics

Please provide as many details about the incident as possible. Your recollection about the incident is invaluable.

Date of Birth

Ethnicity

Race

Gender

Incident Details

Statement

On 8/12/26 approx. 11:10-11:15am next to the PETS referral parking lot, a PEO was cleaning the parking meter by spraying it with a spray bottle. The mist from the bottle dissipated through the air surrounding the sidewalk causing it to hit my face as i walked by. First of all, I breathed and walked into unknown chemical substances sprayed inconsiderately by a public servant that landed on my facial skin.

Location of Incident (if applicable) next to the PETS referral parking lot near 1048 university ave

Date of Incident (if applicable) August 12, 2026

Time of Incident (if applicable) 11:10 AM

What changes to BPD policy, practice, or procedure do you propose? I propose not openly spraying chemicals when members of the public are nearby. if anyone is nearby, i suggest spraying into the towel then wiping the parking meter. Instead of covering the parking meter in a chemical mist that can catch the wind and get on people's skin and in their lungs. If this is already policy, please let me know so i can submit a complaint instead.

Additional Information

Use this space for any additional information you wish to provide about your complaint. (Or, attach relevant documentation you believe will be useful to the Police Accountability Board in evaluating your complaint.)

Upload Document

Incident External Links

How Did You Hear About Us

Policy/Practice/Procedure Form



Tracking Number **ODPA-260929-626156**

Created by - | 09/29/2026 | Version 1

Attachments

No attachments available for this case.

Policy/Practice/Procedure Form



Tracking Number **ODPA-260930-309224**

Created by - | 09/30/2026 | Version 1

Case Details (Version 1)

Personal Information

Basic Information

Email	[REDACTED]
First Name	[REDACTED]
Last Name	[REDACTED]
Phone	
File Anonymously	
Work Telephone	

Mailing Address

Street name	
Apt/Unit	
State	California
City	Berkeley
Zip Code	94704

Occupation

Demographics

Please provide as many details about the incident as possible. Your recollection about the incident is invaluable.

Date of Birth

Ethnicity

Race

Gender

Incident Details

Statement

On Monday, September 21, 2026 there was a car crash on Ashby and Fulton around 8am. I arrived to the Sylvia Mendez Elementary entrance gate on Fulton just in time to see a police car heading south on Fulton with lights and siren blaring. It was quickly followed by a second, both of which needed to go around the many cars queued up on Fulton for our Rolling Drop Off and enter an intersection staffed by our crossing guard and with families in the crosswalks. Then they had to pass the many families that bike on the Russell and Fulton Bike Boulevards and drop off at the Fulton entrance gate. It was a terrifying start to the school day and we are so fortunate that no one was injured by emergency vehicles speeding by our school during Drop Off time.

My first issue is local streets by schools should NOT be used as cut through for emergency responses - ESPECIALLY during drop off/pickup times but frankly anytime during the school day as it's disruptive to learning and can be emotionally disturbing to students. The fire truck that responded to this car crash correctly accessed the scene by using either Shattuck or Adeline to access the crash via Ashby.

Around 8:30am I headed down to Fulton and Ashby to observe the incident. Eastbound car traffic was blocked at Fulton so the drivers were rolling through the light (red and green) without regard to pedestrians and people on bikes to turn south onto Fulton. There was no one directing traffic and likely no one ensuring that all these cars heading off Ashby and onto local streets were driving safe. Two police vehicles were still at the scene.

So my second issue is that cars were then rolling through red lights with pedestrians in the crosswalk due to the lack of police enforcement and instructions at a closed intersection.

Location of Incident (if applicable) Ashby and Fulton

Date of Incident (if applicable) September 21, 2026

Time of Incident (if applicable) 08:30 AM

What changes to BPD policy, practice, or procedure do you propose? The community member wants two main changes:

- Emergency response routes that avoid school streets, especially during drop-off and pickup, and preferably throughout the school day. They suggest using major streets such as Shattuck or Adeline to reach incidents when possible.
- Active traffic control at intersections affected by collisions or closures, including officers directing diverted vehicles, enforcing traffic signals, and ensuring drivers yield to pedestrians and bicyclists.

Their broader concern is protecting children and families from both emergency vehicle traffic and unsafe driving caused by traffic diversions.

Additional Information

Use this space for any additional information you wish to provide

about your complaint. (Or, attach relevant documentation you believe will be useful to the Police Accountability Board in evaluating your complaint.)

Upload Document

Incident External Links

How Did You Hear About Us

Website

Policy/Practice/Procedure Form



Tracking Number **ODPA-260930-309224**

Created by - | 09/30/2026 | Version 1

Attachments

No attachments available for this case.

OFF-AGENDA 2

Legislative Updates Relevant to the PAB's Work



MEMORANDUM

Date: October 2, 2026
To: Honorable Members of the Police Accountability Board
From: Katherine Lee, Interim Director of Police Accountability
 Jose Murillo, ODPa Policy Analyst
Subject: Legislative Updates

The purpose of this memorandum is to provide a legislative update to the PAB, enabling them to stay informed about changes in local, state, and federal law.

