City of Burbank

Flock Safety Automated License Plate Reader Use

Information Guide and Frequently Asked Questions

Executive Summary

The Burbank Police Department (BPD) recognizes that the use of Automatic License Plate Reader (ALPR) technology, particularly systems provided by Flock Safety, has generated public discussion and concern nationwide. We take these concerns seriously and believe transparency is essential. BPD utilizes Flock Safety technology, specifically fifty-seven (57) Falcon ALPR cameras to support public safety operations. Recent national reporting and public discourse regarding automated surveillance, data sharing, and alleged misuse of Flock systems in other jurisdictions have prompted questions from our community.

This document is intended to provide the public with a clear explanation of the configuration, governance, auditing, and use restrictions of Flock Safety technology in the City of Burbank and to identify the safeguards in place to ensure compliance with California law, City policy, and community expectations concerning privacy and civil liberties.

Overview of Burbank's Flock Safety Deployment

BPD currently utilizes Flock Safety technology consisting of 57 Falcon Automatic License Plate Reader cameras operating under an annual subscription aligned with the City's fiscal year. The technology is deployed within public-rights-of way and is used solely as a law enforcement investigative and situational awareness tool to support the city's public safety efforts. It is important to note that these tools are not intended, nor can they be used, for generalized or continuous monitoring of individuals. BPD does not utilize Flock's Pan-Tilt-Zoom (PTZ) Condor cameras, commonly known as "PTZ" cameras, which are capable of actively monitoring large areas.

Purpose and Benefits of the Technology

Flock Safety technology supports public safety operations by assisting BPD in recovering stolen vehicles, identifying suspect vehicles associated with criminal activity, locating missing or at-risk persons, and confirming or eliminating investigative leads using time-stamped and location-based data.

In addition, the visible presence of ALPR technology serves as a deterrent to criminal activity. When individuals engaged in criminal behavior are aware that vehicle movements may be documented, the likelihood of repeat offenses and organized criminal activity in residential and business areas is reduced. Statewide jurisdictions in California utilize Flock Safety Technology, including a dense regional deployment, that creates a network effect which enhances law enforcement's ability to identify important evidence and ultimately locate and arrest out-of-town offenders.

Public Concerns and National Criticism of Flock Safety

Public concerns raised nationally regarding automated surveillance technology include potential misuse of ALPR data, voluntary data sharing with federal agencies, insufficient oversight, and participation in nationwide data-sharing networks without adequate safeguards. These concerns have informed BPD's system configuration and oversight practices.

Contractual and Legal Safeguards

BPD's agreement with Flock Safety and the Department's ALPR Policy requires strict compliance with California law, including the California Values Act codified at Government Code sections 7284 through 7284.12 (SB 54), as well as California Civil Code section 1798.90.5 et seq. (SB 34) governing the use of automated license plate recognition systems. In addition, BPD has adopted a restrictive Department-wide policy (# 462)[1] and procedure-focused approach grounded in California law, policy, and active oversight. BPD conducts ongoing reviews and audits of ALPR data use to confirm that no federal or out-of-state entities have unintended or improper access to ALPR data.

The agreement includes legally binding protections. Flock Safety is prohibited from sharing City data with federal agencies or non-California law enforcement agencies absent a valid court order or subpoena. All use of ALPR data must comply with the California Values Act, which prohibits the use of local resources to assist federal immigration enforcement except in narrow circumstances expressly authorized by state law. Comprehensive audit logging, along with a valid search request, is required for all access, searches, and activity within the system. Data retention limits are enforced through system configuration. It is important to note that the City of Burbank retains ownership and complete control of all data.

Data Retention Policies

Consistent with the BPD ALPR Policy 462 and California Civil Code section 1798.90.5, data retention periods are narrowly defined and enforced through system configuration and audit controls.

ALPR Data

ALPR data is retained for a period of thirty (30) days and data is automatically deleted upon expiration of the retention period unless it has been preserved pursuant to policy or as evidence related to an active criminal investigation.

[1] https://public.powerdms.com/BBKPD/tree/documents/319229

Access Controls and Authorized Users

Who May Access the System

Only authorized personnel with assigned roles may access Flock Systems. Access is granted based on job function and operational need, and only after department-approved training has been completed.

Personal or non-investigative use is strictly prohibited.

Training

Authorized users receive training on lawful use, privacy protections, and BPD's policy.

Auditing, Oversight, and Accountability

Every search and access event is logged with user identification and time stamps. Searches must be conducted for official police purposes and documented with a case or reference number and the reason for the search. Supervisory audits are conducted to identify improper or unauthorized use. Misuse would be treated similarly to the misuse of other criminal justice databases (e.g., CLETS or DMV).

Misuse of ALPR access to assist federal immigration enforcement, which is strictly prohibited under state law, is equivalent to unauthorized access of other criminal justice databases and may result in disciplinary action, up to and including termination.

