

ALPR

PURPOSE

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Brisbane Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

Although the system does not retain private information of any kind, we recognize that your privacy is important to you - and THAT is important to US! Data from our ALPR system, like those from the other agencies in our County and much of the Bay Area, is uploaded and retained by the Northern California Regional Crime Information Center (NCRIC) through their database. NCRIC has a thorough policy and privacy impact assessment to assure the public of our ethical use of this data.

WHO IS AUTHORIZED TO COLLECT OR ACCESS THE DATA?

Police department employees authorized by the Chief of Police are the only people authorized to collect and view ALPR data. This may include Patrol Officers, Detectives, Community Service Officers and Code Enforcement Officers.

HOW IS THE SYSTEM MONITORED TO ENSURE THE DATA IS SECURE?

All data will be closely safeguarded and protected by both procedural and technological means. Computer systems operated by the Brisbane Police Department are part of a secure County Wide network called "LawNet." This system meets or exceeds the standards set forth by the Department of Justice for the security and transmission of law enforcement data.

As such, the Brisbane 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):

- All data downloaded to the mobile workstation and in storage 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).
- Members approved to access data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.
- System audits should be conducted on a regular basis.

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

WHO OWNS THE SURVEILLANCE TECHNOLOGY?

Equipment and Data obtained by ALPR, BWC and MAV are owned by the Brisbane Police Department. All recordings made by members on any department-issued device at any time, and any recording made while acting in an official capacity for this department, regardless of ownership of the device it was made on, shall remain the property of the Department. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

The City of Brisbane also employs the use of video surveillance to enhance security at city facilities. These systems and the data it generates are owned and operated by the City of

Brisbane.

WHAT MEASURES WERE TAKEN TO ENSURE ACCURACY?

If an ALPR system alerts that a vehicle is stolen or otherwise wanted. 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.

HOW LONG WILL THE DATA BE RETAINED?

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) 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.