State Legislative Updates¹

The following bills are being proposed in the state of California regarding peace officers:

NAME OF LEGISLATION	STATUS	SUMMARY/PURPOSE
AB 1537 (Bryan) – Peace Officers: Secondary Employment	09/09/26 - <i>Enrolled and presented to the Governor at 1 p.m.</i>	Prohibits peace officers from engaging in part-time or any other form of secondary employment for the United States (U.S.) Department of Homeland Security (DHS) or any other entity that engages in immigration enforcement
AB 1544 (Krell) – Court proceedings: media access	09/27/26 – <i>Approved by the Governor. Chaptered by Secretary of State - Chapter 520, Statutes of 2026.</i>	Clarifies and strengthens public access rights to court proceedings by prohibiting officials from restricting entry to open court settings—except as necessary to maintain order—makes violations enforceable under the Bane Act, and affirms that existing access rights are not limited or reduced.

¹ <https://post.ca.gov/Status-of-Current-Legislation>

AB 1627 (Avila Farias) - Public employment: disqualifications	09/09/26 - <i>Enrolled and presented to the Governor at 1 p.m.</i>	Disqualifies a person previously employed by the United States Immigration and Customs Enforcement (ICE) or specified out-of-state corrections departments, during specified time periods, from being employed as a peace officer
AB 1896 (Gonzalez) – Public employment: disqualifications	09/14/26 - <i>Enrolled and presented to the Governor at 1:30 p.m.</i>	Amends various existing laws relating to disqualification from public employment, minimum standards relating to peace officers, and adds certain criteria for an individual employed by an entity that engaged in immigration enforcement on or after January 20, 2025, to January 20, 2029, except as provided, among other provisions.
AB 2347 (Ahrens) – Commission on Peace Officer Standards and Training: hate crime training and guidelines	05/14/2026 - <i>In committee: Held under submission.</i>	Requires the Peace Officer Standards and Training Commission (POST) to conduct a comprehensive review of hate crimes training programs and adopt evidence-based training requirements to fill any gaps in the handling of hate crimes, as specified.
SB 691 (Wahab) – Body-worn cameras: policies	09/20/26 - <i>Approved by the Governor. Chaptered by Secretary of State. Chapter 416, Statutes of 2026.</i>	This bill requires, on or before July 1, 2027, each law enforcement agency that has a body-worn camera policy to update that policy to include a procedure for emergency service personnel to request, prior to any public release, the redaction of evidentiary and nonevidentiary recordings of a patient undergoing medical or psychological evaluation, procedure, or treatment by emergency service personnel.
SB 1105 (Perez) – Law Enforcement	09/03/26 - <i>Enrolled and presented to the Governor at 3 p.m.</i>	Current law grants limited arrest authority—and in some cases peace officer status—to federal law enforcement under specific conditions. This bill removes those authorities and prohibits California agencies from participating in joint task forces involving profiling, while requiring

	Attorney General approval and compliance standards for interagency agreements.
--	--

Additional legislation pertaining to public safety in the state of California may be monitored here: <https://legiscan.com/CA/legislation> . ODPa staff will continuously monitor new legislation and update the PAB throughout the year.

The BPD’s Policy and Training Bureau issues an annual legislative update that summarizes legal changes impacting law enforcement. Unless stated otherwise, the changes outlined in the updates took effect in January of the corresponding year. The following BPD Policies include the legislative updates for 2026.

SOURCE	LINK
BPD Policy 1507 “2026 Legislative & Case Law Update”	https://berkeleyca.gov/sites/default/files/2026-02/RELEASE_20260127_T171031_Berkeley%20PD%20Policy%20Manual.pdf#Page=1061
The California Peace Officers Association also provides a yearly California Legislative and Legal Digest.	https://cpoa.org/wp-content/uploads/2024/11/2025-Legislative-Legal-Digest.pdf

Lexipol Policy Updates

The following Lexipol policies have been updated since the PAB’s September 23, 2026 meeting:

BPD POLICY	DESCRIPTION OF CHANGES
1308 “Surveillance Use Policy – Mutual Aid Air Support”	This new policy was implemented following the City Council’s September 29, 2026 approval of the surveillance technology ordinance submission for mutual aid air support. It provides guidance on BPD’s request, receipt, and use of mutual aid air support.
418 “Obtaining Air Support”	Revised air support policy to authorize requests through the Watch Commander/designee, update permitted uses, add prohibited uses and data-sharing restrictions, require written deployment notifications/reporting,

	establish training requirements, and reference Policy 1308.
--	---

Berkeley City Council & Council Committee Meeting Updates

The following items are under consideration by the City Council or its committees and are relevant to the PAB:

October 13, 2026 Regular City Council Meeting

Item #	Item Description	Recommendation
1	Amendment to BMC Chapter 2.99 to Establish Surveillance Technology Vendor Accountability Requirements and to Revise the Annual Surveillance Technology Reporting Schedule	Adopt the second reading of Ordinance No. 8,033-N.S. amending BMC Chapter 2.99 to require enforceable violation, sanction, and termination provisions in surveillance technology vendor agreements; revise the annual Surveillance Technology Report schedule; and conform references to the Police Accountability Board.
17	Homeless Response Team Audit Status Report	Information Report. Provides an update on implementation of recommendations from the July 2025 Homeless Response Team audit, including encampment coordination, outreach/data tracking, and public reporting.

OFF-AGENDA 3

List of Remaining 2026 PAB Meetings

Remaining 2026 Police Accountability Board Meetings

City of Berkeley – Police Accountability Board

The following are the remaining scheduled Police Accountability Board meetings for calendar year 2026, based on the 2026 PAB Meeting Calendar.

Meeting Date
October 7, 2026
October 21, 2026
November 4, 2026
December 9, 2026