Preventing Misuse and Ensuring Lawful Use

BPD has implemented specific safeguards to prevent misuse and ensure lawful use:

- Mandatory training on lawful ALPR use and California legal restrictions
- Regular audits of ALPR searches to ensure compliance
- System-level restrictions that block federal immigration enforcement–related searches in California
- Requirements that all searches be conducted for official police purposes and documented with an associated reference number or reason
- Prohibitions on personal or non-investigative use of ALPR data, consistent with standards applied to CLETS access

Additional safeguards addressed in Department policy Data Sharing and Interagency Access

In accordance with the California Values Act (SB54) and the BPD's ALPR Policy, the Department enforces strict limitations on data sharing. BPD does not share Flock Safety data with federal agencies, including

immigration enforcement authorities, nor with out-of-state agencies. All interstate and nationwide lookup features are disabled.

Data sharing is limited to only California law enforcement agencies. BPD reserves the right to suspend or terminate access if any misuse is discovered.

In 2025, an audit discovered two searches by a federal agency, in May, 2025, which included Burbank's ALPR data. These searches were conducted by the United States Department of Veterans Affairs Police in Loma Linda, California. The first search was related to an attempt to locate a veteran with suicidal ideations. The second search involved a reported critical missing person who was also a veteran. Although Loma Linda is located in California, the Veterans Affairs (VA) Police is a federal agency. The department does not participate in federal immigration enforcement activities, and its jurisdiction is limited to VA-controlled facilities and national cemeteries. Following this discovery, the Veterans Affairs Police was excluded from BPD's sharing network.

Use of Analytics, Facial Recognition, and AI

BPD does not use Flock data with facial recognition technology. ALPR data is not used with biometric identification systems. BPD does not employ behavioral analytics or predictive profiling tools using this data.

System Security and Data Integrity

There have been no known data breaches involving Burbank's Flock systems. BPD monitors vendor security practices and reviews reported issues in other jurisdictions. Targeted audits are conducted when newly reported issues arise to ensure the security and integrity of our data. System access is protected by authentication controls and role-based permissions. Multi-factor authentication is enabled within the Flock system to further protect data captured by BPD's system while simultaneously improving network security.

Transparency and Public Accountability

BPD continues to review its ALPR policies to ensure compliance with state and local law, alignment with community values, and transparency in the use of technology. These reviews include confirmation of data retention settings, access controls, audit practices, and interagency sharing limitations.

Frequently Asked Questions (FAQ)

Q: Does BPD share Flock data with ICE or other federal agencies?

A: No. Consistent with the California Values Act and the Trust Act, BPD does not share Flock data with federal agencies, including immigration enforcement authorities, except as required by a valid court order or subpoena.

Q: How many subpoenas or court orders have been issued for Burbank's ALPR data since its inception?

A: None.

Q: Can out-of-state or federal agencies access BPD's ALPR data?

A: No. Access to BPD ALPR data is limited to authorized personnel and California law enforcement agencies.

Q: How long is ALPR data retained?

A: ALPR data is retained for (30) days. Data is automatically deleted at the expiration of the applicable retention period.

Q: Does BPD opt into Flock's Nationwide Lookup tools?

A: No. BPD has opted out of the Nationwide lookup tools. This configuration ensures compliance with California law and ensures that data captured by BPD system is accessed and used only by California State agencies.

Q: Is facial recognition or biometric identification used with Flock systems?

A: No. BPD does not use facial recognition technology, biometric identification, biometric surveillance, behavioral analytics, or predictive profiling tools in connection with Flock systems. Nor any other technology capable of identifying or analyzing personal human characteristics in connection with its Flock Safety camera system. Flock ALPR cameras are limited to capturing images of vehicles and vehicle license plates and do not include facial recognition functionality. The system cannot be used to identify, analyze, or search for individuals based on race, ethnicity, gender, or other biometric identifiers, as defined under California law.

Q: Has BPD experienced a data breach involving Flock systems?

A: No data breaches involving the BPD Flock systems have been identified to date.

Q: Was there a public hearing prior to the purchase and installation of the Flock cameras?

A: Yes. Through the annual budget process, City Council approved a broader deployment for FY2024-2025 on May 7, May 21, and June 4, 2024, and for FY2025-2026 on May 6, May 20, and June 3, 2025.

Public comment was provided in accordance with City Council meeting protocols and the Ralph M. Brown Act.

Q: Do the Flock cameras used by the Burbank Police Department record audio?

A: No, the ALPR cameras used by the Burbank Police Department do not record audio.

Conclusion

BPD recognizes the sensitivity of surveillance technology and the importance of public trust. The use of Flock Safety systems is intentionally narrow, legally constrained, and subject to ongoing oversight. When used within these clearly defined legal and ethical boundaries, ALPR technology is a valuable tool that enhances public safety while respecting the rights and values of our community. BPD remains committed to transparency, lawful use, and continuous evaluation of whether this technology and vendor remain appropriate for the community.