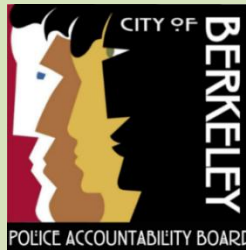


Page numbers for this agenda packet are marked in **blue** to distinguish them from the numbering within individual documents.

PUBLIC MEETING MATERIAL



**POLICE ACCOUNTABILITY BOARD
REGULAR MEETING AGENDA PACKET**

COMMUNICATIONS TO THE PAB

**September 23, 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

Communications

Item	Description
9.C.	1. September 19, 2026 Communication from Secure Justice Regarding "BPD Flock Audit – January through June 2026" 2. September 21, 2026 Communication from Kitt Saginor to the PAB Regarding "Item 9.c. on September 23 rd – ALPR Audit"

Communication 1

**September 19, 2026 Communication from Secure Justice
Regarding "BPD Flock Audit – January through June 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

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

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.)

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.

- 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.

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

Communication 2

**September 21, 2026 Communication from Kitt Saginor to the
PAB Regarding “Item 9.c. on September 23rd – ALPR Audit”**

Murillo, Jose

From: Kitt Saginor [REDACTED]
Sent: Monday, September 21, 2026 9:16 PM
To: Murillo, Jose
Cc: Joshua Cayetano; Office of the Director of Police Accountability
Subject: Item 9.C. on September 23rd - ALPR Audit

Follow Up Flag: Follow up
Flag Status: Flagged

WARNING: This is not a City of Berkeley email. Do not click links or attachments unless you trust the sender and know the content is

Dear Police Accountability Board,

I am concerned that the Flock Automated License Plate Reader Audit January 2026 - June 2026 being presented to you as Item 9.c is of little value for assuring proper access and usage of Berkeley's data as collected by Flock.

Please think about the common ways in which misuse of data from Flock cameras has occurred and has been reported:

1. Persons who were authorized to have access transferred data to ICE personnel or other persons not authorized to have access.
2. Searches targeted vulnerable populations.
3. Searches targeted individuals for illegal reasons: e.g. partners or estranged partners, women seeking reproductive care, persons exercising first amendment rights, etc.
4. Scope of access. was not restricted in accordance with agreements, because Flock changed access or software functionality without alerting agencies.

Does the audit as described in 9.A provide assurance that Berkeley's data has not been misused in THESE ways?

Objective 1: BPD - Authorized Access

This criteria confirms that all users are required to have individual credentials, but it does not determine whether data obtained by an authorized user was subsequently transferred to an unauthorized user. It does not confirm that logins were used ONLY by the person authorized - that login information has not been stolen or shared.

Objective 2: BPD - Permitted uses.

This finding only confirms BPD personnel used permissible terms, it does NOT rule out that the possibility that permissible terms may have been used dishonestly to while targeting individuals for illegal reasons, or that vulnerable populations were targeted using language that concealed impermissible intentions.

Verifying alignment for 100 searches is not a significant check if that is a small percentage of searches conducted.

Objective 3: External - Authorized Access

This finding also does not assess the possibility of searches being conducted on behalf of Federal or out-of-state agencies by personnel who may have access to our data - a group of 45 law enforcement agencies, most of which are NOT Sanctuary Cities.

It does not assess the security of servers that are NOT under the control of Berkeley but on which Berkeley's data resides.

It does not address the fact that Flock sends images overseas to gig workers hired to "train" the AI.

It does not ascertain whether the software created, owned, and maintained by Flock Safety allows access to data through some alternate procedure that does not log queries.

Also not mentioned in the audit, although acknowledged in contract language with Flock, is the fact that Federal agents can use legal tools (such as FISA) to access Berkeley's data without notification.

Objective 4: External - Permitted Uses

The criteria states that prohibited federal agencies are those associated with immigration enforcement, such as ICE and CBP, but it does not recognize that actions in support of the assault on immigrants are widespread throughout the Federal government, including the State Department (whose Diplomatic Security Service abducted a Berkeley resident at Woolsey & Telegraph on July 9th), Health and Human Services, and the Department of Justice.

The findings fail to note that absence of specific terms does not preclude violations of policy. Authorized personnel may have used permissible terms dishonestly for searches that were conducted for impermissible reasons.

The findings mention the use of Flock's audit assistance tools, but the tools are not described or assessed.

For all of these reasons, item 9.c does NOT provide assurance that Berkeley's Flock data is accessed and used only in accordance with law and Berkeley's policies.

It is especially puzzling to me that a police department would accept audit findings which require an assumption that bad actors will choose tell-tale terms that reveal their intentions when they intentionally misuse technology.

Thank you for your work on behalf of Berkeley

Kitt Saginor



References

Chad Marlow, Jay Stanley. "Flock Safety Credibility Lost as it Repeatedly Lies to City Councils, Police Departments, and Public Across the Country." *ACLU News & Commentary*, July 2, 2026 <<https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/flock-safety-credibility-lost-as-it-repeatedly-lies-to-city-councils-police-departments-and-public-across-the-country>>

Jason Koebler, Joseph Cox. "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows" *404 Media*, May 27, 2025 <<https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/>>

Roque Planas. "San Jose Officer Fired for Misusing Flock Camera Database in Domestic Abuse Case." *The Guardian*, September 13, 2026 <<https://www.theguardian.com/us-news/2026/sep/13/san-jose-officer-fired-flock-camera-misuse>>

Joseph Cox. "Flock Uses Overseas Gig Workers to Build Its Surveillance AI." *Wired*, December 1, 2025 <<https://www.wired.com/story/flock-uses-overseas-gig-workers-to-build-its-surveillance-ai/>>

Alex N. Gecan and Vanessa Arredondo. "ICE Seizes Person in Berkeley in Operation in which Little is Known." *Berkeleyside*. July 16, 2026. <<https://www.berkeleyside.org/2026/07/16/ice-state-department-run-immigration-operation-in-berkeley-behind-cops-backs>>

Alexandra Villarreal. "Trump Ally Stephen Miller Leads Sweeping Push to Accelerate Removal of Migrant Children." *The Guardian*, September 19, 2026 <<https://www.theguardian.com/us-news/2026/sep/19/stephen-miller-trump-migrant-children>>

Lorenzo Franceschi-Bicchierai. "Flock Says Its New Tool Will Help Identify Police Abuse, But Hasn't Explained How It Works." *TC TechCrunch*, August 13, 2026 <<https://techcrunch.com/2026/08/13/flock-says-its-new-tool-will-help-identify-police-abuse-but-hasnt-explained-how-it-works/>>